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 «Защищенные информационные системы»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем

Ставрополь
2026

Содержание:

Введение

1. Цели и задачи освоения дисциплины:

Основной целью изучения дисциплины «Защищенные информационные системы» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность».

Для достижения указанной цели в процессе изучения данной дисциплины необходимо решить следующие задачи:

- изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
- изучение современных технологий построения безопасных информационных систем;
- изучение этапов и технологий проектирования и создания безопасных информационных систем;
- изучение современных программных и аппаратных средств защиты информации;
- изучение основных угроз информации в современных информационных системах и сетях;
- изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей;
- формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации; формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

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-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ИД-1 ОПК-1 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	- формулирует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности; - выделяет направления развития технологий проектирования информационных, автоматизированных и автоматических систем; - применяет методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности.
	ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Полностью оценивает роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства использует современные программные и программно-аппаратные (в том числе криптографические) средства защиты информации в профессиональной деятельности
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ИД-2 ОПК-2 выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения	применяет методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью;

	информационной безопасностью	разрабатывает тестовые планы и сценарии тестирования разработанного продукта; проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов разрабатывает модели угроз и нарушителей информационной безопасности информационных систем.
	ИД-3 ОПК-2 решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Реализует выполнение типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; использует средства автоматизированного и ручного функционального тестирования

Практическая работа №1

по учебной дисциплине **«Защищенные информационные системы»**

Понятие, виды и структура информационных систем

1. Цель работы

1. Изучить способы исследования методов аутентификации
2. Исследовать способы управления доступом

2. Подготовка к занятию

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

3. 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.

3.1. 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.

3.2. 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.

3.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

1. организационные;
2. технологические;
3. правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;
2. знаний некоторой известной только ему и проверяющей стороне информации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных

индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (си rect passnrOrd authenti Ceti OH). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted thi гси рагу authenti сан оп). При этом третью сторону называют сервером аутентификации (authenti Ceti оп server) или арбитром (аГbitretor).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

— по хранимой копии пароля или его свёртке (p1 ai ntext-equi a] еп);
— по некоторому проверочному значению (veri f i er-based) ;
— без непосредственной передачи информации о пароле проверяющей стороне (zero-knowl edge) ;
— с использованием пароля для получения криптографического ключа (CryptographiC).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение

злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств, задействованных в них математических и криптографических преобразований, и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя - совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

— интерфейс пользователя;

— интерфейс администратора;

— модуль сопряжения с другими подсистемами безопасности;

— база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:

— подбор в интерактивном режиме;

— подсматривание;

— преднамеренную передачу пароля его владельцем другому лицу;

— захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);

— перехват переданной по сети информации о пароле;

— хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы через:

— внедрение программных закладок;

— обнаружение и использование ошибок, допущенных на стадии разработки;

— выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

— выбрать пароль, который легко запомнить и также легко подобрать;

— записать пароль, который сложно запомнить, и положить запись в доступном месте;

— ввести пароль так, что его смогут увидеть посторонние:

— передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароляя	Получаемый эффектя
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или
Использование в пароле различных групп	Усложняет задачу злоумышленника при попытке подобрать пароль методом
Проверка и отбраковка пароля по	Усложняет задачу злоумышленника при
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его
Ведение журнала истории паролей	Обеспечивает дополнительную степень

Применение эвристического алгоритма, бракующего пароли на основании	Усложняет задачу злоумышленника при попытке подобрать пароль п о словарю
Ограничение числа попыток ввода	Препятствует интерактивному подбору
Поддержка режима принудительной смены	Обеспечивает эффективность требования,
Использование задержки при вводе	Препятствует интерактивному подбору
Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль п о словарю. Если алгоритм генерации

Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи

2. Примеры.

Например 1.

Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.

Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: C=n=1 06

Примем скорость перебора X10 паролей в секунду. Получаем время перебора всех паролей t= C/б10^5секунд~1667минут~28часов~1,2 дня.

Примем, что после каждого из т=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей

T=t*5/3=16667секунд~2778минут~46часов 1,9 дня.

^{T}итог = 1+T = 1,2 + 1,9 = 3,1 ДНЯ

2. Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы n=10.

Длина пароля рассчитывается: k=1 оуп C=1 g C.

Определим количество вариантов C= t * б=10лет* 10 паролей в сек. =

10* 10* 365* 24* 60* 603,15* 10^9 вариантов

Таким образом, получаем длину пароля: k=1 g (3,15* 10^9) = 9,5

Очевидно, что длина пароля должна быть не менее 10 символов.

3. Задания..

1. Определить время перебора всех паролей с параметрами.

Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из т неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	т	v
1	33	10	100	о	о
2	2 6	1 2	1 3	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из П символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	П	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

Контроьные вопросы:

1) Перечислить виды атак на пароли.

2) Перечислить критерии стойкости парольной защиты.

3) Перечислить и охарактеризовать методы противостояния атаке полным перебором.

4) Охарактеризовать влияние длины пароля на вероятность раскрытия.

5) Сформировать рекомендации по составлению паролей.

6) Перечислить типы угроз безопасности парольных систем.

7) Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

8) Определить время перебора всех паролей, состоящих из 6 цифр

Практическая работа №2

по учебной дисциплине **«Защищенные информационные системы»**

Угрозы безопасности в информационных системах

1. Цель работы

1. Исследовать сбор и анализ данных NetFlow

2. Подготовка к занятию

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

3. 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.

3.1. 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.

3.2. 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.

3.3. Требования безопасности по окончании работы

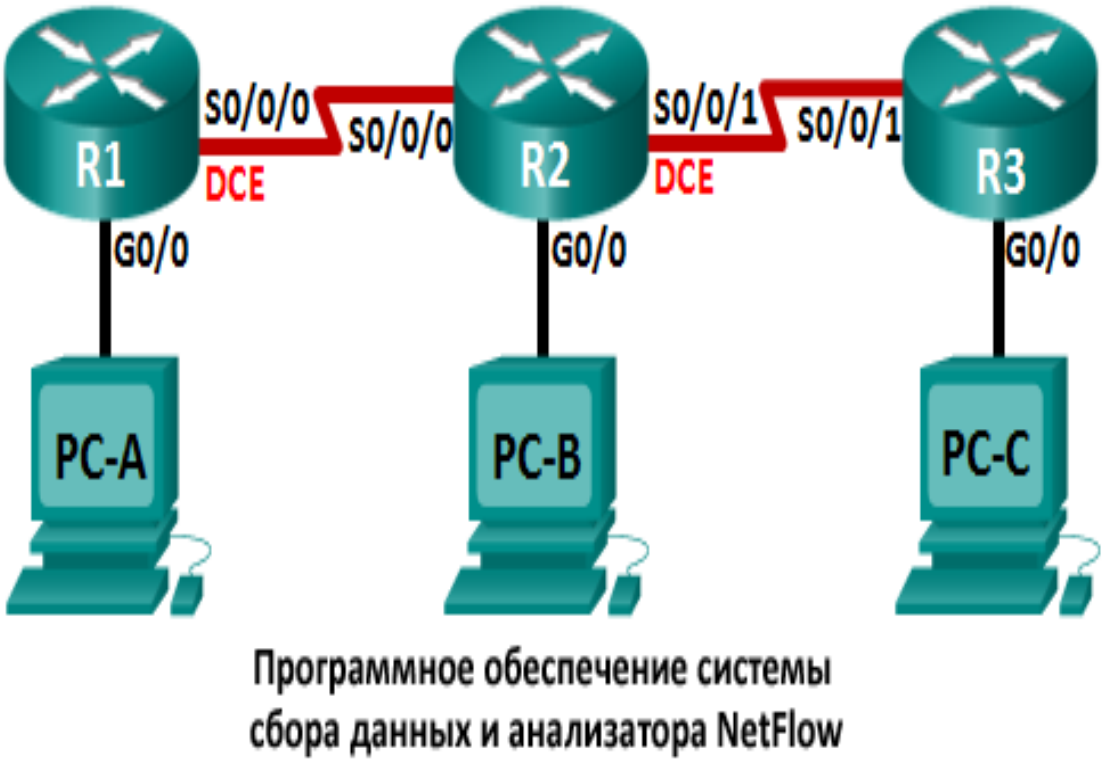
- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить

руководству

Сбор и анализ данных NetFlow

Топология



Программное обеспечение системы сбора данных и анализатора NetFlow

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

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка NetFlow на маршрутизаторе

Часть 3. Анализ NetFlow с помощью интерфейса командной строки

Часть 4. Изучение ПО сбора данных и анализатора NetFlow

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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.

Часть 1: 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 VTY 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.

Часть 2: 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 B. 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

— 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

Часть 3: 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 1: 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 A 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 2: 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 ager 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 3: 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 A.

Шаг 4: 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 ager 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	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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

Часть 4: 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

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

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.

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.

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 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 192.168.2.1 255.255.255.0
 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
```

Контрольные вопросы:

1) Этапы и средства реализации атак. Классификация атак.
2) Таксономия систем обнаружения атак.
3) Совместное применение систем обнаружения атак и других средств защиты.
4) Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
5) Анализ журналов регистрации и сетевого трафика.
6) Анализ заголовков, процессов, сервисов и портов.
7) Настроить NetFlow на маршрутизаторе.

8) Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

Практическая работа №3

по учебной дисциплине **«Защищенные информационные системы»**

Анализ требований стандартов информационной безопасности к защищенным информационным системам

1.Цель работы: Ознакомиться с приложениями, включенными в состав СУБД MySQL. Получить навыки управления учетными записями пользователей и определения привилегий. Ознакомиться с утилитами, входящими в состав СУБД MySQL, получить навыки работы с ними.

2. Подготовка к занятию

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

3. 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.

3.2. 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.

3.3. Требования безопасности по окончании работы

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

руководству

Запуск MySQL

Управление сервером обычно осуществляется из командной строки. Запуск в Windows осуществляется через сеанс командной строки выполнением следующей команды:

```
D:\usr\local\Mysql\bin\mysqld --standalone
```

Эта команда запустит демон mysql в фоновом режиме. В Windows 95/98 не предусмотрен запуск mysqld в виде службы. В Windows 2000 демон mysql запускается в виде службы.

Можно осуществить запуск winmysqladmin.exe, в этом случае все настройки перечисляются в файле my.ini

При запуске mysqld можно указывать следующие опции:

Таблица 1- Опции команды MySQLD

`-?, --help`	Справка
`-b, --basedir=[path]`	Путь к каталогу в котором установлен mysql
`-h, --datadir [homedir]`	Путь к каталогу, в котором хранятся базы данных.
`-l, --log=[filename]`	Имя журнала транзакций
`-L, --language=[language]`	Язык по умолчанию(обычно English).
`-P, --port=[port]`	Порт для соединения.
`--skip-grant-tables`	Игнорировать таблицы привилегий. Это дает любому ПОЛНЫЙ доступ ко всем таблицам. Не следует предоставлять обычным пользователям разрешений на запуск mysqld.
`--skip-name-resolve`	Позволяет предоставлять доступ только тем хостам, чьи IP-адреса указаны в таблицах привилегий. Ипользуется для более высокого уровня защиты.
`--skip-networking`	Использовать подключения только через интерфейс localhost.
`-V, --version`	Вывести информацию о версии.

Наличие в статусной строке иконки светофора с активным зеленым цветом указывает на то, что сервер запущен (см. рис 1).

Рисунок 1 - Приложение winmysqladmin запущено

Теперь можно попытаться войти в сервер. В случае, если предполагается управление сервером через консоль, то необходимо использовать команду **mysql**. Изначально существует единственный пользователь, которому предоставляется право входа - **root**, которая не имеет пароля. Первое, что нужно сделать войти под именем **root** и зарегистрировать нового пользователя

и установить для него пароль. Команда **mysql** может использовать следующие опции:

Таблица 2 - Опции команды MySQL

-?, --help	Справка
-h,--hostname=[hostname]	Имя сервера mysql.
-u, --user=[user]	Имя пользователя для доступа к mysql.
-p, --password=[password]	Пароль пользователя для доступа к mysql.
-P, --port=[port]	Порт для соединения с сервером.
-V, --version	Информация о версии

Примечание. Команды mysqld и mysql имеют еще некоторые опции, но в данный момент они особого интереса не представляют.

Запуск из сеанса ДОС осуществляется как показано на Рисунок 2 (в указанном случае осуществляется подключение к БД mysql).

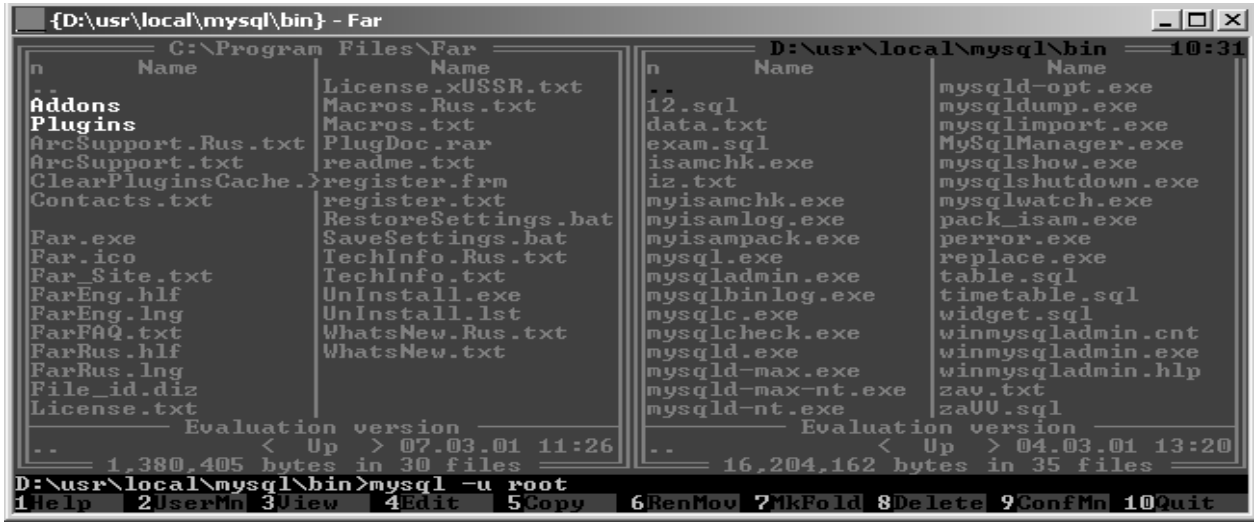


Рисунок 2 - Запуск консоли MYSQL

Для выполнения в строке наберите команду: **mysql –u root**

```
The FAR manager, version 1.70 beta 3 (build 591)
Copyright (C) 1996-2000 Eugene Roshal, Copyright (C) 2000-2001 FAR Group
Evaluation copy, please register.
D:\usr\local\mysql\bin>mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3 to server version: 3.23.41-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> _
```

Рисунок 3 - Успешный запуск консоли

Если вы это получили, значит вы успешно вошли в консоль mysql, которая используется для администрирования сервера.

Для составления отчета вам понадобятся приведение команд, которые вы будете посылать на сервер. В MySQL имеется возможность ведение протокола выполняемых команд, чтобы запустить ведение протокола необходимо выполнить команду

\T filename

!!! обязательно в верхнем регистре. Filename – имя файла, в который будут записываться команды (создается автоматически при выполнении команды, и действует во время жизни сеанса, т.е. в случае отключения от сервера лог прерывается и для возобновления необходимо повторить команду с выводом в новый файл, так как команда затирает имеющиеся в файле данные).

Просмотр списка БД, доступных на сервере осуществляется командой ***SHOW DATABASES.***

Для выполнения в строке наберите команду: **show databases.**

Командой: **USE MYSQL;** – выбираем текущую БД где MYSQL имя БД.

Система привилегий и безопасность в MySQL

— User
— Db
— Host
— Пользовательские привилегии

База данных mysql и таблицы привилегий.

Итак, вы успешно вошли в базу данных mysql, которая используется для администрирования сервера. Что же здесь находится? А находятся здесь 5 таблиц, которые ничем не отличаются от других таблиц баз данных, за исключением того, что эти таблицы используются для предоставления доступа к базам данных и таблицам в них пользователям. Рассмотрим каждую из них.

Введите следующую команду, **show tables,** которая покажет таблицы в базе данных mysql.

Кратко рассмотрим функции каждой из таблиц:

Таблица User

Определяет, разрешено ли пользователю, пытающемуся подключиться к серверу делать это. Содержит имя пользователя, пароль а также привилегии. Если ввести команду show columns from user; то получим следующее:

Таблица 3- Структура таблицы User

Field	Type	Null	Key	Default	Extra
Host	char(60)		PRI		
User	char(16)		PRI		
Password	char(41)				
Select_priv	enum('N','Y')			N	
Insert_priv	enum('N','Y')			N	
Update_priv	enum('N','Y')			N	
Delete_priv	enum('N','Y')			N	
Create_priv	enum('N','Y')			N	
Drop_priv	enum('N','Y')			N	
Reload_priv	enum('N','Y')			N	
Shutdown_priv	enum('N','Y')			N	
Process_priv	enum('N','Y')			N	
File_priv	enum('N','Y')			N	
Grant_priv	enum('N','Y')			N	
References_priv	enum('N','Y')			N	
Index_priv	enum('N','Y')			N	
Alter_priv	enum('N','Y')			N	
Show_db_priv	enum('N','Y')			N	
Super_priv	enum('N','Y')			N	
Create_tmp_table_priv	enum('N','Y')			N	
Lock_tables_priv	enum('N','Y')			N	
Execute_priv	enum('N','Y')			N	
Repl_slave_priv	enum('N','Y')			N	
Repl_client_priv	enum('N','Y')			N	
Create_view_priv	enum('N','Y')			N	
Show_view_priv	enum('N','Y')			N	

Create_routine_priv	enum('N','Y')			N	
Alter_routine_priv	enum('N','Y')			N	
Create_user_priv	enum('N','Y')			N	
Event_priv	enum('N','Y')			N	
Trigger_priv	enum('N','Y')			N	
ssl_type	enum('','ANY','X509','SPECIFIED')				
ssl_cipher	blob			NULL	
x509_issuer	blob			NULL	
x509_subject	blob			NULL	
max_questions	int(11) unsigned			0	
max_updates	int(11) unsigned			0	
max_connections	int(11) unsigned			0	
max_user_connections	int(11) unsigned			0	

Изначально эта таблица содержит пользователя root без пароля. По умолчанию root может входить с любого хоста, имеет все привилегии и доступ ко всем базам данных.Также в таблице содержится запись для пользователя '%'.

В БД MYSQL содержатся таблицы, называемых таблицами привилегий. Система привилегий будет подробно рассмотрена в следующих работах, а пока вы можете выполнить команды на добавления своего пользователя:

Для добавления нового пользователя **your_name**, можно выполнить следующие операторы языка (Insert):

Insert into user (host, user, password, ssl_cipher, x509_issuer, x509_subject) values ('localhost', 'your_name', password('your_pass'), '', '', '');

Выполнением команды

Select host, user, password from user;

Мы выводим перечисленные поля в виде таблицы

Host	User	Password
%	root	456g879k34df9

Если необходимо выделить все столбцы таблицы, то необходимо набрать * в качестве аргумента команды ***select***.

Чтобы изменения вступили в силу нужно перегрузить сервер, предварительно закончив текущий сеанс работы командой ***quit***.

mysqladmin -u root reload (эта команда перегружает сервер)

После установки пароля для пользователя нужно перезагрузить сервер командой mysqladmin reload, чтобы изменения вступили в силу. После этого можно попробовать войти снова:

Mysql/bin/***mysql -u your_name -p mysql***
Enter password:*******

Если же после этой операции вы не получите приглашение ко входу, то необходимо будет повторить вход в сервер под учетной записью **ROOT** и назначить необходимые права**.** Т.о., недостаточно добавить сведения о пользователе в системную БД, дополнительно необходимо назначить права пользователю, после чего можно начинать настраивать таблицы привилегий, вводить новых пользователей, создавать базы данных и таблицы, то есть делать все то, что называется администрированием. Назначить права можно указанием инструкцией ***INSERT*** для заполнения соответствующие привилегии (перечень привилегий см.табл.3)

Mysql/bin/***mysql -u root***
И выполнить следующий запрос к БД:

Mysql>***USE MYSQL;***
Mysql>***GRANT ALL PRIVILEGES ON *.* TO 'your_name'@'localhost' IDENTIFIED BY 'your_pass' WITH GRANT OPTION;***
Mysql>***FLUSH PRIVILEGES;***

Если пароль был случайно забыт, чтобы его задать по новой, придется стереть файлы mysql.frm mysql.MYI и mysql.MYD из папки с базами данных, затем запустить скрипт mysql_install_db и повторить все по новой. Можно воспользоваться ключом MYSQL и ввести **--skip-grant-tables,** при этом все пароли будут имеет пустое поле.

Команда имеет вид ***mysqld --skip-grant-tables.***

Пояснения:

1.Команда insert вставляет данные в таблицу, не забывайте завершать команды ';'.

2.При вводе пароля используйте функцию password(), иначе пароль работать не будет!

3.Все пароли шифруются mysql, поэтому в поле Password вы видите абракадабры. Это делается в целях безопасности.

4.Не есть хорошей практикой назначать привилегии пользователям в таблице user, так как в этом случае они являются глобальными и распространяются на все базы данных. Предоставляйте привилегии каждому пользователю к конкретной базе данных в таблице db, которая будет рассмотрена далее.

5.При задании имени хоста для входа через сеть рекомендуется явно указывать полное имя хоста, а не '%'. В приведенном выше примере пользователю mary разрешается вход на сервер со всех машин домена tomsk.ru. Можно также указывать IP-адреса машин и маски подсетей для большей безопасности.

Таблица Db

Определяет к каким базам данных каким пользователям и с каких хостов разрешен доступ. В этой таблице можно предоставлять каждому пользователю доступ к базам данных и назначать привилегии. Если выполнить команду ***show columns from db;*** получим следующее:

Таблица 4 - Структура таблицы Db

Field	Type	Null	Key	Default	Extra

Host	char(60)		PRI		
Db	char(32)		PRI		
User	char(16)		PRI		
Select_priv	char(1)			N	
Insert_priv	char(1)			N	
Update_priv	char(1)			N	
Delete_priv	char(1)			N	
Create_priv	char(1)			N	
Drop_priv	char(1)			N	

— По умолчанию, все привилегии установлены в 'N'. Например, предоставим юзеру mary доступ к базе данных mysql и дадим ему привилегии **select**, **insert** и **update** (описание основных команд mysql будет дано в следующих лабораторных работах, сейчас ваша цель увидеть, как работают таблицы привилегий).

— Для справки:

```
Insert into db (host, user, db, select_priv, insert_priv, update_priv)
Values (''localhost', 'your_name', mysql, 'Y', 'Y', 'Y');
```

— Привилегии, устанавливаемые в таблице db, распространяются только на базу данных library. Если же установить эти привилегии в таблице user, то они будут распространяться и на другие базы данных, даже если доступ к ним и не установлен явно.

Таблица Host

Таблица host используется для расширения диапазона доступа в таблице db. К примеру, если доступ к какой-либо базе данных должен быть предоставлен более чем одному хосту, тогда следует оставить пустой колонку host в таблице db, и внести в таблицу host необходимые имена хостов. Выполним команду

show columns from host;

Таблица 5 - Структура таблиц Host

Field	Type	Null	Key	Default	Extra
Host	char(60)		PRI		
Db	char(32)		PRI		
Select_priv	char(1)			N	
Insert_priv	char(1)			N	
Update_priv	char(1)			N	
Delete_priv	char(1)			N	
Create_priv	char(1)			N	
Drop_priv	char(1)			N	

Как видно из таблицы, здесь также можно задавать привилегии для доступа к базе данных.Они обычно редко используются без необходимости. Все привилегии доступа нужно задавать в таблице db для каждого пользователя, а в таблице host только перечислить имена хостов.Сервер читает все таблицы, проверяет имя пользователя, пароль, имя хоста, имя базы данных, привилегии.Если в таблице db привилегии select, insert установлены в 'Y', а в таблице host в 'N', то в итоге юзер все равно получит 'Y'.Чтобы не вносить путаницы, лучше назначать привилегии в таблице db.

Эти 3 таблицы являются основными.В новых версиях MySQL, начиная с 3.22 добавлены еще 2 таблицы- tables_priv и columns_priv, которые позволяют задать права доступа к определенной таблице в базе данных и даже к определенной колонке. Они работают подобно таблице db, только ссылаются на таблицы и колонки. Также, начиная с версии 3.22 можно использовать команду GRANT для предоставления доступа к базам данных, таблицам и колонкам таблиц, что избавляет от необходимости вручную модифицировать таблицы db, tables_priv и columns_priv. Команда GRANT будет подробно рассмотрена в следующих разделах.

Привилегии, предоставляемые MySQL

Таблица 6 - Привилегии пользователя

Привилегия	Колонка	Где используется

select	Select_priv	таблицы
insert	Insert_priv	таблицы
Update	Update_priv	таблицы
delete	Delete_priv	таблицы
index	Index_priv	таблицы
alter	Alter_priv	таблицы
create	Create_priv	БД, таблицы, индексы
drop	Drop_priv	БД или таблицы
grant	Grant_priv	БД или таблицы
References	References_priv	БД или таблицы
reload	Reload_priv	администрирование сервера
Shutdown	Shutdown_priv	администрирование сервера
Process	Process_priv	администрирование сервера
file	File_priv	доступ к файлам на сервере

Основные утилиты MySQL.

В состав дистрибутива MySQL входят следующие утилиты:

— mysqld
— mysql
— mysqladmin
— mysqlaccess
— mysqlshow
— mysqldump
— isamchk

Утилиты **mysqld** и **mysql** были подробно рассмотрены ранее, поэтому возвращаться к ним не будем. Кратко рассмотрим остальные.

Mysqladmin

Утилита для администрирования сервера. Может использоваться администратором, а также некоторыми пользователями, которым предоставлены определенные привилегии, например – **Reload_priv, Shutdown_priv, Process_priv** и **File_priv**. Данная команда может использоваться для создания баз данных, изменения пароля пользователя(администратор может изменить пароль любому пользователю, а рядовой пользователь – только свой собственный), перезагрузки и остановки сервера, просмотра списка процессов, запущенных на сервере. Mysqladmin поддерживает следующие команды:

Таблица 7 - Опции команды MySQLadmin

Create [database_name]	Создает базу данных
Drop [database_name]	Удаляет базу данных и все таблицы в ней
Reload	Перезагружает сервер
Shutdown	Останавливает работу сервера MySQL
Processlist	Выводит список процессов на сервере
Status	Выводит сообщение о статусе сервера

Пример использования mysqladmin для изменения пароля:

mysqladmin -u your_name password your_pass

Следует заметить, что в случае использования mysqladmin для установки пароля, не требуется использование функции password().Mysqladmin сам заботится о шифровании пароля.

Mysqlaccess

Используется для проверки привилегий пользователя для доступа к конкретной базе данных. Общий синтаксис:

mysqlaccess [host] [user] [db] опции

Полезная утилита для проверки прав доступа пользователя, если он получает сообщение Access denied, при попытке соединиться с базой данных.

Опции:

Таблица 8 - Опции команды MySQLAccess

-?, --help	Справка
-u, --user=[username]	Имя пользователя
-p, --password=[password]	Пароль пользователя
-h, --host=[hostname]	Имя хоста для проверки прав доступа
-d, --db=[dbname]	Имя базы данных для проверки прав доступа
-U, --superuser=[susername]	Имя суперпользователя(root)
-P, --spassword=[spassword]	Пароль администратора
-b, --brief	Выводит краткие сведения о таблице

Mysqlshow

Используется, чтобы показать, с какими базами данных работает сервер, какие таблицы содержит каждая БД и какие колонки есть в каждой таблице.Синтаксис:

mysqlshow [опции] [database [table [field]]]

Mysqlshow может использовать следующие параметры:

Таблица 9 - Параметры команды Mysqlshow

-?, --help	Справка
-h, --host=[hostname]	Имя сервера
-k, --key	Показать ключи для таблицы
-p, --password=[password]	Пароль пользователя
-u, --user=[username]	Имя пользователя
-p, --port=[port]	Порт для связи
-V, --version	Вывести информацию о версии

Если ввести mysqlshow без аргументов, будут показаны все базы данных, если указать имя БД, будут показаны все таблицы в ней.

Команды

mysqlshow

mysqlshow mysql

Mysqldump

Программа mysqldump используется для создания дампа содержания базы данных MySQL. Она пишет инструкции SQL в стандартный вывод. Эти инструкции SQL могут быть переназначены в файл. Можно резервировать базу данных MySQL, используя mysqldump, но при этом Вы должны убедиться, что в этот момент с базой данных не выполняется никаких других действий. А то mysqldump Вам такого нарезервирует...

Программа mysqldump поддерживает следующие параметры (Вы можете использовать короткую или подробную версию):

Таблица 10 - Опции команды MySQLdump

-#, --debug=[options]	**Вывести в протокол отладочную информацию. В общем виде 'd:t:o, filename`.**
-?, --help	Справка.
-c, --compleat-insert	Генерируйте полные инструкции insert (не исключая значений, которые соответствуют значениям столбца по умолчанию).
-h, --host=[hostname]	Соединиться с сервером hostname.
-d, --no-data	Экспорт только схемы информации (исключая данные).
-t, --no-create-info	Экспорт только данных, исключая информацию для создания таблицы. Противоположность -d.
-p, --password=[password]	Пароль пользователя, для соединения с сервером MySQL. Обратите внимание, что не должно быть пробела между -p и паролем.

-q, --quick	Не буферизовать результаты запроса, дамп выдать непосредственно к STDOUT.
-u, --user=[username]	Имя пользователя. Если не задано, используется текущий логин.
-v, --verbose	Вывести подробную информацию относительно различных стадий выполнения mysqldump.
-P, --port=[port]	Порт для связи.
-V, --version	Информация о версии.

Вы можете направить вывод mysqldump в клиентскую программу MySQL, чтобы копировать базу данных. ПРИМЕЧАНИЕ: Вы должны убедиться, что база данных не изменяется в это время, иначе Вы получите противоречивую копию!

Для справки:

mysqldump -u root -p mysql user>mysql-1.sql

mysqldump -u root mysql>mysql-2.sql

Примечание флаг –p используется в случае, если пользователь наделен паролем.

После выполнения этой команды у нас появился файл mysql-1.sql и mysql-2.sql. Загрузим их в текстовый редактор, чтобы поподробнее изучить, и, возможно, немного поправить.

Задание

Запустите сервер MySQL. Зарегистрируйте своего пользователя в консольном приложении, задайте ему права.

С помощью утилиты Mysqlshow выполните команду на просмотр структуры и состав таблиц базы Mysql. Приведите в отчете её схему. С помощью утилиты Mysqldump получите полный дамп базы Mysql (данные и таблицы), а также отдельные дампы таблиц и данных.

Контрольные вопросы:

1. Каким способом возможен запуск серверной части СУБД.

2. Что такое привилегия. Каково её предназначение.

3. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

Практическая работа №4

по учебной дисциплине **«Защищенные информационные системы»**

Политика и модели безопасности в информационных системах

1. Цель работы:

1) Изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера;

2) Практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана «Outpost»;

3) Изучение работы рассматриваемых систем в «совместном» режиме для защиты и тестирования рабочих станций на наличие уязвимостей.

2. Подготовка к занятию

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

3. 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.

3.1. 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.

3.2. 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.

3.3. Требования безопасности по окончании работы

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

1. Теоретические сведения.

Интенсивная информатизация государственных и муниципальных управленческих структур, промышленных предприятий и корпораций, силовых ведомств, научных, медицинских и других учреждений выдвинула на первый план вопросы безопасности информационных ресурсов.

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую. Как правило, через «дыры» в данных сервисах осуществляется большая часть удачных атак извне, которые, зачастую, кончаются потерей компанией секретных данных.

Ярким примером наличия подобных уязвимостей могут послужить популярные операционные системы WindowsXP и FreeBSD. Так, в MS Windows, по-умолчанию, работает довольно много неиспользуемых сервисов, которые в большинстве своем связаны с открытыми портами, через которые злоумышленник может провести атаку. Всем, наверное, известен факт, когда

множество «автономных» пользовательских компьютеров пострадали во всем мире в результате атаки на порт 135 (RPC). Что касается FreeBSD, то здесь также после стандартной установки в системе работают демоны, которые в обычных случаях не требуются, а значит, являются дополнительными источниками уязвимостей в компьютере. Атаки на почтовый сервер sendmail приводят к полному получению злоумышленником контроля над хостом. Откуда sendmail, спросите вы? Да, иногда, в UNIX-системах, в том числе адаптированных для работы в качестве рабочей станции, в конфигурации «по-умолчанию» можно встретить и такие сервисы…

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому, «самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

Тем не менее, при использовании специальных средств защиты, подобных нежелательных событий можно, как правило, избежать.

Основными средствами защиты на сегодняшней день являются две категории специализированных программ:

Межсетевые экраны (брандмауэры, FireWall, МСЭ);

Сканеры (сканеры открытых портов и сервисов).

Следует сказать, что брандмауэр – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

1.1. Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls).

Архитектура firewall

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания правил. В сущности, создаются два списка: отрицание (deny) и разрешение

(permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

- если никакое правило соответствия не найдено, то удалить пакет из сети;
- если соответствующее правило найдено в списке разрешений, то пропустить пакет;
- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. Отметим преимущества firewall, основанного на фильтрации пакетов:

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;
- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

- нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
- нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
- работа ведется с ограниченной информацией пакета;

— в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
— слабо защищен сам компьютер, на котором запущен firewall, то есть предметом атаки может стать сам этот компьютер;
— нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
— возможно, что большой объем правил будет тормозить проверку.

Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

— уникальный идентификатор сессии передачи, который используется для контроля;
— состояние сессии передачи: установлено, передано или закрыто;
— информация о последовательности пакетов;
— адрес источника цепи;
— адрес получателя цепи;
— физический интерфейс, используемый для получения цепи;
— физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи. Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре. Основные преимущества firewall цепного уровня:

— firewall цепного уровня быстрее программного, так как производит меньше проверок;
— firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
— возможно скрытие внутренней топологии сети.

Недостатки firewall цепного уровня:

— нет проверки пакетов на программном уровне;
— слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
— нет проверки передаваемых данных;
— трудно проверить разрешение или отрицание передачи пакетов.

Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется proxy-сервис, который кэширует информацию для более быстрой ее обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через proxy, который является шлюзом. У proxy две части: сервер и клиент. Сервер принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях. Достоинства proxy:

— понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;
— сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;

— возможен запрет доступа к некоторым сетевым сервисам;
— есть возможность управления пакетами данных;
— есть сокрытие внутренних адресов и топологии сети, так как proxy является фильтром;
— остается видимость прямого соединения сетей;
— proxy может перенаправлять запросы сетевых сервисов на другие компьютеры;
— есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
— возможно создание подробных отчетных записей для администратора.

Недостатки proxy:

— требует изменения сетевого стека на машине, где стоит firewall;
— нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как proxy перехватывает работу портов;
— неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно proxy;
— так как proxy должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой proxy;
— нет proxy для UDPи RPC;
— иногда необходима специальная настройка клиента для работы с proxy;
— proxy не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;
— корректность работы proxy напрямую связана с правильностью обработки сетевого стека;
— использование proxy может требовать дополнительных паролей, что неудобно для пользователей.

Динамическая фильтрация пакетов (dynamic packet filter firewalls)

В основном этот уровень повторяет предыдущий, за двумя важными исключениями:

— возможно изменение правил обработки пакетов «на лету»;
— включена поддержка UDP.

Уровень kernel proxy

Уровень kernel proxy возник достаточно недавно. Основная его идея — попытка поместить описанный выше алгоритм firewall программного уровня в ядро операционной системы, что избавляет компьютер от лишних затрат времени на передачу данных между ядром и программой proxy. Это повышает производительность и позволяет производить более полную проверку проходящей информации.

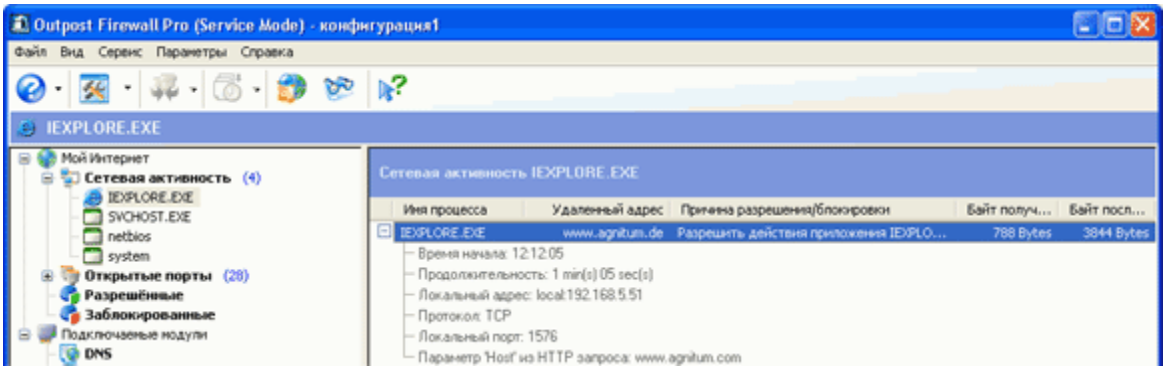
Примеры межсетевых экранов

1. Аппаратный (D-Link)

DFL-1100

Межсетевой экран для сетей крупных предприятий

2. Программный (Agnitum Outpost)



1.2. Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

Архитектура сканера

Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из

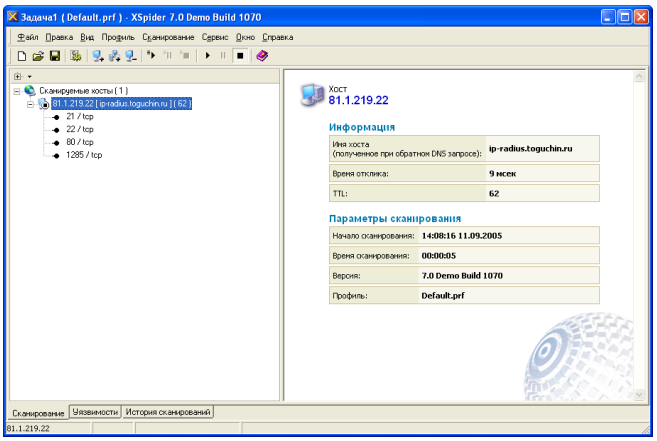
наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы. Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 10000.

Пример сканера XSpider



2. Порядок выполнения работы.

Условия выполнения лабораторной работы. Данная работа должна выполняться в присутствии администратора компьютерного класса или уполномоченного им лица, которому предоставляются права на осуществление следующих действий в операционных системах Windows2000 – XP, работающих как в сетевом режиме, так и в одиночном режиме:

1.1. права на установку программного обеспечения;

1.2. права на работу как в составе рабочей группы или домена Windows, так и в составе локального администратора рабочей станции;

1.3. права на предоставление учетной записи учащимся, позволяющей установку ПО.

Практическая работа проводится в двух вариантах:

1. Автономный.

В компьютерном классе должны находиться не менее 2-х машин, объединенных в сеть. На первой устанавливается *сетевой сканер* или *межсетевой экран*. В случае установки МСЭ вторая машина используется для тестирования защиты первой от ICMP пакетов с помощью стандартной утилиты *ping*. При «автономном» тестировании сканера вторая машина будет использоваться в качестве исследуемого объекта.

2. Совместный.

В компьютерном классе должны находиться также не менее 2-х машин, объединенных в сеть. На части из них устанавливается *сканер*, на остальных – МСЭ. При этом для проверки защиты рабочей станции от ICMP пакетов с помощью МСЭ (а также для тестирования сканера) будет использоваться сетевой сканер.

Администратор! Обрати внимание. После установки изучаемого ПО межсетевые экраны могут заблокировать доступ сетевого трафика к рабочим станциям, тем самым, нарушив работоспособность сети. Для предотвращения данной ситуации необходимо сразу назначить всем МСЭ политику «разрешения».

Порядок работы

Работа будет проходить в два этапа. Первый этап предназначен для изучения работы XSpider, Outpost и WindowsXP в «автономном» режиме. Второй этап – для изучения работы в совместном режиме. На каждом этапе студенты делятся на две группы, одна из которых будет работать с МСЭ, вторая – со сканером или псевдосканером (утилитой ping).

Действия, общие для двух этапов:

1. Взять из папки \\m00\fit2005 файлы установки сканера XSpider и МСЭ Agnitum Outpost;
2. На каждом рабочем месте выполнить установку сканера и МСЭ;
3. При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
4. Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;
5. Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» -> «Выполнить» -> “cmd” -> “ipconfig /all”;

Этап 1. Автономный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)
2. Смотреть на ответные пинг-пакеты.
3. Фиксировать моменты, когда ответные пакеты пропадают и появляются.
4. Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить состояние ответов на ping-запросы у напарника;
4. Повторить п.1-2 несколько раз.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

Этап 2. Совместный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить утилиту сканирования сети XSpider;
2. В меню «Правка» выбрать «Добавить хост»;
3. Введите IP-адрес хоста напарника;
4. Узнать у напарника текущий режим работы МСЭ;
5. В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не

будет без установки в XSpider специальной опции: меню «Профиль» -> «Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».
6. Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить, как работает XSpider у напарника;
4. Повторить п.1-2 несколько раз для двух режимов XSpider – требующего ICMP-ответа и не требующего.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

По завершению лабораторной работы установленное в процессе занятия ПО необходимо удалить из системы.

3. Отчет

После окончания практической части лабораторной работы студенты должны предоставить письменный отчет, содержащий информацию о проделанной работе и ответы на вопросы в следующем формате:

1. Ф.И.О.
2. Ф.И.О. Напарника
3. Имя и адрес рабочего компьютера.
4. Имя и адрес исследуемого компьютера.
5. Опишите утилиту ping, методы и случаи ее применения.

6. Описать данные, полученные о компьютере напарника с помощью XSpider
7. Какого типа уязвимости были найдены?
8. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
9. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия? (доп +)
10. Выводы.

Контрольные вопросы :

9) Опишите утилиту ping, методы и случаи ее применения.

10)Описать данные, полученные о компьютере с помощью XSpider

11)Опишите типы уязвимостей компьютерных систем

12)Как можно предотвратить появление таких уязвимостей с помощью изученных средств?

13)Описать известные типы МСЭ и отличия между ними.

Практическая работа №5

по учебной дисциплине **«Защищенные информационные системы»**

Межсетевое экранирование

1. Цель работы

1. Исследовать настройки туннеля VPN GRE по схеме «точка-точка»
2. Исследовать принципы настройки базового PPP с аунтификацией.

2. Подготовка к занятию

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

3. 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.

3.1. 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.

3.2. 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.

3.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить

руководству

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология

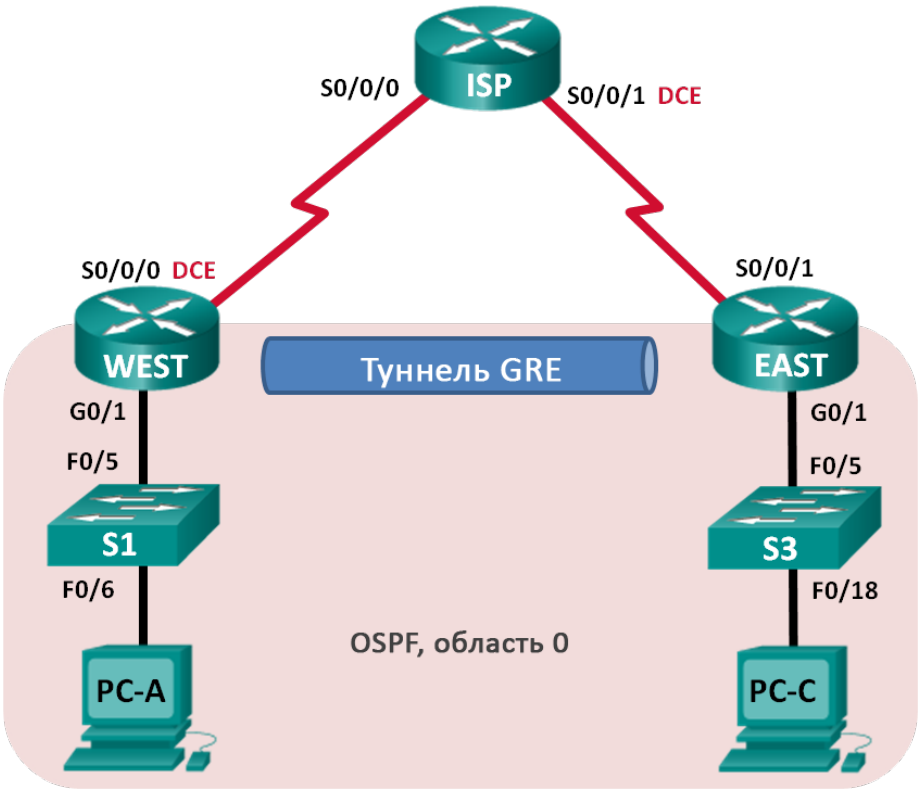


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы

сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4
- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка-точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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 порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 5: Базовая настройка устройств

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

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

- Отключите поиск DNS.
- Назначьте имена устройств.
- Зашифруйте незашифрованные пароли.
- Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
- Настройте ведение журнала состояния консоли на синхронный режим.
- Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

— Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

EAST(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхо-запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 6: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

— Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

WEST(config)# **interface tunnel 0**
WEST(config-if)# **ip address 172.16.12.1 255.255.255.252**
WEST(config-if)# **tunnel source s0/0/0**
WEST(config-if)# **tunnel destination 10.2.2.1**

— Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

EAST(config)# **interface tunnel 0**

EAST(config-if)# **ip address 172.16.12.2 255.255.255.252**

EAST(config-if)# **tunnel source 10.2.2.1**

EAST(config-if)# **tunnel destination 10.1.1.1**

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

— Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

WEST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.1.1 YES manual up up

Serial0/0/0 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Tunnel0 172.16.12.1 YES manual up up

EAST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.2.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.2.2.1 YES manual up up

Tunnel0 172.16.12.2 YES manual up up

— С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

_____

_____

_____

_____

Используется протокол туннелирования GRE. Для маршрутизатора WEST источник туннеля — 10.1.1.1 (Serial0/0/0), а назначение — 10.2.2.1. Для маршрутизатора EAST источник туннеля — 10.2.2.1, а назначение — 10.1.1.1.

WEST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.1/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/0

Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:12, output 00:00:12, output hang never
Last clearing of "show interface" counters 00:01:29
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
5 packets input, 620 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5 packets output, 620 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out

EAST# **show interfaces tunnel 0**
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 172.16.12.2/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.2.2.1, destination 10.1.1.1
Tunnel Subblocks:
src-track:

Tunnel0 source tracking subblock associated with Serial0/0/1

Set of tunnels with source Serial0/0/1, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 00:01:28, output 00:01:28, output hang never

Last clearing of "show interface" counters 00:02:50

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

— Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

WEST# **ping 172.16.12.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

— С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

_____ 172.16.12.1 > 172.16.12.2

WEST# **traceroute 172.16.12.2**

Type escape sequence to abort.

Tracing the route to 172.16.12.2

VRF info: (vrf in name/id, vrf out name/id)

1 172.16.12.2 20 msec 20 msec *

— Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

_____ 172.16.12.2 > 172.16.12.1

С какими интерфейсами связаны эти IP-адреса? Почему?

_____

_____

_____

_____

Интерфейсы Tunnel 0 на маршрутизаторах WEST и EAST. Трафик использует туннель.

— Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 7: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

— Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

WEST(config)# **router ospf 1**

WEST(config-router)# **network 172.16.1.0 0.0.0.255 area 0**

WEST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

— Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

EAST(config)# **router ospf 1**

EAST(config-router)# **network 172.16.2.0 0.0.0.255 area 0**

EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

Шаг 2: Проверка маршрутизации OSPF.

— Отправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.1.1.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/1

L 172.16.1.1/32 is directly connected, GigabitEthernet0/1

O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.1/32 is directly connected, Tunnel0

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

_____

_____

Для связи с сетью 172.16.2.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.2.

— Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

_____

_____

Для связи с сетью 172.16.1.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.1.

EAST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.2.2.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.1/32 is directly connected, Serial0/0/1
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O 172.16.1.0/24 [110/1001] via 172.16.12.1, 00:02:44, Tunnel0
C 172.16.2.0/24 is directly connected, GigabitEthernet0/1
L 172.16.2.1/32 is directly connected, GigabitEthernet0/1
C 172.16.12.0/30 is directly connected, Tunnel0
L 172.16.12.2/32 is directly connected, Tunnel0

Шаг 3: Проверьте связь между конечными устройствами.

— Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

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

— Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

_____

_____

172.16.1.1 > 172.16.12.2 (интерфейс туннеля на маршрутизаторе EAST) > 172.16.2.3

Вопросы на закрепление

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?

_____

_____

_____

_____

Протокол IPsec можно настроить таким образом, чтобы обеспечивалось шифрование данных для защищенного туннеля GRE.

2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

_____

_____

Новые сети необходимо добавить к тем же протоколам маршрутизации, что и интерфейс туннеля.

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.

Настройки устройств

Маршрутизатор WEST

```
WEST# show run
Building configuration...

Current configuration : 1798 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname WEST
!
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 Tunnel0
 ip address 172.16.12.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 10.2.2.1
!
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 172.16.1.1 255.255.255.0
 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 172.16.1.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access 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 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end

Маршрутизатор ISP

ISP# show run
Building configuration...

Current configuration : 1406 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!

```
hostname ISP
!
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
!
!
!
!
!
!
!
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 10.1.1.2 255.255.255.252
!
```

```
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 02050D480809
 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 045802150C2E
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Маршрутизатор EAST

```
EAST# show run
Building configuration...

Current configuration : 1802 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname EAST
!
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
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!

```
!
interface Tunnel0
 ip address 172.16.12.2 255.255.255.252
 tunnel source 10.2.2.1
 tunnel destination 10.1.1.1
!
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 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
router ospf 1
 network 172.16.2.0 0.0.0.255 area 0
```

```
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 00071A150754
 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 030752180500
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Настройка базового PPP с аутентификацией (вариант для инструктора)

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология

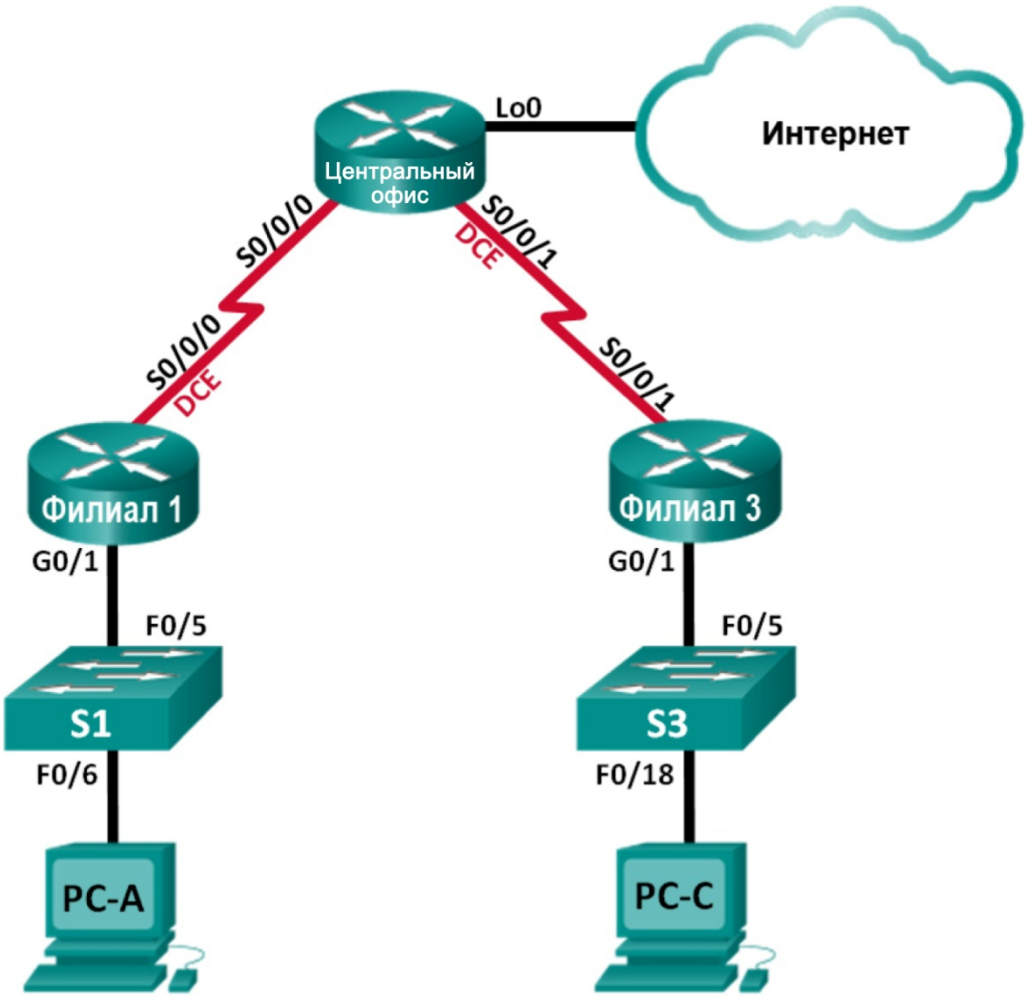


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Филиал 1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
Central	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
Филиал 3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	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

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка инкапсуляции PPP

Часть 3. Настройка аутентификации CHAP PPP

Исходные данные/сценарий

PPP — очень распространенный протокол WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных каналах PPP. Вы также изучите влияние, оказываемое

изменениями инкапсуляции и аутентификации на состояние последовательного канала.

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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 порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 8: Базовая настройка устройств

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

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

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

— Отключите поиск DNS.

— Настройте имя устройства.

— Зашифруйте незашифрованные пароли.

— Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

— Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

— Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

— Настройте ведение журнала состояния консоли на синхронный режим.

— Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

— Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

— На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

— Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса

значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

— На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

— На всех маршрутизаторах выполните команды **show ip route ospf**, **show ip ospf interface brief** и **show ip ospf neighbor**, чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

Филиал 1:

Branch1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:04:10, Serial0/0/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.2.2.0/30 [110/128] via 10.1.1.2, 00:04:20, Serial0/0/0
O 192.168.3.0/24 [110/129] via 10.1.1.2, 00:03:21, Serial0/0/0

Branch1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/0	1	0	10.1.1.1/30	64	P2P	1/1
Gi0/1	1	0	192.168.1.1/24	1	DR	0/0

Branch1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
209.165.200.225	0	FULL/ -	00:00:33	10.1.1.2	Serial0/0/0

Главный:

Central# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

O 192.168.1.0/24 [110/65] via 10.1.1.1, 00:07:43, Serial0/0/0
O 192.168.3.0/24 [110/65] via 10.2.2.1, 00:06:38, Serial0/0/1

Central# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	10.2.2.2/30	64	P2P	1/1
Se0/0/0	1	0	10.1.1.2/30	64	P2P	1/1

Central# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.3.1	0	FULL/ -	00:00:33	10.2.2.1	Serial0/0/1
192.168.1.1	0	FULL/ -	00:00:36	10.1.1.1	Serial0/0/0

Филиал 3:

Branch3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.2.2.2, 00:08:14, Serial0/0/1
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.1.1.0/30 [110/128] via 10.2.2.2, 00:08:14, Serial0/0/1
O 192.168.1.0/24 [110/129] via 10.2.2.2, 00:08:14, Serial0/0/1

Branch3# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	10.2.2.1/30	64	P2P	1/1
Gi0/1	1	0	192.168.3.1/24	1	DR	0/0

Branch3# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
209.165.200.225	0	FULL/ -	00:00:37	10.2.2.2	Serial0/0/1

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Все устройства должны успешно выполнять эхо-запросы ко всем остальным устройствам, указанным в топологии. Если это не так, выполняйте поиск и устранение неполадок то до тех пор, пока не удастся установить сквозное соединение.

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

Шаг 7: Сохраните настройки.

Часть 9: Настройка инкапсуляции PPP

Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.

На маршрутизаторах выполните команду **show interfaces serial** *идентификатор_интерфейса* для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  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)
  Last input 00:00:02, output 00:00:05, 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: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1003 packets input, 78348 bytes, 0 no buffer
     Received 527 broadcasts (0 IP multicasts)
```

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

1090 packets output, 80262 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

2 carrier transitions

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

Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco.

_____ HDLC

Шаг 2: Измените инкапсуляцию на PPP.

— Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1».

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

Branch1(config-if)#

Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Branch1(config-if)#

Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

— Введите команду для отображения состояния канала и протокола канала для интерфейса S0/0/0 маршрутизатора «Филиал 1». Задокументируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

_____

_____

Branch1# **show ip interface brief**

Состояние канала – активен, а протокол канала не функционирует.

Branch1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol
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 10.1.1.1 YES manual up down
Serial0/0/1 unassigned YES unset administratively down down

— Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду **encapsulation ppp** на интерфейсе S0/0/0 для маршрутизатора Central.

Central(config)# **interface s0/0/0**
Central(config-if)# **encapsulation ppp**
Central(config-if)#
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

— Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» находится в активном состоянии и настроен с инкапсуляцией PPP.

Укажите состояние протокола PPP (LCP). _____ Open

Укажите, согласование каких протоколов NCP было выполнено.

_____

_____

Протокол управления протоколом IP (IPCP) и протокол управления протоколом обнаружения устройств Cisco (CDPCP)

Branch1# **show interfaces s0/0/0**
Serial0/0/0 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 10.1.1.1/30

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)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 00:03:58
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
77 packets input, 4636 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
117 packets output, 5800 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets
22 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
18 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

Central# **show interfaces s0/0/0**
Serial0/0/0 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 10.1.1.2/30
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)

Last input 00:00:02, output 00:00:03, output hang never

Last clearing of "show interface" counters 00:01:20

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

41 packets input, 2811 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

40 packets output, 2739 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

Шаг 3: Намеренно разорвите последовательное подключение.

— Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

Branch1# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch1# **debug ppp packet**

PPP packet display debugging is on

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central# **debug ppp packet**

PPP packet display debugging is on

— Наблюдайте за сообщениями команды debug PPP при проходе трафика по последовательному каналу между маршрутизаторами «Филиал 1» и «Главный».

Branch1#

Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#

Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

— Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора «Филиал 1». Запишите команду, использованную для изменения инкапсуляции на HDLC.

_____

_____

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation hdlc**

— Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Филиал 1». Последовательное подключение завершено, и протокол линии связи не функционирует. Маршрут к 10.1.1.2 («Главный») удалён из таблицы маршрутизации.

Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected

Jun 20 02:29:50.295: PPP: NET STOP send to AAA.

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.29

Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN

Branch1(config-if)#

Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

— Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Главный». Маршрутизатор «Главный» продолжает попытки установить подключение к маршрутизатору «Филиал 1», как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, интерфейсы снова прекращают работу. Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством вследствие несоответствия инкапсуляции для последовательного канала.

Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN

Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification

.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message

.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]

.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING

.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction

.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]

.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 02:29:52.296: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]

.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10

.Jun 20 02:29:54.308: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]

.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding

<Данные опущены>

.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10

.Jun 20 02:30:10.436: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate

.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.

.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<Данные опущены>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running

.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING

.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]

.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Что происходит в случае, если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

_____

_____

_____

_____

_____

_____

Канал отключается, и отношения смежности OSPF нарушаются. PPP продолжает попытки установить подключение к другому концу канала, что видно из сообщения «Phase is ESTABLISHING» («Текущий этап — УСТАНОВКА»). Однако, поскольку он продолжает получать пакет, не являющийся пакетом NCP, LCP не удается выполнить согласование, и канал по-прежнему не работает.

— Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1», чтобы исправить несоответствующую инкапсуляцию.

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

— Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Branch1(config-if)#

Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification

Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message

Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]

Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING

Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction

Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line

Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

Jun 20 03:01:59.399: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP: Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
<Данные опущены>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from LOADING to FULL, Loading Done

Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]

— Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Главный» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10

Jun 20 03:01:59.393: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating

Jun 20 03:01:59.393: PPP: NET STOP send to AAA.

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN

.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1

.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1

.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]

.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING

.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction

.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line

<Данные опущены>

.Jun 20 03:01:59.401: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP

.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Address 10.1.1.2 (0x03060A010102)

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]

<Данные опущены>

.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open

.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60

.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]

.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]

Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]

Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open

Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]

Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Основываясь на сообщении команды debug, укажите, через какие этапы проходит PPP, если другой конец последовательного канала на маршрутизаторе Central настроен с инкапсуляцией PPP.

_____

_____

_____

_____

PPP проходит через следующие этапы: DOWN (отключён), ESTABLISHING (установка), и UP (активен).

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

_____

_____

Канал начинает работать, и отношения смежности OSPF восстанавливаются.

— Введите команду **undebug all** (или **u all**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

— После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

_____

_____

Последовательный интерфейс 0/0/0 активен, и протокол активен.

Branch1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Central# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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 10.1.1.2 YES manual up up

Serial0/0/1 10.2.2.2 YES manual up up

Loopback0 209.165.200.225 YES manual up up

— Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» настроен на инкапсуляцию PPP. Ниже запишите команду для проверки инкапсуляции PPP.

_____

_____

_____

_____

Branch1# **show interfaces s0/0/0**

Central# **show interfaces s0/0/0**

— Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами «Главный» и «Филиал 3» измените на инкапсуляцию PPP.

Central(config)# **interface s0/0/1**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **encapsulation ppp**

Branch3(config-if)#

Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done

— Перед переходом к части 3 убедитесь в том, что сквозное соединение восстановлено.

Часть 10: Настройка аутентификации CHAP PPP

Шаг 1: Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

_____

_____

show running-config с модификаторами выходных данных или **show interfaces** *идентификатор_интерфейса*

Шаг 2: Настройте аутентификацию CHAP PPP для канала между маршрутизатором «Главный» и маршрутизатором «Филиал 3».

— Настройте имя пользователя для аутентификации CHAP.

Central(config)# **username Branch3 password cisco**

Branch3(config)# **username Central password cisco**

— Выполните команды **debug ppp** на маршрутизаторе «Филиал 3» для наблюдения за процессом, который связан с аутентификацией.

Branch3# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch3# **debug ppp packet**

PPP packet display debugging is on

— Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **ppp authentication chap**

— Изучите сообщения команды debug PPP на маршрутизаторе «Филиал 3», выдаваемые во время согласования с маршрутизатором «Главный».

Branch3(config-if)#

Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed

Jun 20 04:25:02.079: PPP: NET STOP send to AAA.

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN

.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2

.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]

.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING

.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction

.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]

<Данные опущены>

.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]

.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 04:25:02.091: Se0/0/1 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 04:25:02.091: Se0/0/1 LCP: MagicNumber 0xF7B20F10 (0x0506F7B20F10)

.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open

.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]

.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User

.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User

.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10

<Данные опущены>

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done

.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]

.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит маршрутизатор «Филиал 3», прежде чем будет установлена связь с маршрутизатором «Главный».

_____

_____

_____

_____

PPP проходит через следующие этапы: DOWN (отключён), ESTABLISHING (установка), AUTHENTICATING (подлинность проверяется) и UP (активен).

— Введите команду **debug ppp authentication** для наблюдения за сообщениями аутентификации CHAP на маршрутизаторе Central.

Central# **debug ppp authentication**

PPP authentication debugging is on

— Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе «Главный».

Central(config)# **interface s0/0/1**

Central(config-if)# **ppp authentication chap**

— Наблюдайте за сообщениями команд debug PPP, относящихся к аутентификации CHAP на маршрутизаторе «Главный».

Central(config-if)#

.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction

.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]

.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request

.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA

.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"

.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4

.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

— Введите команду **undebug all** (или **u all**) на маршрутизаторах «Главный» и «Филиал 3» и отключите всю отладку.

Central# **undebug all**

All possible debugging has been turned off

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

— На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1». Назначьте **cisco** в качестве пароля.

Central(config)# **username Branch1 password cisco**

— На маршрутизаторах «Главный» и «Филиал 1» настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

_____

_____

Интерфейс S0/0/0 включается и выключается.

Примечание. Для ускорения процесса выключите интерфейс и снова его включите.

.Jun 20 05:23:55.032: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

Central(config-if)#

.Jun 20 05:23:57.064: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:23:57.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Central(config-if)#

.Jun 20 05:24:03.144: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:24:03.156: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Central(config-if)#

— Для исследования возникшего процесса используйте команду **debug ppp negotiation**.

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central(config-if)#

.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP

.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message

.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]

.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING

.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction

.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15

.Jun 20 05:25:26.229: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 05:25:26.233: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.233: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open

.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer

.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING

.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification

.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN

Объясните, что приводит к окончательному завершению канала.

Запишите ниже команду, выполненную для устранения неполадки.

_____

_____

_____

_____

_____

_____

Канал завершается, поскольку рукопожатие CHAP невозможно без наличия правильного имени пользователя на маршрутизаторе «Филиал 1».

Branch1(config)# **username Central password cisco**

— Введите команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

— Проверьте связь между конечными устройствами.

Вопросы на закрепление

1. Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

   _____

   _____

   К таким признакам относятся следующие: сеть больше не стабилизируется, поскольку некоторые из маршрутов удалены, и протокол канала отключен.

2. Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?

   _____

   _____

   К таким признакам относятся следующие: маршрут удален из таблицы маршрутизации, и протокол канала включается и выключается.

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.

Настройки устройств

Филиал 1

```
Branch1# show run
Building configuration...

Current configuration : 1832 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch1
!
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 Central password 7 1511021F0725
!
!
!
!
!
!
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 10.1.1.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 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
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 094F471A1A0A
 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 121A0C041104
 login
 transport input all
line vty 5 15
 password 7 110A1016141D
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Главный

```
Central#show run
Building configuration...

Current configuration : 1964 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Central
!
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 Branch3 password 7 1511021F0725
username Branch1 password 7 05080F1C2243
!
redundancy
!
!
!
!
!
!
!
!

```
!
!
!
!
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
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 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
```

```
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 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 ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 00071A150754
 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
line vty 5 15
 password 7 14141B180F0B
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Филиал 3

```
Branch3# show run
Building configuration...

Current configuration : 1929 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname Branch3
!
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 Central password 7 0822455D0A16
!
redundancy
!
!
!
!
!
```

```
!
!
!
!
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
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
```

```
 network 192.168.3.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 13061E010803
 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 045802150C2E
```

```
 login
 transport input all
line vty 5 15
 password 7 13061E010803
 login
 transport input all
!
scheduler allocate 20000 1000
!
End
```

Контрольные вопросы:

14)Смоделировать и исследовать PT распределенную сеть на основе протокола PPP.

15)Настроить аутентификацию PPP CHAP.

16)Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.

17)Настроить инкапсуляцию PPP.

18)Перечислить отличия HDLC и PPP.

19)Перечислить поля кадров HDLC и PPP

20)Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.

21)Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

22)Смоделировать и исследовать в PT Visual Studio структуру двухточеченой сети.

23)Сформулировать требования к оборудованию для реализации GRE.

24)Перечислить основные этапы конфигурирования GRE.

25)Синтаксис команд для включения GRE туннеля в Cisco IOS.

26)Реализация защищенного GRE туннеля с использованием IPSec.

27)Настроить статическую маршрутизацию при использовании GRE.

28)Настроить динамическую маршрутизацию при использовании GRE..

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 «Защищенные информационные системы»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем

Ставрополь
2026

Содержание:

Лабораторная работа №1

1. Цель работы

1. Изучить способы исследования методов аутентификации
2. Исследовать способы управления доступом

2. Подготовка к занятию

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

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 руководству

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

1. организационные;
2. технологические;
3. правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;
2. знаний некоторой известной только ему и проверяющей стороне информации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной

оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого
оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (си rect passnrOrd authenti Ceti ОН). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted thi гси рагу authenti сан оп). При этом третью сторону называют сервером аутентификации (authenti Ceti оп server) или арбитром (аГbitretor).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

— по хранимой копии пароля или его свёртке (p1 ai ntext-equi a] еп);
— по некоторому проверочному значению (veri f i er-based) ;
— без непосредственной передачи информации о пароле проверяющей стороне (zero-
knowl edge) ;
— с использованием пароля для получения криптографического ключа (CryptographiC).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение

злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя - совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

— интерфейс пользователя;

— интерфейс администратора;

— модуль сопряжения с другими подсистемами безопасности;

— база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:

— подбор в интерактивном режиме;

— подсматривание;

— преднамеренную передачу пароля его владельцем другому лицу;

— захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);

— перехват переданной по сети информации о пароле;

— хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы через:

— внедрение программных закладок;

— обнаружение и использование ошибок, допущенных на стадии разработки;

— выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

— выбрать пароль, который легко запомнить и также легко подобрать;

— записать пароль, который сложно запомнить, и положить запись в доступном месте;

— ввести пароль так, что его смогут увидеть посторонние:

— передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароляя	Получаемый эффектя
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или
Использование в пароле различных групп	Усложняет задачу злоумышленника при попытке подобрать пароль методом
Проверка и отбраковка пароля по	Усложняет задачу злоумышленника при
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его
Ведение журнала истории паролей	Обеспечивает дополнительную степень

Применение эвристического алгоритма, бракующего пароли на основании	Усложняет задачу злоумышленника при попытке подобрать пароль п о словарю
Ограничение числа попыток ввода	Препятствует интерактивному подбору
Поддержка режима принудительной смены	Обеспечивает эффективность требования,
Использование задержки при вводе	Препятствует интерактивному подбору
Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль п о словарю. Если алгоритм генерации
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент

2. Примеры.

Например 1.

Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.

Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: C=n=1 06

Примем скорость перебора X10 паролей в секунду. Получаем время перебора всех паролей t= C/б10^5секунд~1667минут~28часов~1,2 дня.

Примем, что после каждого из т=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей

T=t*5/3=16667секунд~2778минут~46часов 1,9 дня.

^{T}итог = 1+T = 1,2 + 1,9 = 3,1 ДНЯ

2. Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы n=10.

Длина пароля рассчитывается: k=1 оуп C=1 g C.

Определим количество вариантов C= t * б=10лет* 10 паролей в сек. =

10* 10* 365* 24* 60* 603,15* 10^9 вариантов

Таким образом, получаем длину пароля: k=1 g (3,15* 10^9) = 9,5

Очевидно, что длина пароля должна быть не менее 10 символов.

3. Задания..

1. Определить время перебора всех паролей с параметрами.

Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из т неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	т	v
1	33	10	100	o	o
2	2 6	1 2	1 3	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из П символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	П	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

Контроьные вопросы:

1) Перечислить виды атак на пароли.
2) Перечислить критерии стойкости парольной защиты.
3) Перечислить и охарактеризовать методы противостояния атаке полным перебором.
4) Охарактеризовать влияние длины пароля на вероятность раскрытия.
5) Сформировать рекомендации по составлению паролей.

6) Перечислить типы угроз безопасности парольных систем.

7) Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

8) Определить время перебора всех паролей, состоящих из 6 цифр

Лабораторная работа №2

1. Цель работы:

1. Исследовать сбор и анализ данных NetFlow

2. Подготовка к занятию

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

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

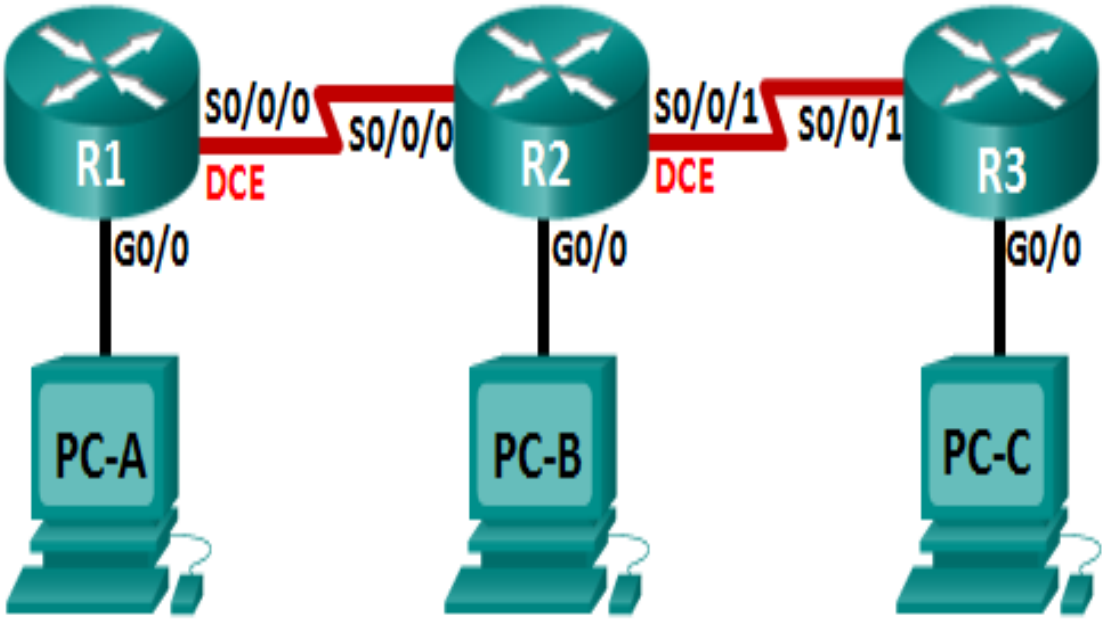
- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

Сбор и анализ данных NetFlow **(вариант для инструктора)**

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология



Программное обеспечение системы сбора данных и анализатора NetFlow

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

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка NetFlow на маршрутизаторе

Часть 3. Анализ NetFlow с помощью интерфейса командной строки

Часть 4. Изучение ПО сбора данных и анализатора NetFlow

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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.

Часть 1: 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 VTY 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.

Часть 2: 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 B. 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

— 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

Часть 3: 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 1: 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 2: 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 ager 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	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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 3: 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 A.

Шаг 4: 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 ager 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
```

Часть 4: 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

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

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.

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.

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 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 192.168.2.1 255.255.255.0
 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
```

Контрольные вопросы:

9) Этапы и средства реализации атак. Классификация атак.

10)Таксономия систем обнаружения атак.

11)Совместное применение систем обнаружения атак и других средств защиты.

12)Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.

13)Анализ журналов регистрации и сетевого трафика.

14)Анализ заголовков, процессов, сервисов и портов.

15)Настроить NetFlow на маршрутизаторе.

16)Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

Лабораторная работа №3

1.Цель работы:

Ознакомиться с приложениями, включенными в состав СУБД MySQL. Получить навыки управления учетными записями пользователей и определения привилегий. Ознакомиться с утилитами, входящими в состав СУБД MySQL, получить навыки работы с ними.

2. Подготовка к занятию

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

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 руководству

Запуск MySQL

Управление сервером обычно осуществляется из командной строки. Запуск в Windows осуществляется через сеанс командной строки выполнением следующей команды:

```
D:\usr\local\Mysql\bin\mysqld --standalone
```

Эта команда запустит демон mysql в фоновом режиме. В Windows 95/98 не предусмотрен запуск mysqld в виде службы. В Windows 2000 демон mysql запускается в виде службы.

Можно осуществить запуск winmysqladmin.exe, в этом случае все настройки перечисляются в файле my.ini

При запуске mysqld можно указывать следующие опции:

Таблица 11- Опции команды MySQLD

`-?, --help`	Справка
`-b, --basedir=[path]`	Путь к каталогу в котором установлен mysql
`-h, --datadir [homedir]`	Путь к каталогу, в котором хранятся базы данных.
`-l, --log=[filename]`	Имя журнала транзакций
`-L, --language=[language]`	Язык по умолчанию(обычно English).
`-P, --port=[port]`	Порт для соединения.
`--skip-grant-tables`	Игнорировать таблицы привилегий. Это дает любому ПОЛНЫЙ доступ ко всем таблицам. Не следует предоставлять обычным пользователям разрешений на запуск mysqld.
`--skip-name-resolve`	Позволяет предоставлять доступ только тем хостам, чьи IP-адреса указаны в таблицах привилегий. Ипользуется для более высокого уровня защиты.
`--skip-networking`	Использовать подключения только через интерфейс localhost.
`-V, --version`	Вывести информацию о версии.

Наличие в статусной строке иконки светофора с активным зеленым цветом указывает на то, что сервер запущен (см. рис 1).

Рисунок 4 - Приложение winmysqladmin запущено

Теперь можно попытаться войти в сервер. В случае, если предполагается управление сервером через консоль, то необходимо использовать команду **mysql**. Изначально существует единственный пользователь, которому предоставляется право входа - **root**, которая не имеет пароля. Первое, что нужно сделать войти под именем **root** и зарегистрировать нового пользователя и установить для него пароль. Команда **mysql** может использовать следующие

опции:

Таблица 12 - Опции команды MySQL

-?, --help	Справка
-h,--hostname=[hostname]	Имя сервера mysql.
-u, --user=[user]	Имя пользователя для доступа к mysql.
-p, --password=[password]	Пароль пользователя для доступа к mysql.
-P, --port=[port]	Порт для соединения с сервером.
-V, --version	Информация о версии

Примечание. Команды mysqld и mysql имеют еще некоторые опции, но в данный момент они особого интереса не представляют.

Запуск из сеанса ДОС осуществляется как показано на Рисунок 2 (в указанном случае осуществляется подключение к БД mysql).

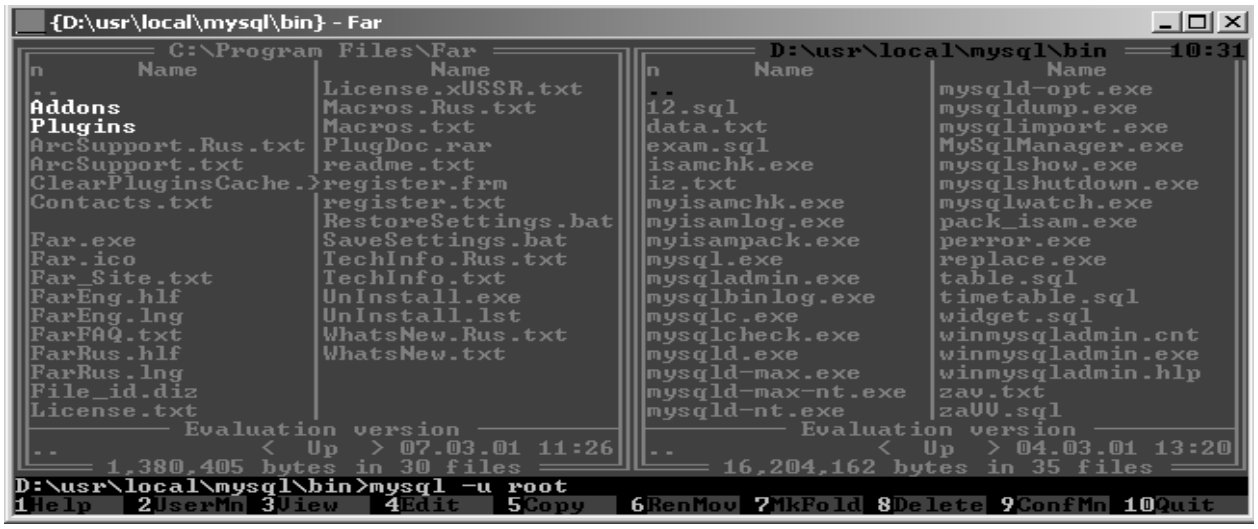


Рисунок 5 - Запуск консоли MYSQL

Для выполнения в строке наберите команду: **mysql –u root**

Рисунок 6 - Успешный запуск консоли

Если вы это получили, значит вы успешно вошли в консоль mysql, которая используется для администрирования сервера.

Для составления отчета вам понадобятся приведение команд, которые вы будете посылать на сервер. В MySQL имеется возможность ведение протокола выполняемых команд, чтобы запустить ведение протокола необходимо выполнить команду

\T filename

!!! обязательно в верхнем регистре. Filename – имя файла, в который будут записываться команды (создается автоматически при выполнении команды, и действует во время жизни сеанса, т.е. в случае отключения от сервера лог прерывается и для возобновления необходимо повторить команду с выводом в новый файл, так как команда затирает имеющиеся в файле данные).

Просмотр списка БД, доступных на сервере осуществляется командой ***SHOW DATABASES.***

Для выполнения в строке наберите команду: **show databases.**

Командой: **USE MYSQL;** – выбираем текущую БД где MYSQL имя БД.

Система привилегий и безопасность в MySQL

— User
— Db
— Host
— Пользовательские привилегии

База данных mysql и таблицы привилегий.

Итак, вы успешно вошли в базу данных mysql, которая используется для администрирования сервера. Что же здесь находится? А находятся здесь 5 таблиц, которые ничем не отличаются от других таблиц баз данных, за исключением того, что эти таблицы используются для предоставления доступа к базам данных и таблицам в них пользователям. Рассмотрим каждую из них. Введите следующую команду, **show tables,** которая покажет таблицы в базе

данных mysql.

Кратко рассмотрим функции каждой из таблиц:

Таблица User

Определяет, разрешено ли пользователю, пытающемуся подключиться к серверу делать это. Содержит имя пользователя, пароль а также привилегии. Если ввести команду show columns from user; то получим следующее:

Таблица 13- Структура таблицы User

Field	Type	Null	Key	Default	Extra
Host	char(60)		PRI		
User	char(16)		PRI		
Password	char(41)				
Select_priv	enum('N','Y')			N	
Insert_priv	enum('N','Y')			N	
Update_priv	enum('N','Y')			N	
Delete_priv	enum('N','Y')			N	
Create_priv	enum('N','Y')			N	
Drop_priv	enum('N','Y')			N	
Reload_priv	enum('N','Y')			N	
Shutdown_priv	enum('N','Y')			N	
Process_priv	enum('N','Y')			N	
File_priv	enum('N','Y')			N	
Grant_priv	enum('N','Y')			N	
References_priv	enum('N','Y')			N	
Index_priv	enum('N','Y')			N	
Alter_priv	enum('N','Y')			N	
Show_db_priv	enum('N','Y')			N	
Super_priv	enum('N','Y')			N	
Create_tmp_table_priv	enum('N','Y')			N	
Lock_tables_priv	enum('N','Y')			N	
Execute_priv	enum('N','Y')			N	
Repl_slave_priv	enum('N','Y')			N	
Repl_client_priv	enum('N','Y')			N	
Create_view_priv	enum('N','Y')			N	

Show_view_priv	enum('N','Y')			N	
Create_routine_priv	enum('N','Y')			N	
Alter_routine_priv	enum('N','Y')			N	
Create_user_priv	enum('N','Y')			N	
Event_priv	enum('N','Y')			N	
Trigger_priv	enum('N','Y')			N	
ssl_type	enum('','ANY','X509','SPECIFIED')				
ssl_cipher	blob			NULL	
x509_issuer	blob			NULL	
x509_subject	blob			NULL	
max_questions	int(11) unsigned			0	
max_updates	int(11) unsigned			0	
max_connections	int(11) unsigned			0	
max_user_connections	int(11) unsigned			0	

Изначально эта таблица содержит пользователя root без пароля. По умолчанию root может входить с любого хоста, имеет все привилегии и доступ ко всем базам данных.Также в таблице содержится запись для пользователя '%'.

В БД MYSQL содержатся таблицы, называемых таблицами привилегий. Система привилегий будет подробно рассмотрена в следующих работах, а пока вы можете выполнить команды на добавления своего пользователя:

Для добавления нового пользователя **your_name**, можно выполнить следующие операторы языка (Insert):

Insert into user (host, user, password, ssl_cipher, x509_issuer, x509_subject)
values ('localhost', 'your_name', password('your_pass'), '', '', '');

Выполнением команды

Select host, user, password from user;

Мы выводим перечисленные поля в виде таблицы

Host	User	Password
%	root	456g879k34df9

Если необходимо выделить все столбцы таблицы, то необходимо набрать * в качестве аргумента команды ***select***.

Чтобы изменения вступили в силу нужно перегрузить сервер, предварительно закончив текущий сеанс работы командой ***quit***.

mysqladmin -u root reload (эта команда перегружает сервер)

После установки пароля для пользователя нужно перезагрузить сервер командой mysqladmin reload, чтобы изменения вступили в силу. После этого можно попробовать войти снова:

Mysql/bin/***mysql -u your_name -p mysql***
Enter password:*******

Если же после этой операции вы не получите приглашение ко входу, то необходимо будет повторить вход в сервер под учетной записью **ROOT** и назначить необходимые права**.** Т.о., недостаточно добавить сведения о пользователе в системную БД, дополнительно необходимо назначить права пользователю, после чего можно начинать настраивать таблицы привилегий, вводить новых пользователей, создавать базы данных и таблицы, то есть делать все то, что называется администрированием. Назначить права можно указанием инструкцией ***INSERT*** для заполнения соответствующие привилегии (перечень привилегий см.

Таблица 3)

Mysql/bin/***mysql -u root***

И выполнить следующий запрос к БД:

Mysql>***USE MYSQL;***

Mysql>***GRANT ALL PRIVILEGES ON *.* TO 'your_name'@'localhost' IDENTIFIED BY 'your_pass' WITH GRANT OPTION;***

Mysql>***FLUSH PRIVILEGES;***

Если пароль был случайно забыт, чтобы его задать по новой, придется стереть файлы mysql.frm mysql.MYI и mysql.MYD из папки с базами данных, затем запустить скрипт mysql_install_db и повторить все по новой. Можно воспользоваться ключом MYSQL и ввести **--skip-grant-tables,** при этом все пароли будут имеет пустое поле.

Команда имеет вид ***mysqld --skip-grant-tables.***

Пояснения:

1.Команда insert вставляет данные в таблицу, не забывайте завершать команды ';'.

2.При вводе пароля используйте функцию password(), иначе пароль работать не будет!

3.Все пароли шифруются mysql, поэтому в поле Password вы видите абракадабры. Это делается в целях безопасности.

4.Не есть хорошей практикой назначать привилегии пользователям в таблице user, так как в этом случае они являются глобальными и распространяются на все базы данных. Предоставляйте привилегии каждому пользователю к конкретной базе данных в таблице db, которая будет рассмотрена далее.

5.При задании имени хоста для входа через сеть рекомендуется явно указывать полное имя хоста, а не '%'. В приведенном выше примере пользователю mary разрешается вход на сервер со всех машин домена tomsk.ru. Можно также указывать IP-адреса машин и маски подсетей для

большей безопасности.

Таблица Db

Определяет к каким базам данных каким пользователям и с каких хостов разрешен доступ. В этой таблице можно предоставлять каждому пользователю доступ к базам данных и назначать привилегии. Если выполнить команду ***show columns from db;*** получим следующее:

Таблица 14 - Структура таблицы Db

Field	Type	Null	Key	Default	Extra
Host	char(60)		PRI		
Db	char(32)		PRI		
User	char(16)		PRI		
Select_priv	char(1)			N	
Insert_priv	char(1)			N	
Update_priv	char(1)			N	
Delete_priv	char(1)			N	
Create_priv	char(1)			N	
Drop_priv	char(1)			N	

— По умолчанию, все привилегии установлены в 'N'. Например, предоставим юзеру mary доступ к базе данных mysql и дадим ему привилегии **select**, **insert** и **update** (описание основных команд mysql будет дано в следующих лабораторных работах, сейчас ваша цель увидеть, как работают таблицы привилегий).

— Для справки:

```
Insert into db (host, user, db, select_priv, insert_priv, update_priv)
Values (''localhost', 'your_name', mysql, 'Y', 'Y', 'Y');
```

— Привилегии, устанавливаемые в таблице db, распространяются только на базу данных library. Если же установить эти привилегии в таблице user, то

они будут распространяться и на другие базы данных, даже если доступ к ним и не установлен явно.

Таблица Host

Таблица host используется для расширения диапазона доступа в таблице db. К примеру, если доступ к какой-либо базе данных должен быть предоставлен более чем одному хосту, тогда следует оставить пустой колонку host в таблице db, и внести в таблицу host необходимые имена хостов. Выполним команду

show columns from host;

Таблица 15 - Структура таблиц Host

Field	Type	Null	Key	Default	Extra
Host	char(60)		PRI		
Db	char(32)		PRI		
Select_priv	char(1)			N	
Insert_priv	char(1)			N	
Update_priv	char(1)			N	
Delete_priv	char(1)			N	
Create_priv	char(1)			N	
Drop_priv	char(1)			N	

Как видно из таблицы, здесь также можно задавать привилегии для доступа к базе данных.Они обычно редко используются без необходимости. Все привилегии доступа нужно задавать в таблице db для каждого пользователя, а в таблице host только перечислить имена хостов.Сервер читает все таблицы, проверяет имя пользователя, пароль, имя хоста, имя базы данных, привилегии.Если в таблице db привилегии select, insert установлены в 'Y', а в таблице host в 'N', то в итоге юзер все равно получит 'Y'.Чтобы не вносить путаницы, лучше назначать привилегии в таблице db.

Эти 3 таблицы являются основными.В новых версиях MySQL, начиная с 3.22 добавлены еще 2 таблицы- tables_priv и columns_priv, которые позволяют задать права доступа к определенной таблице в базе данных и даже к

определенной колонке. Они работают подобно таблице db, только ссылаются на таблицы и колонки. Также, начиная с версии 3.22 можно использовать команду GRANT для предоставления доступа к базам данных, таблицам и колонкам таблиц, что избавляет от необходимости вручную модифицировать таблицы db, tables_priv и columns_priv. Команда GRANT будет подробно рассмотрена в следующих разделах.

Привилегии, предоставляемые MySQL

Таблица 16 - Привилегии пользователя

Привилегия	**Колонка**	**Где используется**
select	Select_priv	таблицы
insert	Insert_priv	таблицы
Update	Update_priv	таблицы
delete	Delete_priv	таблицы
index	Index_priv	таблицы
alter	Alter_priv	таблицы
create	Create_priv	БД, таблицы, индексы
drop	Drop_priv	БД или таблицы
grant	Grant_priv	БД или таблицы
References	References_priv	БД или таблицы
reload	Reload_priv	администрирование сервера
Shutdown	Shutdown_priv	администрирование сервера
Process	Process_priv	администрирование сервера
file	File_priv	доступ к файлам на сервере

Основные утилиты MySQL.

В состав дистрибутива MySQL входят следующие утилиты:

— mysqld
— mysql
— mysqladmin
— mysqlaccess
— mysqlshow
— mysqldump
— isamchk

Утилиты **mysqld** и **mysql** были подробно рассмотрены ранее, поэтому возвращаться к ним не будем. Кратко рассмотрим остальные.

Mysqladmin

Утилита для администрирования сервера. Может использоваться администратором, а также некоторыми пользователями, которым предоставлены определенные привилегии, например – **Reload_priv, Shutdown_priv, Process_priv** и **File_priv**. Данная команда может использоваться для создания баз данных, изменения пароля пользователя(администратор может изменить пароль любому пользователю, а рядовой пользователь – только свой собственный), перезагрузки и остановки сервера, просмотра списка процессов, запущенных на сервере. Mysqladmin поддерживает следующие команды:

Таблица 17 - Опции команды MySQLadmin

Create [database_name]	Создает базу данных
Drop [database_name]	Удаляет базу данных и все таблицы в ней
Reload	Перезагружает сервер
Shutdown	Останавливает работу сервера MySQL
Processlist	Выводит список процессов на сервере
Status	Выводит сообщение о статусе сервера

Пример использования mysqladmin для изменения пароля:

mysqladmin -u your_name password your_pass

Следует заметить, что в случае использования mysqladmin для установки пароля, не требуется использование функции password().Mysqladmin сам заботится о шифровании пароля.

Mysqlaccess

Используется для проверки привилегий пользователя для доступа к конкретной базе данных. Общий синтаксис:

mysqlaccess [host] [user] [db] опции

Полезная утилита для проверки прав доступа пользователя, если он получает сообщение Access denied, при попытке соединиться с базой данных.

Опции:

Таблица 18 - Опции команды MySQLAccess

-?, --help	Справка
-u, --user=[username]	Имя пользователя
-p, --password=[password]	Пароль пользователя
-h, --host=[hostname]	Имя хоста для проверки прав доступа
-d, --db=[dbname]	Имя базы данных для проверки прав доступа
-U, --superuser=[susername]	Имя суперпользователя(root)
-P, --spassword=[spassword]	Пароль администратора
-b, --brief	Выводит краткие сведения о таблице

Mysqlshow

Используется, чтобы показать, с какими базами данных работает сервер, какие таблицы содержит каждая БД и какие колонки есть в каждой таблице.Синтаксис:

mysqlshow [опции] [database [table [field]]]

Mysqlshow может использовать следующие параметры:

Таблица 19 - Параметры команды Mysqlshow

-?, --help	Справка
-h, --host=[hostname]	Имя сервера
-k, --key	Показать ключи для таблицы
-p, --password=[password]	Пароль пользователя
-u, --user=[username]	Имя пользователя
-p, --port=[port]	Порт для связи
-V, --version	Вывести информацию о версии

Если ввести mysqlshow без аргументов, будут показаны все базы данных, если указать имя БД, будут показаны все таблицы в ней.

Команды

mysqlshow

mysqlshow mysql

Mysqldump

Программа mysqldump используется для создания дампа содержания базы данных MySQL. Она пишет инструкции SQL в стандартный вывод. Эти инструкции SQL могут быть переназначены в файл. Можно резервировать базу данных MySQL, используя mysqldump, но при этом Вы должны убедиться, что в этот момент с базой данных не выполняется никаких других действий. А то mysqldump Вам такого нарезервирует...

Программа mysqldump поддерживает следующие параметры (Вы можете использовать короткую или подробную версию):

Таблица 20 - Опции команды MySQLdump

-#, --debug=[options]	**Вывести в протокол отладочную информацию. В общем виде 'd:t:o, filename`.**
-?, --help	Справка.
-c, --compleat-insert	Генерируйте полные инструкции insert (не исключая значений, которые соответствуют значениям столбца по умолчанию).
-h, --host=[hostname]	Соединиться с сервером hostname.
-d, --no-data	Экспорт только схемы информации (исключая данные).
-t, --no-create-info	Экспорт только данных, исключая информацию для создания таблицы. Противоположность -d.
-p, --password=[password]	Пароль пользователя, для соединения с

	сервером MySQL. Обратите внимание, что не должно быть пробела между -p и паролем.
-q, --quick	Не буферизовать результаты запроса, дамп выдать непосредственно к STDOUT.
-u, --user=[username]	Имя пользователя. Если не задано, используется текущий логин.
-v, --verbose	Вывести подробную информацию относительно различных стадий выполнения mysqldump.
-P, --port=[port]	Порт для связи.
-V, --version	Информация о версии.

Вы можете направить вывод mysqldump в клиентскую программу MySQL, чтобы копировать базу данных. ПРИМЕЧАНИЕ: Вы должны убедиться, что база данных не изменяется в это время, иначе Вы получите противоречивую копию!

Для справки:

mysqldump -u root -p mysql user>mysql-1.sql

mysqldump -u root mysql>mysql-2.sql

Примечание флаг –p используется в случае, если пользователь наделен паролем.

После выполнения этой команды у нас появился файл mysql-1.sql и mysql-2.sql. Загрузим их в текстовый редактор, чтобы поподробнее изучить, и, возможно, немного поправить.

Задание

Запустите сервер MySQL. Зарегистрируйте своего пользователя в консольном приложении, задайте ему права.

С помощью утилиты Mysqlshow выполните команду на просмотр структуры и состав таблиц базы Mysql. Приведите в отчете её схему. С помощью утилиты Mysqldump получите полный дамп базы Mysql (данные и таблицы), а также

отдельные дампы таблиц и данных.

Контрольные вопросы:

1. Каким способом возможен запуск серверной части СУБД.
2. Что такое привилегия. Каково её предназначение.
3. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

Лабораторная работа №4

1. Цель работы:

1) Изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера;

2) Практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана «Outpost»;

3) Изучение работы рассматриваемых систем в «совместном» режиме для защиты и тестирования рабочих станций на наличие уязвимостей.

2. Подготовка к занятию

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

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 руководству

1. Теоретические сведения.

Интенсивная информатизация государственных и муниципальных управленческих структур, промышленных предприятий и корпораций, силовых ведомств, научных, медицинских и других учреждений выдвинула на первый план вопросы безопасности информационных ресурсов.

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую. Как правило, через «дыры» в данных сервисах осуществляется большая часть удачных атак извне, которые, зачастую, кончаются потерей компанией секретных данных.

Ярким примером наличия подобных уязвимостей могут послужить популярные операционные системы WindowsXP и FreeBSD. Так, в MS Windows, по-умолчанию, работает довольно много неиспользуемых сервисов, которые в большинстве своем связаны с открытыми портами, через которые злоумышленник может провести атаку. Всем, наверное, известен факт, когда

множество «автономных» пользовательских компьютеров пострадали во всем мире в результате атаки на порт 135 (RPC). Что касается FreeBSD, то здесь также после стандартной установки в системе работают демоны, которые в обычных случаях не требуются, а значит, являются дополнительными источниками уязвимостей в компьютере. Атаки на почтовый сервер sendmail приводят к полному получению злоумышленником контроля над хостом. Откуда sendmail, спросите вы? Да, иногда, в UNIX-системах, в том числе адаптированных для работы в качестве рабочей станции, в конфигурации «по-умолчанию» можно встретить и такие сервисы…

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому, «самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

Тем не менее, при использовании специальных средств защиты, подобных нежелательных событий можно, как правило, избежать.

Основными средствами защиты на сегодняшней день являются две категории специализированных программ:

Межсетевые экраны (брандмауэры, FireWall, МСЭ);

Сканеры (сканеры открытых портов и сервисов).

Следует сказать, что брандмауэр – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

1.1. Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls).

Архитектура firewall

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания

правил. В сущности, создаются два списка: отрицание (deny) и разрешение (permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

— если никакое правило соответствия не найдено, то удалить пакет из сети;
— если соответствующее правило найдено в списке разрешений, то пропустить пакет;
— если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. Отметим преимущества firewall, основанного на фильтрации пакетов:

— фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
— этот метод легко реализуем аппаратно;
— одно-единственное правило может стать ключевым при защите всей сети;
— фильтры не требуют специальной конфигурации компьютера;
— метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

— нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
— нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
— работа ведется с ограниченной информацией пакета;

— в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
— слабо защищен сам компьютер, на котором запущен firewall, то есть предметом атаки может стать сам этот компьютер;
— нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
— возможно, что большой объем правил будет тормозить проверку.

Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

— уникальный идентификатор сессии передачи, который используется для контроля;
— состояние сессии передачи: установлено, передано или закрыто;
— информация о последовательности пакетов;
— адрес источника цепи;
— адрес получателя цепи;
— физический интерфейс, используемый для получения цепи;
— физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи. Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре. Основные преимущества firewall цепного уровня:

— firewall цепного уровня быстрее программного, так как производит меньше проверок;
— firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
— возможно скрытие внутренней топологии сети.

Недостатки firewall цепного уровня:

— нет проверки пакетов на программном уровне;
— слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
— нет проверки передаваемых данных;
— трудно проверить разрешение или отрицание передачи пакетов.

Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется proxy-сервис, который кэширует информацию для более быстрой ее обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через proxy, который является шлюзом. У proxy две части: сервер и клиент. Сервер принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от

имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях. Достоинства proxy:

— понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;
— сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;
— возможен запрет доступа к некоторым сетевым сервисам;
— есть возможность управления пакетами данных;
— есть сокрытие внутренних адресов и топологии сети, так как proxy является фильтром;
— остается видимость прямого соединения сетей;
— proxy может перенаправлять запросы сетевых сервисов на другие компьютеры;
— есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
— возможно создание подробных отчетных записей для администратора.

Недостатки proxy:

— требует изменения сетевого стека на машине, где стоит firewall;
— нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как proxy перехватывает работу портов;
— неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно proxy;
— так как proxy должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой proxy;
— нет proxy для UDPи RPC;
— иногда необходима специальная настройка клиента для работы с proxy;
— proxy не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;

— корректность работы proxy напрямую связана с правильностью обработки сетевого стека;
— использование proxy может требовать дополнительных паролей, что неудобно для пользователей.

Динамическая фильтрация пакетов (dynamic packet filter firewalls)

В основном этот уровень повторяет предыдущий, за двумя важными исключениями:

— возможно изменение правил обработки пакетов «на лету»;
— включена поддержка UDP.

Уровень kernel proxy

Уровень kernel proxy возник достаточно недавно. Основная его идея — попытка поместить описанный выше алгоритм firewall программного уровня в ядро операционной системы, что избавляет компьютер от лишних затрат времени на передачу данных между ядром и программой proxy. Это повышает производительность и позволяет производить более полную проверку проходящей информации.

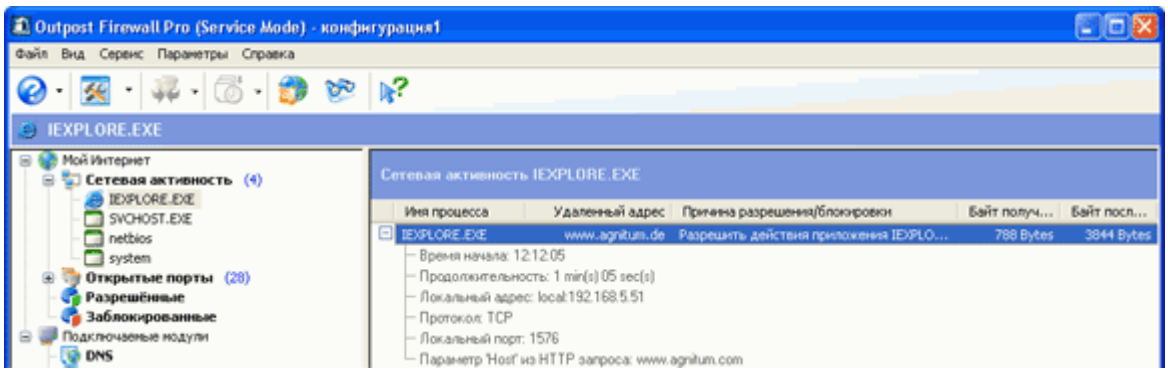
Примеры межсетевых экранов

1. Аппаратный (D-Link)

DFL-1100

Межсетевой экран для сетей крупных предприятий

2. Программный (Agnitum Outpost)



1.2. Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

Архитектура сканера

Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с

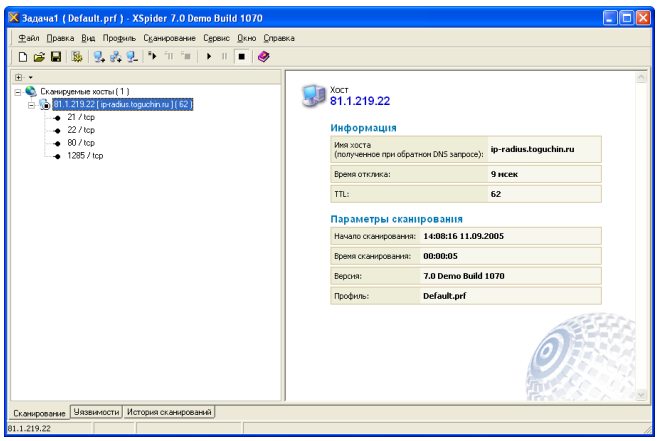
начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

— Идентификацию доступных сетевых ресурсов;
— Идентификацию доступных сетевых сервисов;
— Идентификацию имеющихся уязвимостей сетевых сервисов;
— Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы. Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 10000.

Пример сканера XSpider



2. Порядок выполнения работы.

Условия выполнения лабораторной работы. Данная работа должна выполняться в присутствии администратора компьютерного класса или уполномоченного им лица, которому предоставляются права на осуществление следующих действий в операционных системах Windows2000 – XP, работающих как в сетевом режиме, так и в одиночном режиме:

1.1. права на установку программного обеспечения;

1.2. права на работу как в составе рабочей группы или домена Windows, так и в составе локального администратора рабочей станции;

1.3. права на предоставление учетной записи учащимся, позволяющей установку ПО.

Лабораторная работа проводится в двух вариантах:

1. Автономный.

В компьютерном классе должны находиться не менее 2-х машин, объединенных в сеть. На первой устанавливается *сетевой сканер* или *межсетевой экран*. В случае установки МСЭ вторая машина используется для тестирования защиты первой от ICMP пакетов с помощью стандартной утилиты *ping*. При «автономном» тестировании сканера вторая машина будет использоваться в качестве исследуемого объекта.

2. Совместный.

В компьютерном классе должны находиться также не менее 2-х машин, объединенных в сеть. На части из них устанавливается *сканер*, на остальных – МСЭ. При этом для проверки защиты рабочей станции от ICMP пакетов с помощью МСЭ (а также для тестирования сканера) будет использоваться сетевой сканер.

Администратор! Обрати внимание. После установки изучаемого ПО межсетевые экраны могут заблокировать доступ сетевого трафика к рабочим станциям, тем самым, нарушив работоспособность сети. Для предотвращения данной ситуации необходимо сразу назначить всем МСЭ политику «разрешения».

Порядок работы

Работа будет проходить в два этапа. Первый этап предназначен для изучения работы XSpider, Outpost и WindowsXP в «автономном» режиме. Второй этап – для изучения работы в совместном режиме. На каждом этапе студенты делятся на две группы, одна из которых будет работать с МСЭ, вторая – со сканером или псевдосканером (утилитой ping).

Действия, общие для двух этапов:

1. Взять из папки \\m00\fit2005 файлы установки сканера XSpider и МСЭ Agnitum Outpost;
2. На каждом рабочем месте выполнить установку сканера и МСЭ;
3. При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
4. Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;

5. Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» -> «Выполнить» -> “cmd” -> “ipconfig /all”;

Этап 1. Автономный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)
2. Смотреть на ответные пинг-пакеты.
3. Фиксировать моменты, когда ответные пакеты пропадают и появляются.
4. Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить состояние ответов на ping-запросы у напарника;
4. Повторить п.1-2 несколько раз.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

Этап 2. Совместный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить утилиту сканирования сети XSpider;
2. В меню «Правка» выбрать «Добавить хост»;
3. Введите IP-адрес хоста напарника;

4. Узнать у напарника текущий режим работы МСЭ;
5. В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» -> «Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

6. Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить, как работает XSpider у напарника;
4. Повторить п.1-2 несколько раз для двух режимов XSpider – требующего ICMP-ответа и не требующего.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

По завершению лабораторной работы установленное в процессе занятия ПО необходимо удалить из системы.

3. Отчет

После окончания практической части лабораторной работы студенты должны предоставить письменный отчет, содержащий информацию о проделанной работе и ответы на вопросы в следующем формате:

1. Ф.И.О.
2. Ф.И.О. Напарника
3. Имя и адрес рабочего компьютера.
4. Имя и адрес исследуемого компьютера.
5. Опишите утилиту ping, методы и случаи ее применения.
6. Описать данные, полученные о компьютере напарника с помощью XSpider
7. Какого типа уязвимости были найдены?
8. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
9. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия? (доп +)
10. Выводы.

Контрольные вопросы :

17)Опишите утилиту ping, методы и случаи ее применения.

18)Описать данные, полученные о компьютере с помощью XSpider

19)Опишите типы уязвимостей компьютерных систем

20)Как можно предотвратить появление таких уязвимостей с помощью изученных средств?

21)Описать известные типы МСЭ и отличия между ними.

Лабораторная работа №5

1. Цель работы:

1. Исследовать настройки туннеля VPN GRE по схеме «точка-точка»

2. Подготовка к занятию

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

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 руководству

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология

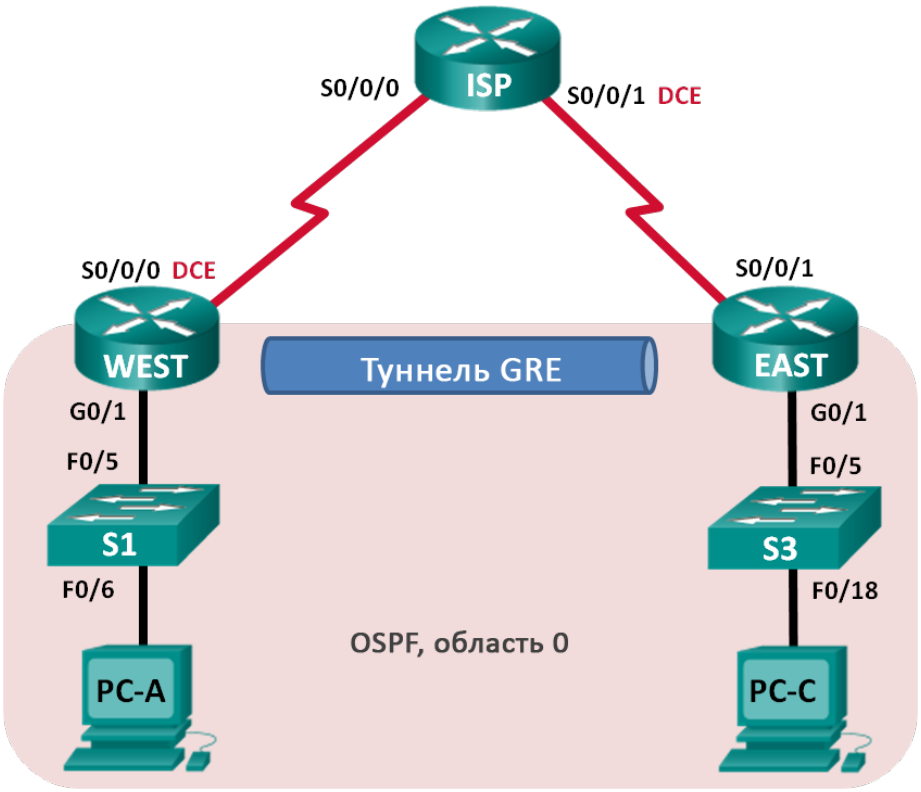


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4
- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка-точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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 порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 5: Базовая настройка устройств

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

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

- Отключите поиск DNS.
- Назначьте имена устройств.
- Зашифруйте незашифрованные пароли.
- Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

— Настройте ведение журнала состояния консоли на синхронный режим.

— Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

— Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

EAST(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхо-запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 6: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

— Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

WEST(config)# **interface tunnel 0**

WEST(config-if)# **ip address 172.16.12.1 255.255.255.252**

WEST(config-if)# **tunnel source s0/0/0**

WEST(config-if)# **tunnel destination 10.2.2.1**

— Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

EAST(config)# **interface tunnel 0**

EAST(config-if)# **ip address 172.16.12.2 255.255.255.252**

EAST(config-if)# **tunnel source 10.2.2.1**

EAST(config-if)# **tunnel destination 10.1.1.1**

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

— Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

WEST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.1.1 YES manual up up

Serial0/0/0 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Tunnel0 172.16.12.1 YES manual up up

EAST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.2.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.2.2.1 YES manual up up

Tunnel0 172.16.12.2 YES manual up up

— С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

_____

_____

_____

_____

Используется протокол туннелирования GRE. Для маршрутизатора WEST источник туннеля — 10.1.1.1 (Serial0/0/0), а назначение — 10.2.2.1. Для маршрутизатора EAST источник туннеля — 10.2.2.1, а назначение — 10.1.1.1.

WEST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.1/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/0

Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 00:00:12, output 00:00:12, output hang never

Last clearing of "show interface" counters 00:01:29

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

EAST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.2/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.2.2.1, destination 10.1.1.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/1

Set of tunnels with source Serial0/0/1, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 00:01:28, output 00:01:28, output hang never

Last clearing of "show interface" counters 00:02:50

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

— Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

WEST# **ping 172.16.12.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

— С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

_____ 172.16.12.1 > 172.16.12.2

WEST# **traceroute 172.16.12.2**

Type escape sequence to abort.

Tracing the route to 172.16.12.2

VRF info: (vrf in name/id, vrf out name/id)

1 172.16.12.2 20 msec 20 msec *

— Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

_____ 172.16.12.2 > 172.16.12.1

С какими интерфейсами связаны эти IP-адреса? Почему?

_____

_____

Интерфейсы Tunnel 0 на маршрутизаторах WEST и EAST. Трафик использует туннель.

— Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 7: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

— Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

WEST(config)# **router ospf 1**

WEST(config-router)# **network 172.16.1.0 0.0.0.255 area 0**

WEST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

— Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

EAST(config)# **router ospf 1**

EAST(config-router)# **network 172.16.2.0 0.0.0.255 area 0**

EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

Шаг 2: Проверка маршрутизации OSPF.

— Отправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.1.1.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/1
L 172.16.1.1/32 is directly connected, GigabitEthernet0/1
O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C 172.16.12.0/30 is directly connected, Tunnel0
L 172.16.12.1/32 is directly connected, Tunnel0

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

_____

_____

Для связи с сетью 172.16.2.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.2.

— Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

_____

_____

Для связи с сетью 172.16.1.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.1.

EAST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.2.2.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.1/32 is directly connected, Serial0/0/1
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O 172.16.1.0/24 [110/1001] via 172.16.12.1, 00:02:44, Tunnel0
C 172.16.2.0/24 is directly connected, GigabitEthernet0/1
L 172.16.2.1/32 is directly connected, GigabitEthernet0/1

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.2/32 is directly connected, Tunnel0

Шаг 3: Проверьте связь между конечными устройствами.

— Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

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

— Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

_____

_____

172.16.1.1 > 172.16.12.2 (интерфейс туннеля на маршрутизаторе EAST) > 172.16.2.3

Вопросы на закрепление

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?

_____

_____

_____

_____

Протокол IPsec можно настроить таким образом, чтобы обеспечивалось шифрование данных для защищенного туннеля GRE.

2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

_____

_____

Новые сети необходимо добавить к тем же протоколам маршрутизации, что и интерфейс туннеля.

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.

Настройки устройств

Маршрутизатор WEST

```
WEST# show run
Building configuration...

Current configuration : 1798 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname WEST
!
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 Tunnel0
 ip address 172.16.12.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 10.2.2.1
!
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 172.16.1.1 255.255.255.0
 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 172.16.1.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
!
!
control-plane
!
!
banner motd ^C
```

```
Unauthorized Access 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 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Маршрутизатор ISP

```
ISP# show run
Building configuration...

Current configuration : 1406 bytes
!
version 15.2
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
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
!
!
!
!
```

```
!
!
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 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 02050D480809
 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 045802150C2E
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Маршрутизатор EAST

```
EAST# show run
Building configuration...

Current configuration : 1802 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname EAST
!
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
!
!
!
!
!
redundancy
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 ip address 172.16.12.2 255.255.255.252
 tunnel source 10.2.2.1
 tunnel destination 10.1.1.1
!
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 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
router ospf 1
 network 172.16.2.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
```

```
 password 7 00071A150754
 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 030752180500
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Контрольные вопросы:

22)Смоделировать и исследовать в PT Visual Studio структуру двухточеченой сети.

23)Сформулировать требования к оборудованию для реализации GRE.

24)Перечислить основные этапы конфигурирования GRE.

25)Синтаксис команд для включения GRE туннеля в Cisco IOS.

26)Реализация защищенного GRE туннеля с использованием IPSec.

27)Настроить статическую маршрутизацию при использовании GRE.

28)Настроить динамическую маршрутизацию при использовании GRE.

1. Исследовать принципы настройки базового PPP с аунтификацией.

Лабораторная работа №6

1. Цель работы:

1. Исследовать принципы настройки базового PPP с аунтификацией.

2. Подготовка к занятию

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

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 руководству

Настройка базового PPP с аутентификацией **(вариант для инструктора)**

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология

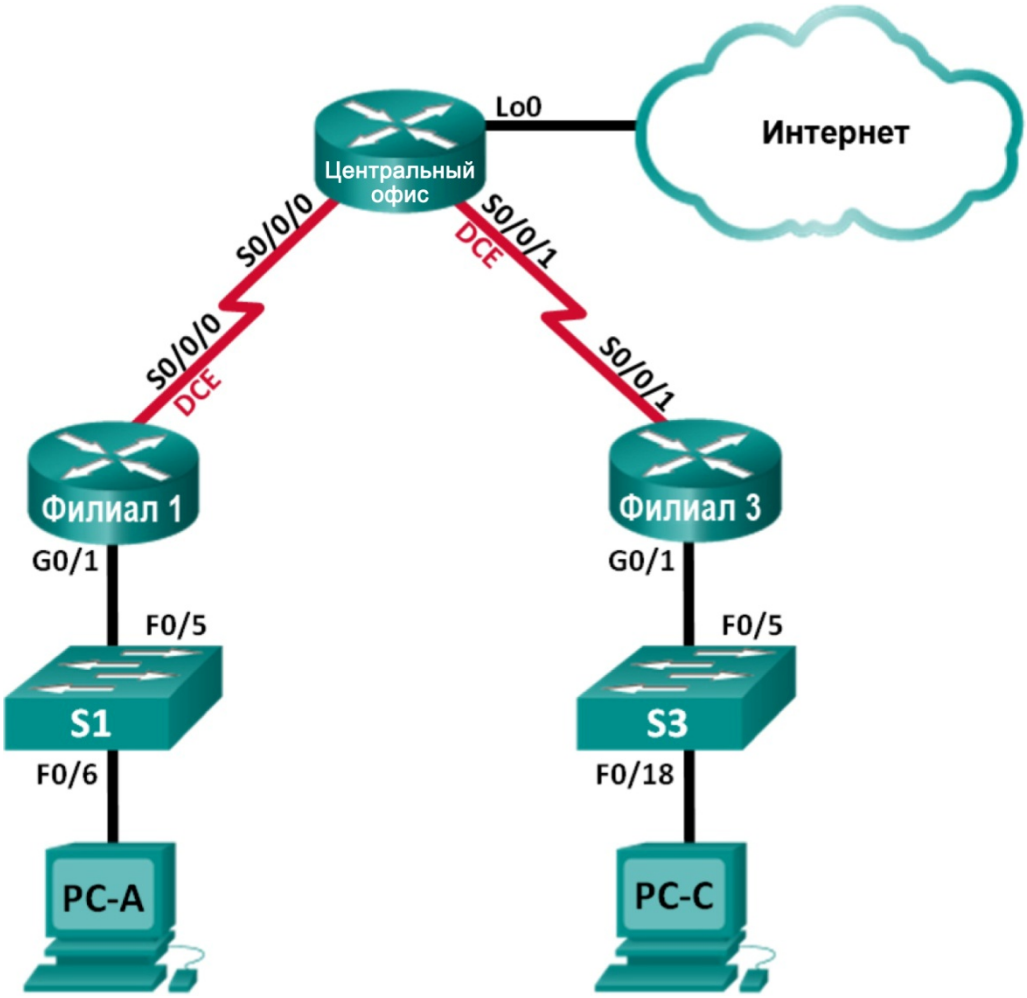


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Филиал 1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
Central	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
Филиал 3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	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

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка инкапсуляции PPP

Часть 3. Настройка аутентификации CHAP PPP

Исходные данные/сценарий

PPP — очень распространенный протокол WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных

каналах PPP. Вы также изучите влияние, оказываемое изменениями инкапсуляции и аутентификации на состояние последовательного канала.

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.

Примечание для инструктора. Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

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 порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 8: Базовая настройка устройств

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

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

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

— Отключите поиск DNS.

— Настройте имя устройства.

— Зашифруйте незашифрованные пароли.

— Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

— Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

— Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

— Настройте ведение журнала состояния консоли на синхронный режим.

— Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

— Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

— На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

— Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

— На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

— На всех маршрутизаторах выполните команды **show ip route ospf**, **show ip ospf interface brief** и **show ip ospf neighbor**, чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

Филиал 1:

Branch1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:04:10, Serial0/0/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.2.2.0/30 [110/128] via 10.1.1.2, 00:04:20, Serial0/0/0
O 192.168.3.0/24 [110/129] via 10.1.1.2, 00:03:21, Serial0/0/0

Branch1# **show ip ospf interface brief**

```
Interface    PID   Area          IP Address/Mask    Cost  State Nbrs F/C
Se0/0/0      1     0             10.1.1.1/30        64    P2P   1/1
Gi0/1        1     0             192.168.1.1/24     1     DR    0/0
```

Branch1# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
209.165.200.225   0   FULL/  -        00:00:33    10.1.1.2        Serial0/0/0
```

Главный:

Central# **show ip route ospf**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

O     192.168.1.0/24 [110/65] via 10.1.1.1, 00:07:43, Serial0/0/0
O     192.168.3.0/24 [110/65] via 10.2.2.1, 00:06:38, Serial0/0/1
```

Central# **show ip ospf interface brief**

```
Interface    PID   Area          IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0             10.2.2.2/30        64    P2P   1/1
Se0/0/0      1     0             10.1.1.2/30        64    P2P   1/1
```

Central# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       0   FULL/  -        00:00:33    10.2.2.1        Serial0/0/1
192.168.1.1       0   FULL/  -        00:00:36    10.1.1.1        Serial0/0/0
```

Филиал 3:

Branch3# **show ip route ospf**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.2.2.2, 00:08:14, Serial0/0/1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/128] via 10.2.2.2, 00:08:14, Serial0/0/1
O     192.168.1.0/24 [110/129] via 10.2.2.2, 00:08:14, Serial0/0/1
```

Branch3# **show ip ospf interface brief**

```
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               10.2.2.1/30        64    P2P   1/1
Gi0/1        1     0               192.168.3.1/24     1     DR    0/0
```

Branch3# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
```

209.165.200.225 0 FULL/ - 00:00:37 10.2.2.2 Serial0/0/1

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Все устройства должны успешно выполнять эхо-запросы ко всем остальным устройствам, указанным в топологии. Если это не так, выполняйте поиск и устранение неполадок то до тех пор, пока не удастся установить сквозное соединение.

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

Шаг 7: Сохраните настройки.

Часть 9: Настройка инкапсуляции PPP

Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.

На маршрутизаторах выполните команду **show interfaces serial** *идентификатор_интерфейса* для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  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)
  Last input 00:00:02, output 00:00:05, 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: fifo
```

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

1003 packets input, 78348 bytes, 0 no buffer

Received 527 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

1090 packets output, 80262 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

2 carrier transitions

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

Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco.

_____ HDLC

Шаг 2: Измените инкапсуляцию на PPP.

— Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1».

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

Branch1(config-if)#

Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Branch1(config-if)#

Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

— Введите команду для отображения состояния канала и протокола канала для интерфейса S0/0/0 маршрутизатора «Филиал 1». Задокументируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

_____

_____

Branch1# **show ip interface brief**

Состояние канала – активен, а протокол канала не функционирует.

Branch1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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 10.1.1.1 YES manual up down

Serial0/0/1 unassigned YES unset administratively down down

— Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду **encapsulation ppp** на интерфейсе S0/0/0 для маршрутизатора Central.

Central(config)# **interface s0/0/0**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

— Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» находится в активном состоянии и настроен с инкапсуляцией PPP.

Укажите состояние протокола PPP (LCP). _____ Open

Укажите, согласование каких протоколов NCP было выполнено.

_____

_____

Протокол управления протоколом IP (IPCP) и протокол управления протоколом обнаружения устройств Cisco (CDPCP)

Branch1# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

  Hardware is WIC MBRD Serial

  Internet address is 10.1.1.1/30

  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)

  Last input 00:00:00, output 00:00:00, output hang never

  Last clearing of "show interface" counters 00:03:58

  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

  Queueing strategy: fifo

  Output queue: 0/40 (size/max)

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

    77 packets input, 4636 bytes, 0 no buffer

    Received 0 broadcasts (0 IP multicasts)

    0 runts, 0 giants, 0 throttles

    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

    117 packets output, 5800 bytes, 0 underruns

    0 output errors, 0 collisions, 8 interface resets

    22 unknown protocol drops

    0 output buffer failures, 0 output buffers swapped out

    18 carrier transitions

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

Central# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 10.1.1.2/30

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)

Last input 00:00:02, output 00:00:03, output hang never

Last clearing of "show interface" counters 00:01:20

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

41 packets input, 2811 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

40 packets output, 2739 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

Шаг 3: Намеренно разорвите последовательное подключение.

— Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

Branch1# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch1# **debug ppp packet**

PPP packet display debugging is on

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central# **debug ppp packet**

PPP packet display debugging is on

— Наблюдайте за сообщениями команды debug PPP при проходе трафика по последовательному каналу между маршрутизаторами «Филиал 1» и «Главный».

Branch1#

Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#

Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

— Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора «Филиал 1». Запишите команду, использованную для изменения инкапсуляции на HDLC.

_____

_____

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation hdlc**

— Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Филиал 1». Последовательное подключение завершено, и протокол линии связи не функционирует. Маршрут к 10.1.1.2 («Главный») удалён из таблицы маршрутизации.

Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected

Jun 20 02:29:50.295: PPP: NET STOP send to AAA.

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.29

Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN

Branch1(config-if)#

Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

— Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Главный». Маршрутизатор «Главный» продолжает попытки установить подключение к маршрутизатору «Филиал 1», как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, интерфейсы снова прекращают работу. Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством вследствие несоответствия инкапсуляции для последовательного канала.

Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification

Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message

Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected

Jun 20 02:29:50.296: PPP: NET STOP send to AAA.

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1

Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1

Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN

Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification

.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message

.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]

.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING

.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction

.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]

.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 02:29:52.296: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]

.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10

.Jun 20 02:29:54.308: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]

.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding

<Данные опущены>

.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10

.Jun 20 02:30:10.436: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate

.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.

.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]

.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]

.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING

.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]

.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 02:30:14.452: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)

.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]

.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding

<Данные опущены>

.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10

.Jun 20 02:30:32.580: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)

.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate

.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.

.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]

.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]

.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running

.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING

.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]

.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Что происходит в случае, если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

_____

_____

_____

_____

_____

_____

Канал отключается, и отношения смежности OSPF нарушаются. PPP продолжает попытки установить подключение к другому концу канала, что видно из сообщения «Phase is ESTABLISHING» («Текущий этап — УСТАНОВКА»). Однако, поскольку он продолжает получать пакет, не

являющийся пакетом NCP, LCP не удается выполнить согласование, и канал по-прежнему не работает.

— Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1», чтобы исправить несоответствующую инкапсуляцию.

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

— Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Branch1(config-if)#

Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification

Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message

Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]

Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING

Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction

Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line

Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

Jun 20 03:01:59.399: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP: Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]

<Данные опущены>

Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.2

Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2

Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from LOADING to FULL, Loading Done

Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]

— Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Главный» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10

Jun 20 03:01:59.393: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating

Jun 20 03:01:59.393: PPP: NET STOP send to AAA.

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated
.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1
.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<Данные опущены>
.Jun 20 03:01:59.401: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP

.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Address 10.1.1.2 (0x03060A010102)

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]

<Данные опущены>

.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open

.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Основываясь на сообщении команды debug, укажите, через какие этапы проходит PPP, если другой конец последовательного канала на маршрутизаторе Central настроен с инкапсуляцией PPP.

_____

_____

_____

_____

PPP проходит через следующие этапы: DOWN (отключён), ESTABLISHING (установка), и UP (активен).

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

_____

_____

Канал начинает работать, и отношения смежности OSPF восстанавливаются.

— Введите команду **undebug all** (или **u all**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

— После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

_____

_____

Последовательный интерфейс 0/0/0 активен, и протокол активен.

Branch1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Central# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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 10.1.1.2 YES manual up up

Serial0/0/1 10.2.2.2 YES manual up up

Loopback0 209.165.200.225 YES manual up up

— Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» настроен на инкапсуляцию PPP. Ниже запишите команду для проверки инкапсуляции PPP.

_____

_____

_____

_____

Branch1# **show interfaces s0/0/0**

Central# **show interfaces s0/0/0**

— Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами «Главный» и «Филиал 3» измените на инкапсуляцию PPP.

Central(config)# **interface s0/0/1**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **encapsulation ppp**

Branch3(config-if)#

Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done

— Перед переходом к части 3 убедитесь в том, что сквозное соединение восстановлено.

Часть 10: Настройка аутентификации CHAP PPP

Шаг 1: Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

_____

_____

show running-config с модификаторами выходных данных или **show interfaces** *идентификатор_интерфейса*

Шаг 2: Настройте аутентификацию CHAP PPP для канала между маршрутизатором «Главный» и маршрутизатором «Филиал 3».

— Настройте имя пользователя для аутентификации CHAP.

Central(config)# **username Branch3 password cisco**

Branch3(config)# **username Central password cisco**

— Выполните команды **debug ppp** на маршрутизаторе «Филиал 3» для наблюдения за процессом, который связан с аутентификацией.

Branch3# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch3# **debug ppp packet**

PPP packet display debugging is on

— Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **ppp authentication chap**

— Изучите сообщения команды debug PPP на маршрутизаторе «Филиал 3», выдаваемые во время согласования с маршрутизатором «Главный».

Branch3(config-if)#

Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed

Jun 20 04:25:02.079: PPP: NET STOP send to AAA.

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN

.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2

.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]

.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING

.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction

.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]

<Данные опущены>

.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]

.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 04:25:02.091: Se0/0/1 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 04:25:02.091: Se0/0/1 LCP: MagicNumber 0xF7B20F10 (0x0506F7B20F10)

.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open

.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]

.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User

.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User

.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10

<Данные опущены>

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done

.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]

.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит маршрутизатор «Филиал 3», прежде чем будет установлена связь с маршрутизатором «Главный».

_____

_____

_____

_____

PPP проходит через следующие этапы: DOWN (отключён), ESTABLISHING (установка), AUTHENTICATING (подлинность проверяется) и UP (активен).

— Введите команду **debug ppp authentication** для наблюдения за сообщениями аутентификации CHAP на маршрутизаторе Central.

Central# **debug ppp authentication**

PPP authentication debugging is on

— Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе «Главный».

Central(config)# **interface s0/0/1**

Central(config-if)# **ppp authentication chap**

— Наблюдайте за сообщениями команд debug PPP, относящихся к аутентификации CHAP на маршрутизаторе «Главный».

Central(config-if)#

.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction

.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]

.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request

.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA

.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"

.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4

.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

— Введите команду **undebug all** (или **u all**) на маршрутизаторах «Главный» и «Филиал 3» и отключите всю отладку.

Central# **undebug all**

All possible debugging has been turned off

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

— На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1». Назначьте **cisco** в качестве пароля.

Central(config)# **username Branch1 password cisco**

— На маршрутизаторах «Главный» и «Филиал 1» настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

_____

_____

Интерфейс S0/0/0 включается и выключается.

Примечание. Для ускорения процесса выключите интерфейс и снова его включите.

.Jun 20 05:23:55.032: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

Central(config-if)#

.Jun 20 05:23:57.064: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:23:57.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Central(config-if)#

.Jun 20 05:24:03.144: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:24:03.156: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Central(config-if)#

— Для исследования возникшего процесса используйте команду **debug ppp negotiation**.

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central(config-if)#

.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP

.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message

.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]

.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING

.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction

.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15

.Jun 20 05:25:26.229: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 05:25:26.233: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.233: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open

.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer

.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING

.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification

.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN

Объясните, что приводит к окончательному завершению канала.

Запишите ниже команду, выполненную для устранения неполадки.

_____

_____

_____

_____

_____

_____

Канал завершается, поскольку рукопожатие CHAP невозможно без наличия правильного имени пользователя на маршрутизаторе «Филиал 1».

Branch1(config)# **username Central password cisco**

— Введите команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

— Проверьте связь между конечными устройствами.

Вопросы на закрепление

1. Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

   _____

   _____

   К таким признакам относятся следующие: сеть больше не стабилизируется, поскольку некоторые из маршрутов удалены, и протокол канала отключен.

2. Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?

   _____

   _____

   К таким признакам относятся следующие: маршрут удален из таблицы маршрутизации, и протокол канала включается и выключается.

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.

Настройки устройств

Филиал 1

```
Branch1# show run
Building configuration...

Current configuration : 1832 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch1
!
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 Central password 7 1511021F0725
!
!
!
!
!
!
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 10.1.1.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
```

```
 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
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 094F471A1A0A
 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 121A0C041104
 login
 transport input all
line vty 5 15
 password 7 110A1016141D
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Главный

```
Central#show run
Building configuration...

Current configuration : 1964 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Central
```

```
!
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 Branch3 password 7 1511021F0725
username Branch1 password 7 05080F1C2243
!
redundancy
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
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 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 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 ^C
  Unauthorized Access Prohibited.^C
!
line con 0
 password 7 00071A150754
 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
line vty 5 15
 password 7 14141B180F0B
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Филиал 3

```
Branch3# show run
```

```
Building configuration...


Current configuration : 1929 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch3
!
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 Central password 7 0822455D0A16
!
redundancy
!
!
!
!
!
!
!
!
!
!
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
```

```
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 13061E010803
```

```
 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 045802150C2E
 login
 transport input all
line vty 5 15
 password 7 13061E010803
 login
 transport input all
!
scheduler allocate 20000 1000
!
End
```

Контрольные вопросы:

1) Смоделировать и исследовать PT распределенную сеть на основе протокола PPP.
2) Настроить аутентификацию PPP CHAP.
3) Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.

4) Настроить инкапсуляцию PPP.

5) Перечислить отличия HDLC и PPP.

6) Перечислить поля кадров HDLC и PPP

7) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.

8) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

Лабораторная работа №7

1. Цель работы:

Изучить мероприятия по созданию, распределению и хранению ключей при использовании пакета КРИПТОН® Подпись для организации электронного документооборота. Получить представление о задачах, возлагаемых на администратора и пользователей системы электронных документов.

2. Подготовка к занятию

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

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

руководству

1.Порядок работы

Последовательно, в течение отведенного расписанием занятий времени, отработать следующие вопросы:

– изучить теоретический материал;

– оформить конспект к работе, получить допуск к выполнению работы;

– выполнить упражнения из практической части работы;

– оформить отчет по лабораторной работе и защитить его.

2.Теоретическое введение

Организация IETF разработала протокол для обеспечения безопасности в Internet, известный под названием IPSec. Протокол IPSec предназначен для криптографической защиты заголовка IP-пакета или всего IP-пакета. Этот протокол предусматривает обязательную аутентификацию IP-заголовка и возможную защиту информации об отправителе и адресате, содержащейся в некоторых полях IP-заголовка.

Поскольку данный протокол обеспечивает защиту информации на сетевом уровне, эта защита невидима для работающих приложений, т.е. он легко развертывается в существующих сетях.

Все протоколы, представленные в IPSec, можно разделить на протоколы непосредственно производящие обработку передаваемых данных (для обеспечения их защиты) и протоколы, которые позволяют автоматически согласовать параметры секретных соединений (далее –согласование), необходимые протоколам первой группы. Ядро IPSec составляют три протокола: протокол аутентификации (Authentication Header, AH), протокол шифрования (Encapsulating Security Payload, ESP) и протокол обмена ключами (Internet Key Exchange, IKE). Функции по поддержанию защищенного канала распределяются между этими протоколами следующим образом:

– протокол AH гарантирует целостность и аутентичность данных;

– протокол ESP шифрует передаваемые данные, гарантируя конфиденциальность, но он может также поддерживать аутентификацию и целостность данных;

– протокол IKE решает вспомогательную задачу автоматического предоставления конечным точкам канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

IPSec обеспечивает проверку подлинности на уровне компьютера и шифрование данных для VPN-подключений, использующих протокол L2TP. IPSec выполняет согласование между компьютером и удаленным сервером туннеля перед установлением L2TP-подключения, что защищает и пароли, и данные.

L2TP использует с IPSec стандартные протоколы проверки подлинности PPP, такие как EAP, MS-CHAP, CHAP, SPAP и PAP.

Уровень шифрования определяется параметрами секретных соединений, называемых также сопоставлением безопасности IPSec. Сопоставление безопасности – это комбинация адреса назначения, протокола безопасности и уникального идентификатора, называемого индексом параметров безопасности.

Протоколы безопасности IPSEC

Протоколы безопасности обеспечивают защиту данных и подлинности для каждого пакета IP. Служба IPSEC в Windows 2000 использует протоколы AH и EPS.

AH (Authentication Header)

Протокол AH обеспечивает проверку подлинности, целостность и отсутствие повторов для всего пакета (заголовка IP и полезных данных); AH подписывает весь пакет. Данные не шифруются, поэтому конфиденциальность не обеспечивается. Данные доступны для чтения, но защищены от изменения. Протокол AH использует для подписания пакетов алгоритмы HMAC.

Например, Мария, работающая на компьютере A, отправляет данные Ивану на компьютер B. Заголовок IP, заголовок AH и данные защищены от изменения подписью. Это позволяет Ивану быть уверенным в том, что данные были отправлены именно Марией и не были изменены.

Проверка целостности и подлинности обеспечивается путем вставки заголовка AH между заголовком IP и заголовком транспортного протокола (TCP или UDP).

ESP (Encapsulating Security Payload)

ESP помимо проверки подлинности, целостности и отсутствия повторов обеспечивает также конфиденциальность.

ESP обычно не подписывает пакеты, если не используется туннель. Обычно обеспечивается только защита данных, но не заголовка IP.

Например, Мария, работающая на компьютере A, отправляет данные Ивану на компьютер B. Данные шифруются, поскольку ESP обеспечивает

конфиденциальность. При получении, после завершения процесса проверки, данные пакета расшифровываются. Иван может быть уверен в том, что данные отправлены именно Марией, что они не были изменены, а также в том, что никто другой не сможет их прочесть.

Безопасность обеспечивается путем вставки заголовка ESP между и заголовком транспортного протокола (TCP или UDP).

Протокол IKE

Протокол IKE представляет собой набор протоколов аутентификации и обмена аутентифицированными ключами. Каждый протокол из этого набора представляет собой гибрид, использующий часть протокола Окли (протокол определения ключа Окли - Oakley Key Determination Protocol), часть механизма SKEME (Механизм для многостороннего обмена секретными ключами через Internet – Versatile Secure Key Exchange Mechanism for Internet) и часть протокола ISAKMP (Протокол установления защищенных соединений и управления ключами-Internet Security Association and Key Management Protocol).

Протокол ISAKMP обеспечивает аутентификацию и обмен аутентифицированными ключами между двумя общающимися сторонами, позволяя им согласовывать и утверждать различные защитные средства, криптографические алгоритмы, параметры безопасности, механизмы аутентификации и тому подобные, т.е. все то, что в совокупности называется сопоставлением безопасности (secure associations). Однако в протоколе ISAKMP не определены конкретные способы обмена ключами, что позволяет применять его в сочетании с разными протоколами.

Будучи гибридом, протокол IKE представляет собой набор двусторонних протоколов, предназначенных для обмена аутентифицированными сеансовыми ключами, большинство из которых использует механизм обмена ключами Диффи-Хеллмана и предоставляет пользователям широкие возможности для переговоров в интерактивном режиме.

Принцип работы IPSEC

Для наглядности в данном примере рассматривается использование IPSEC для компьютеров одного домена. Алиса, работающая с приложением на компьютере A, отправляет сообщение Бобу.

1. Драйвер IPSEC на компьютере A проверяет список фильтров IP в активной политике на наличие совпадающего адреса или типа трафика

исходящих пакетов.

2. Драйвер IPSEC предоставляет ISAKMP сведения для начала согласования безопасности с компьютером B.

3. Служба ISAKMP на компьютере B получает запрос для согласования безопасности.

4. Два компьютера выполняют обмен ключами, устанавливают соответствие безопасности ISAKMP и создают общий секретный ключ.

5. Два компьютера согласовывают уровень безопасности для передачи данных, устанавливая пару соответствий безопасности IPSEC и ключей для защиты пакетов IP.

6. Используя сопоставление безопасности IPSEC для исходящего трафика и ключ, драйвер IPSEC на компьютере A подписывает пакеты для проверки целостности и зашифровывает пакеты, если было согласовано шифрование.

7. Драйвер IPSEC на компьютере A отправляет пакеты на соответствующий тип подключения для передачи на компьютер B.

8. Компьютер B получает защищенные пакеты и передает их драйверу IPSEC.

9. Используя сопоставление безопасности IPSEC для входящего трафика и ключ, драйвер IPSEC на компьютере B проверяет подпись целостности и, при необходимости, расшифровывает пакеты.

10. Драйвер IPSEC на компьютере B передает расшифрованные пакеты драйверу TCP/IP, который передает их в принимающее приложение.

Для Алисы и Боба все эти процессы не видны. Стандартные маршрутизаторы и коммутаторы, передающие данные между сторонами подключения, не требуют использования IPSEC. Они автоматически пересылают зашифрованные пакеты IP в место назначения. Однако, если маршрутизатор функционирует как брандмауэр, шлюз безопасности или прокси-сервер, для прохождения безопасных пакетов IP необходимо включить специальную фильтрацию.

Управление политикой безопасности IP

Оснастка «Управление политикой безопасности IP» используется для настройки в Windows IP-безопасности (IPSec), ключевой линии обороны на

случай внутренних (частная сеть) и внешних (Интернет, внешние сети) атак. Хотя в большинстве стратегий сетевой безопасности акцент делается на предотвращение атак на сеть организации извне, множество важных сведений может быть потеряно в результате внутренних атак с расшифровкой передаваемых по сети данных. Большая часть данных передается по сети в зашифрованном виде, но сотрудники, обслуживающий персонал или посетители могут подключиться к сети и скопировать данные для последующего анализа. Кроме того, могут быть предприняты атаки на другие компьютеры на сетевом уровне. Брандмауэры для защиты от такой внутренней угрозы не годятся, поэтому использование IPSEC значительно повышает безопасность корпоративных данных.

IPSEC шифрует данные, передаваемые между двумя компьютерами, защищая их от изменения и интерпретации при просмотре в сети. Администратор должен сначала определить доверительные отношения между двумя компьютерами, а затем указать для них способ защиты трафика. Эта конфигурация содержится в политике IPSEC, создаваемой и применяемой администратором.

Свойства политики IPSEC

Политики IPSEC могут применены к локальным компьютерам, членам домена, доменам, организационным подразделениям или любым объектам групповой политики в Active Directory. Политики IPSEC организации должны основываться на принятых в организации правилах безопасной работы. Политики могут содержать несколько действий безопасности, называемых правилами, что позволяет применять одну политику к нескольким компьютерам.

Для хранения политик IPSEC используются два расположения.

1. Active Directory.
2. Определен локально в реестре для автономных компьютеров и компьютеров, не являющихся частью доверенного домена Windows 2000/2003 постоянно. Если компьютер временно не подключен к доверенному домену Windows 2000/2003, сведения политики кэшируются в локальном реестре.

Windows содержит предопределенные политики, которые могут быть активизированы, изменены в соответствии с потребностями или использованы в качестве шаблона при создании собственных настраиваемых политик. Каждая определенная политика должна применяться к сценарию плана безопасности. При назначении политики серверу DHCP, DNS (Domain Name System), WINS, SNMP (Simple Network Management Protocol) или серверу удаленного доступа можно использовать дополнительные параметры.

Политики IPSEC, назначенные объекту групповой политики в Active Directory, становятся частью групповой политики и переносятся на компьютеры, входящие в Active Directory при распространении групповой политики.

При назначении политики IPSEC в Active Directory следует иметь в виду следующее.

– Политики IPSEC, назначенные политике домена, подавляют любую локальную активную политику IPSEC только в том случае, если компьютер является членом этого домена.

– Политики IPSEC, назначенные организационному подразделению, подавляют политику IPSEC, назначенную политике домена, на всех компьютерах, входящих в это организационное подразделение. Политика IPSEC, назначенная организационному подразделению низшего уровня, подавляет политику IPSEC, назначенную организационному подразделению высшего уровня на всех компьютерах, входящих в это подразделение.

Предопределенные политики IPSEC

Windows 2000/XP содержит набор предопределенных политик IPSEC. По умолчанию все предопределенные политики предназначены для компьютеров, являющихся членами домена Windows 2000/2003. Их можно назначать без дополнительной настройки, изменять или использовать в качестве шаблонов при создании собственных политик

Предопределенные политики

Клиент (Только ответ)

Используется только для компьютеров, безопасная связь для которых большую часть времени не требуется. Например, клиенты интрасети могут не требовать использования IPSEC, кроме случаев, когда запрос исходит с другого компьютера. Эта политика позволяет компьютеру, на котором она активизирована, должным образом отвечать на запросы безопасной связи. Эта политика содержит стандартное правило ответа, позволяющее выполнять согласование с компьютерами, требующими использования IPSEC. Защита применяется только к трафику по запрошенному протоколу и через запрошенный порт.

Сервер (запрос безопасности)

Используется для компьютеров, для которых большую часть времени требуется безопасная связь. В качестве примера можно привести сервер, через который передаются важные данные. В данной политике компьютер принимает незащищенный трафик, но всегда выполняет попытку защитить дополнительные связи, посылая отправителю запрос безопасности. Эта политика допускает полное отсутствие защиты трафика, если другой компьютер не поддерживает IPSEC.

Безопасность сервера (требовать безопасность)

Эта политика используется для компьютеров, постоянно требующих безопасной связи. Примером может служить сервер, передающий весьма важные данные, или шлюз безопасности, защищающий интрасеть от

посторонних. Эта политика отклоняет небезопасные входящие связи, а исходящий трафик всегда защищен. Небезопасная связь не допускается, даже если другая сторона не поддерживает IPSEC.

Предопределенные правила

Как и предопределенные политики, предопределенное правило отклика может быть активизировано без дополнительной настройки или изменено в соответствии с конкретными потребностями. Оно добавляется в каждую создаваемую политику, но не активизируется автоматически. Правило предназначено для любых компьютеров, которые не требуют безопасности, но должны иметь возможность дать соответствующий отклик при запросе безопасной связи от другого компьютера.

Предопределенные действия фильтра

Как и предопределенные правила, предопределенные действия фильтра могут быть активизированы без дополнительной настройки, изменены или использованы в качестве шаблона при определении собственных действий фильтра. Следующие действия доступны для активизации в любом новом или существующем правиле.

– **Требовать безопасность**. Высокая безопасность. Небезопасные связи не допускаются.

– **Запрос безопасности (необязательно)**. Безопасность от средней до низкой. Небезопасная связь допускается для обеспечения связи с компьютерами, не выполняющими согласование IPSEC.

Добавление или изменение политики IPSEC

1. В оснастке «Управление политикой безопасности IP» выберите создание новой политики или изменение текущей.

Чтобы	Выполните следующие действия
Создать новую политику	Выберите в дереве консоли **Политики безопасности IP на** описание, а затем выберите в меню **Действие** команду **Создать политику безопасности IP**. Выполняйте инструкции мастера политики безопасности IP до вывода на экран диалогового окна новой политики.
Изменить существующую политику	Щелкните нужную политику правой кнопкой мыши и выберите команду **Свойства**.

2. На вкладке **Общие** введите уникальное имя в поле **Имя**.

3. В поле **Описание** введите описание политики безопасности, например укажите группы или домены, которые она затрагивает.

4. Если компьютер является частью домена, введите значение в поле **Проверять политику на наличие изменений каждые** число **минут**, чтобы задать частоту выполнения агентом политики проверки групповой политики на наличие обновлений

5. При наличии особых потребностей в безопасности при обмене ключами нажмите кнопку **Дополнительно**.

6. Перейдите на вкладку **Правила** и создайте все необходимые правила для политики.

Добавление и изменение правила

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите, следует ли использовать мастер добавления:

— чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению правила безопасности, убедитесь в том, что флажок **Использовать мастер** установлен, нажмите кнопку **Далее** и следуйте выводимым на экран инструкциям;

— для того чтобы добавить или изменить правило вручную, снимите флажок **Использовать мастер**, нажмите кнопку **Добавить** или **Изменить** и выполните следующие шаги данной процедуры.

3. На соответствующих вкладках задайте список фильтров IP, действие фильтра, тип подключения, методы проверки подлинности и параметры туннеля.

Добавление и изменение действия фильтра

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, нажмите кнопку **Изменить**, а затем перейдите на вкладку **Действие фильтра**.

3. Выберите, следует ли использовать мастер добавления:

— чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению действия фильтра, убедитесь в том, что флажок **Использовать мастер** установлен, а затем следуйте выводимым на экран инструкциям;

— для того чтобы выполнить добавление или изменение действий фильтра вручную, снимите флажок **Использовать мастер**, а затем нажмите кнопку **Добавить** для добавления действия фильтра или кнопку **Изменить** для изменения настроек действия фильтра.

4. Выберите действие фильтра.

— Выберите **Разрешить**, чтобы разрешить получение или отправку незашифрованных пакетов. Безопасность для этих пакетов запрашиваться не будет.

— Выберите **Блокировать**, чтобы пакеты, совпадающие с данным фильтром, немедленно отбрасывались. Безопасность для этих пакетов запрашиваться не будет.

—

— Выберите **Согласовать безопасность**, чтобы использовать для обеспечения безопасности пакетов, совпадающих с фильтром, методы безопасности из списка **Методы безопасности в порядке предпочтения**. Запросы безопасности для этих пакетов будут приниматься.

5. Если входящие незащищенные пакеты блокировать не требуется, но необходимо обеспечить безопасность исходящих запросов и последующего двустороннего обмена данными, установите флажок **Принимать небезопасную связь, но отвечать с помощью IPSEC**.

6. Если требуется сделать возможной связь с другими компьютерами, не поддерживающими IPSEC, и обеспечить продолжение связи при отсутствии ответа на запрос согласования безопасности IPSEC, установите флажок **Разрешать связь с компьютерами, не поддерживающими IPSEC**. Если этот параметр включен, то после сбоя согласования IPSEC с конкретным узлом безопасность IPSEC для связи с этим узлом отключается на некоторое время.

7. Установка флажка **Сеансовые циклы безопасной пересылки (PFS)** гарантирует, что основные ключи или исходные данные ключа не используются для создания ключа сеанса более одного раза.

8. На вкладке **Общие** введите уникальное имя.

9. Введите описание. Например, можно указать уровни безопасности, представляемые данным действием ключа.

10. Если выбрано действие **Согласовать безопасность**, добавьте новые или измените существующие методы безопасности для действия фильтра.

Задание туннеля IPSEC

1. В области сведений оснастки «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Параметры туннеля** укажите компьютер, который будет конечной точкой туннеля:

Чтобы	Выполните следующие действия
Отключить туннелирование для данного правила	Выберите **Это правило не указывает туннель IPSEC**.
Использовать туннелированную связь с конкретным компьютером	Выберите **Конечная точка туннеля указана данным IP-адресом**.

Определение методов проверки подлинности IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Методы проверки подлинности** нажмите кнопку **Добавить**. При изменении настроек существующего метода выберите изменяемый метод проверки подлинности и нажмите кнопку **Изменить**.

4. Определите методы проверки подлинности:

— выберите **Стандарт Windows 2000 (Kerberos V5)**, чтобы использовать для служб проверки подлинности протокол безопасности Kerberos V5, если данное правило применяется к компьютерам, которые заверены доверенным доменом Windows 2000;

— чтобы использовать для служб проверки подлинности сертификат открытого ключа, выберите **Использовать сертификат данного Центра сертификации**.

— Если выбрано использование сертификата, нажмите кнопку **Обзор** для выбора корневого центра сертификации.

— Чтобы указать для использования при проверке подлинности собственный ключ, выберите **Использовать данную строку для защиты обмена ключами**.

Указание типа подключения IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Тип подключения** выберите тип сетевых подключений, для которых будет применяться данное правило:

— чтобы применить правило ко всем сетевым подключениям, созданным на данном компьютере, выберите **Все сетевые подключения**;

— чтобы применить правило ко всем локальным подключениям, созданным на данном компьютере, выберите **Локальное сетевое подключение**;

— чтобы применить правило к удаленным сетевым подключениям, созданным на данном компьютере, выберите **Удаленный доступ**.

3.Практическая часть

Создать политику безопасности IPSEC, реализующей следующие требования:

1. Весь SMTP и POP3-трафик между локальным компьютером и любым другим, поддерживающим шифрование, должен использовать обязательное шифрование для всех сетевых подключения.

2. Весь IP-трафик между локальным компьютером и подсетью 195.17.72.0/255.255.255.0 должен использовать обязательное шифрование для всех сетевых подключения.

3. Весь IP-трафик между локальным компьютером и подсетью 195.17.73.0/255.255.255.0 должен использовать обязательное шифрование для всех сетевых подключения с использованием сертификата открытого ключа для проверки подлинности, выданного центром сертификации VeriSign.

Отчет должен содержать последовательность действий по созданию и настройке параметров политики, правил и фильтров.

4.Контрольные вопросы

1. Назначение протокола IPSec.
2. Состав семейства протоколов IPSec.
3. Средства настройки IPSec в Windows 2000/XP.
4. Состав политики безопасности.
5. Создание правил и фильтров для политики безопасности.
6. Возможные методы проверки подлинности IPSec.
7. Возможные места хранения назначенных политик безопасности.

Основная литература

1. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2005

2. Мао Венбо Современная криптография: теория и практика. М.: Издательский дом «Вильямс», 2005

Дополнительная литература

1. Справочная система ОС Windows 2000/XP

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению самостоятельных работ
по дисциплине «Защищенные информационные системы»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026

СОДЕРЖАНИЕ

Введение

Основной целью изучения дисциплины «Защищенные информационные системы» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 Информационная безопасность.

Для достижения указанной цели в процессе изучения данной дисциплины необходимо решить следующие задачи:

- изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
- изучение современных технологий построения безопасных информационных систем;
- изучение этапов и технологий проектирования и создания безопасных информационных систем;
- изучение современных программных и аппаратных средств защиты информации;
- изучение основных угроз информации в современных информационных системах и сетях;
- изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей;
- формирование умений в разработке проектов комплексных защищенных инфра структур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации; формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

№ п/п	Содержание компетенции	Шифр
Общие профессиональные компетенции		**ОПК-(№)**
1.	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1
2.	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ	– современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; современные технологии построения безопасных информационных систем; – этапы и технологию проектирования и создания безопасных информационных систем; современные программные и аппаратные средства защиты информации; – основные угрозы информации в информационных системах и сетях; – инструментальные программные и аппаратные средства анализа

	защищенности информационных систем и сетей.
УМЕТЬ	– проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности; применять современные программные средства защиты информации; – применять современные аппаратные средства защиты информационных процессов в компьютерных системах; применять программные библиотеки и пакеты для создания безопасных информационных систем.
ВЛАДЕТЬ	– навыками разработки комплексной инфраструктуры защищенной информационной системы; – навыками базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов; навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации.

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области защищенных информационных системах. На лабораторных занятиях 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 занятиям, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

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 студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;

– подготовка к лабораторным занятиям, оформление отчета по выполненному лабораторной работе 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 занятиям;

– решение задач и практических заданий;

– подготовка отчетов по лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Защищенные информационные системы»

Коды реализуемых копетенций, индикаторов	Вид деятельности студентов	Средства и технологии оценки	Обьем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ИД-1$_{ОПК-1}$, ИД-3 $_{ОПК-1,}$ ИД-2$_{ОПК-2}$, ИД-3$_{ОПК-2}$	Самостоятельное изучение литературы	Собеседование	6.00	4.00	10.00
ИД-1$_{ОПК-1}$, ИД-3 $_{ОПК-1,}$ ИД-2$_{ОПК-2}$, ИД-3$_{ОПК-2}$	Подготовка к экзамену	Вопросы к экзамену	6.00	2.00	8.00

		Итого за 3 семестр	12.00	6.00	18.00
2 семестр					
ИД-1$_{ОПК-1}$, ИД-3 $_{ОПК-1}$, ИД-2$_{ОПК-2}$, ИД-3$_{ОПК-2}$	Выполнение курсовой работы	Задания для курсовой работы	21.00	3.00	24.00
		Итого за 2 семестр	21.00	3.00	24.00
		Итого	33.00	9.00	42.00

3. Контрольные точки и виды отчетности по ним

По дисциплине предусмотрен текущий контроль на каждом учебном занятии и по каждому разделу учебной дисциплины.

Формы текущего контроля:

- устный опрос;
- защита отчетов по лабораторным занятиям.

Устный опрос осуществляется на каждом учебном занятии (лекции, лабораторные занятия). Все практические занятия, выполняемые по разделам дисциплины, подлежат оцениванию по результатам проверки отчета и собеседованию.

Критерии оценки для проверки умений при выполнении лабораторных заданий:

- оценка «отлично» выставляется, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретной задачи, свободно без затруднений справился с поставленной задачей, показав владение разносторонними приемами и навыками ее выполнения, не допустил ошибок и неточностей;
- оценка «хорошо» выставляется, если студент продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, справился с поставленной задачей, показав владение необходимыми приемами и навыками ее выполнения, при этом допустил не более одной ошибки;
- оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретной задачи, с трудом справился с поставленной задачей, при этом допустил не более двух ошибок;
- оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, не справился с поставленной задачей или допустил при ее решении три и более серьезные ошибки.

4. Методические указания по подготовке к лабораторным занятиям

При подготовке к лабораторной работе студенту следует:

- изучить (повторить) теоретический материал, посвящённый теме практического занятия;
- ознакомиться с заданием на лабораторную работу;
- проверить свой уровень подготовки с помощью вопросов и заданий для самоконтроля.

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

занятия.

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.

Требования безопасности во время работы:

– выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторной работе;

– 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.

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.

По результатам выполнения лабораторной работы студенты оформляют и защищают в индивидуальном порядке в форме собеседования результаты выполнения заданий.

При подготовке и выполнении лабораторных работ совместно с оформлением отчетов по лабораторным занятиям позволяет успешно овладеть умениями, необходимыми для дальнейшей учебной и профессиональной деятельности.

Задания, выполняемые по лабораторным работам

2 семестр:

Практическая работа 1. Исследование методов аутентификации.

Базовый уровень:

1. Перечислить виды атак на пароли.
2. Перечислить критерии стойкости парольной защиты.
3. Перечислить и охарактеризовать методы противостояния атаке полным перебором.
4. Охарактеризовать влияние длины пароля на вероятность раскрытия.
5. Сформировать рекомендации по составлению паролей.

Повышенный уровень:

6. Перечислить типы угроз безопасности парольных систем.
7. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
8. Определить время перебора всех паролей, состоящих из 6 цифр.

Практическая работа 2. Исследование механизмов обнаружения сетевых аномалий.

Базовый уровень:

9. Этапы и средства реализации атак. Классификация атак.
10. Таксономия систем обнаружения атак.
11. Совместное применение систем обнаружения атак и других средств защиты.
12. Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
13. Анализ журналов регистрации и сетевого трафика.

Повышенный уровень:

14. Анализ заголовков, процессов, сервисов и портов.
15. Настроить NetFlow на маршрутизаторе.
16. Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

Практическая работа 3. Настройка безопасности в MySQL.

Базовый уровень:

17. Каким способом возможен запуск серверной части СУБД.
18. Что такое привилегия. Каково её предназначение.

Повышенный уровень:

19. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

Практическая работа 4. Механизмы функционирования межсетевых экранов

Базовый уровень:

20. Опишите утилиту ping, методы и случаи ее применения.
21. Описать данные, полученные о компьютере с помощью XSpider.
22. Опишите типы уязвимостей компьютерных систем.

Повышенный уровень:

23. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
24. Описать известные типы МСЭ и отличия между ними.

Практическая работа 5. Протоколы туннелирования. Организация защищенных удаленных подключений.

Базовый уровень:

25. Смоделировать и исследовать в PT Visual Studio структуру двухточеченой сети.
26. Сформулировать требования к оборудованию для реализации GRE.
27. Перечислить основные этапы конфигурирования GRE.
28. Синтаксис команд для включения GRE туннеля в Cisco IOS.
29. Реализация защищенного GRE туннеля с использованием IPSec.
30. Смоделировать и исследовать PT распределенную сеть на основе протокола PPP.
31. Настроить аутентификацию PPP CHAP.
32. Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.
33. Настроить инкапсуляцию PPP.
34. Перечислить отличия HDLC и PPP.

Повышенный уровень:

35. Настроить статическую маршрутизацию при использовании GRE.
36. Настроить динамическую маршрутизацию при использовании GRE.
37. Перечислить поля кадров HDLC и PPP
38. Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.
39. Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

Задания, выполняемые по практическим занятиям

2 семестр:

Практическое занятие 1. Исследование механизмов защиты информации в автоматизированных системах.

Базовый уровень:

1. Что, по Вашему мнению, означает термин «политика паролей»?
2. Перечислите простые правила политики паролей ОС Windows XP?
3. Под какой учетной записью можно производить настройку политики безопасности ОС Windows XP?

Повышенный уровень:

4. Объясните, почему данный параметр является самым важным.
5. От какого параметра зависит опция Блокировка учетной записи, и каким образом она устанавливается?
6. Объясните значение параметра Пороговое значение блокировки.

Практическое занятие 2. Этапы разработки политики информационной безопасности.

Базовый уровень:

7. Что называется политикой безопасности.
8. Для каких целей составляется политика безопасности.
9. Какие шаги необходимо выполнить для составления политики безопасности.

Повышенный уровень:

10. Что является общей политикой безопасности предприятия.
11. Как происходит заполнение матрицы общей политики безопасности предприятия.

Практическое занятие 3. Разработка политики информационной безопасности.

Базовый уровень:

12. Дайте определение понятия - Политика информационной безопасности.
13. Что такое процесс анализа рисков? Какова роль анализа рисков в процессе формирования политики безопасности компании.
14. В чем отличие полного анализа рисков от базового?

Повышенный уровень:

15. Назовите основные разделы стандарта ISO 17799.

Практическое занятие 4. Виды аутентификации пользователей.

Базовый уровень:

16. Что такое одноразовые пароли?
17. Опишите принцип работы OTP-токенов.
18. Приведите пример аутентификации пользователя при использовании OTP-токеном метода «запрос—ответ».

Повышенный уровень:

19. Назовите поведенческие биометрические характеристики.
20. Опишите принцип работы биометрических систем

Практическое занятие 5. Исследование механизма защиты информации в VPN. Исследование методов доступа к данным в MySQL.

Базовый уровень:

21. Приведите пример аутентификации пользователя при использовании OTP-токеном метода «только ответ».
22. Приведите пример аутентификации пользователя при использовании OTP-токеном метода «синхронизация по времени».
23. Пояснить структуру таблицы Db
24. Перечислить типы переменных в MySQL».

Повышенный уровень:

25. Приведите пример аутентификации пользователя при использовании OTP-токеном метода «синхронизация по событию».
26. Разработать модель базы данных с заданными привилегиями пользователя».

5. Примерная тематика заданий для самостоятельной работы студентов

2 семестр:

Базовый уровень:

1. Цель и задачи проекта.
2. Требования регуляторов.
3. Контентная категоризация.
4. Классификация информации по уровню конфиденциальности.
5. Метки документов
6. Основные направления защиты.
7. Защита документов.
8. Защита каналов утечки.
9. Мониторинг (аудит) действий пользователей.
10. Классификация внутренних нарушителей.
11. Нетехнические меры защиты от внутренних угроз.
12. Психологические меры.
13. Организационные меры
14. Персональные firewall'bi и персональные устройства firewall'a.
15. VPNи Dial-incерверы.
16. Внутренние серверы.
17. DNS- серверы.
18. SMTP-серверы.
19. Основные характеристики пакетных фильтров в ОС FreeBSD.
20. Определение злоупотреблений.

Повышенный уровень:

21. Определение аномалий.
22. Возможные ответные действия IDS.
23. Системы Honey Pot и Padded Cell.
24. Выбор IDS.
25. Определение окружения IDS.
26. Авторитетные паше-серверы.
27. Кэширующие name- серверы.
28. Resolver'bi.
29. Безопасное инсталлирование и конфигурирование ОС
30. Обеспечение безопасности технологий создания активного содержимого.
31. URLsи cookies.
32. Требования к аутентификации и шифрованию.
33. Аутентификация, основанная на IP-адресе.
34. Автоматизированные инструментальные средства анализа лог-файлов

6. Список рекомендуемой литературы

Основная литература:

1. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с

2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с.

Дополнительная литература:

1. Защита информации в операционных системах : (спец. 090103 Организация и технология защиты информации, 090102 – Компьютерная безопасность) : учеб. пособие / авт. сост.: И. В. Зайцева / М. В. Романкова / Федеральное агентство по образованию,

Ставроп. гос. ун-т. - Ставрополь : Изд-во СГУ, 2008. - 318 З-402 с. - Библиогр.: с. 311-312.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2008. – 256 с

Методическая литература:

Интернет-ресурсы:

1. http://tasic-moe.ru/newsletter9/page3.htm
2. http://www.statgraphics.com Пакет прикладных программ Statgraphics
3. http://www.statsoft.ru/home/textbook/default.htm Электронный учебник StatSoft
4. http://www.exponenta.ru Образовательный математический сайт

Программное обеспечение

Не предусмотрено

Материально-техническое обеспечение дисциплины

Компьютерные классы с наличием компьютеров из расчета один студент за один компьютер

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук имени профессора Н.И. Червякова
Кафедра «Организация и технология защиты информации»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению курсовой работы
по дисциплине «Защищенные информационные системы»

для направления подготовки
10.04.01– Информационная безопасность
Направленность (профиль) «Информационная безопасность киберфизических систем»

Ставрополь – 2026

Печатается по решению
Учебно-методического совета
Северо-Кавказского
федерального университета

Методические указания по выполнению курсовой работы по дисциплине «Защищенные информационные системы». Учебно-методическое пособие / авт.– сост.: В.М. Бисюков – Ставрополь: Изд-во СКФУ, 2020. – 24 с.

Пособие разработано в соответствии с ФГОС ВО и предназначено для студентов направления 10.04.01– Информационная безопасность

Разработано:
доцентом кафедры ОТЗИ Бисюковым В.М.

Рецензент:
кандидат технических наук, доцент Стадников Р.Ю.

Содержание

1 Общие требования к выполнению курсовой работы

Курсовая работа – обязательный вид учебной работы, выполняется студентом в течение семестра.

Курсовая работ является самостоятельной исследовательской работой студента и представляет собой логически завершенное и оформленное научное исследование. Курсовая работа направлена на формирование у студента навыков научно-исследовательской работы, повышение уровня его профессиональной (теоретической и практической) подготовки, углубление знаний по учебной дисциплине, развитие интереса и навыков самостоятельной работы с научной и справочной литературой.

1.1 Цели и задачи курсовой работы

Выполнение курсовой работы имеет целью расширение знаний студентов, обучение методам теоретического анализа явлений и закономерностей науки, отработку навыков самостоятельного применения теоретических знаний к комплексному решению профессиональных задач, использования справочной литературы, методов математической обработки экспериментальных данных, компьютерных технологий.

Системой курсовых работ студент подготавливается к выполнению выпускной квалификационной работы.

В процессе выполнения курсовой работы студентом должны решаться следующие задачи:

−приобретение новых теоретических знаний в соответствии с темой работы и заданием руководителя;

−развитие умений систематизировать, обобщать и логично излагать концепции, альтернативные точки зрения исследуемых проблем;

−развитие учебно-исследовательских и методических умений, необходимых для построения системы научного анализа изучаемого аспекта;

−совершенствование профессиональной подготовки.

1.2 Тематика курсовых работ

Одним из важных компонентов в системе постановки курсового проектирования (курсовой работы) является правильное определение тематики.

Тематика курсовых работ должна быть актуальной, отвечать учебным задачам данного предмета, а также потребностям науки и практики. Актуальность тематики курсовых работ - это, прежде всего, научность, современность и направленность к получению студентами навыков самостоятельной творческой работы.

Темы курсовых работ должны быть комплексными, т.е. содержать ряд взаимосвязанных между собой проблем и строиться на фактическом материале профильных предприятий и учреждений, а также на итогах учебной и производственной практики студентов, на научных работах членов кафедры, студенческих научных кружков и проблемных групп, с использование новейших достижений отечественной и зарубежной науки, актуальных прикладных аспектов.

Темы курсовых работ утверждаются на заседании кафедры, ведущей дисциплины, по которым учебными планами предусмотрены курсовые работы. Выписка из протокола заседания кафедры передается в дирекцию факультетата, где формируется распоряжение об утверждении тем курсовых работ. В течение 10 дней после выхода распоряжения об утверждении тем курсовых работ специалист по учебно-методической работе дирекции вносит названия тем в автоматизированную базу университета.

Основные содержательные и процессуальные аспекты, необходимые для выполнения работы, оформляются кафедрой в заданиях на курсовую работу (Приложение А). В заданиях необходимо четко сформулировать название темы работы и требования, определяющие его объем, содержание, а также исходные данные для выполнения количественных расчетов.

1.3 Содержание и структура курсовых работ

Курсовая работа (проект) должна содержать элементы новизны, наряду с фундаментальным аспектом должен быть проведен анализ современного состояния изучаемой проблемы, а также отражены региональные особенности.

Задание по курсовой работе необходимо индивидуализировать с учетом интересов и способностей студентов.

Курсовая работа (проект) должна состоять из:

- содержания;
- введения;
- теоретической части;
- эмпирической части;
- заключения;
- списка использованных источников;
- приложения.

В отдельных случаях, в соответствии с тематикой работы, эмпирическая часть может отсутствовать.

Титульный лист оформляется в соответствии с Приложением Б.

Содержание включает названия разделов, подразделов работы с указанием страницы начала каждой части (Приложение В).

Во введении обосновывается актуальность выбранной темы исследования; отражаются объект, предмет, задачи, цели, методы, новизна, теоретическая и практическая значимость исследования.

Теоретическая часть должна содержать анализ состояния изучаемой проблемы на основе обзора научной, научно-информационной, справочной литературы. Представленный материал должен быть логически связан с целью исследования. В параграфах теоретической части необходимо отражать отдельные компоненты проблемы и завершать их выводами.

Эмпирическая (практическая, расчетно-графическая) часть (при наличии) включает описание системы экспериментального исследования, обоснование методов исследования, анализ результатов экспериментального исследования, схемы, графические и математические способы интерпретации полученных данных, выводы.

Заключение содержит выводы, подтверждающие или опровергающие первоначальные предположения (гипотезы), перспективы дальнейшего изучения проблемы, связь с практикой, анализ реализации целей и задач исследования.

Список использованных источников должен содержать перечень всех используемых автором нормативных документов, монографий, учебных и учебно-методических пособий, статей и интернет-источников (Приложение Г).

При ссылке в тексте номер источника из списка литературы заключается в квадратные скобки, например, [1], [1, 3-4] или [1-2].

Приложение содержит весь фактический материал экспериментальных исследований (анкеты, опросники, схемы, чертежи, расчетные материалы, карты, рисунки, ответы респондентов и т.д.).

2. Рекомендации по подготовке и оформлению курсовой работы

Курсовые работы (проекты) рекомендуется представлять в объеме 30-40 страниц. Текст работы должен быть напечатан через 1,5 интервала на одной стороне стандартного листа белой бумаги (А - 4).

Текст курсовой работы выполняют с использованием компьютера на одной стороне листа белой бумаги, формата А4, шрифт - Times New Roman 14-го размера, межстрочный интервал - 1,5. Номер страницы проставляют в правом нижнем углу листа. Страницы текстового материала следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему документу. Титульный лист текстового документа включают в общую нумерацию страниц. Номер страницы на титульном листе не проставляют. Расстояние от края бумаги до границ текста следует оставлять: в начале строк - 30 мм; в конце строк - 10 мм; от верхней или нижней строки текста до верхнего или нижнего края бумаги - 20 мм. Размер абзацного отступа должен быть одинаковым по всему тексту работы и равным 12,5 мм.

Разделы должны иметь порядковые номера в пределах всей курсовой работы, обозначенные арабскими цифрами. Подразделы должны иметь нумерацию в пределах каждого раздела. Номера подразделов состоят из номера раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Нумерация пунктов должна состоять из номера раздела, подраздела и пункта, разделенных точкой.

Заголовок разделов, подразделов и пунктов следует печатать с абзацного отступа, с прописной буквы, без точки в конце, не подчеркивая. Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

Ниже каждого заголовка должна быть оставлена одна свободная строка, выше - не менее одной свободной строки. Оставляют свободные строки между разделами и подразделами.

Пример

1 Методы испытаний

1.1 Аппараты, материалы и реактивы

2 Подготовка к испытанию

2.1 Нумерация пунктов первого подраздела третьего раздела документа

3

3.2 Подготовка к испытанию

3.3 Нумерация пунктов второго подраздела третьего раздела документа

Если раздел или подраздел состоит из одного пункта, он также нумеруется. Если текст документа подразделяется только на пункты, они нумеруются порядковыми номерами в пределах документа.

Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например: 4.2.1; 4.2.1.1; 4.2.1.2; 4.2.2 и т. д. Между подпунктами и текстом интервалы не оставляются. Подпункты с тройной нумерацией (1.1.1…) и больше в содержание не выносятся.

Внутри пунктов или подпунктов могут быть приведены перечисления.

Перед каждым перечислением следует ставить дефис или, при необходимости ссылки в тексте документа на одно из перечислений, строчную букву, после которой ставится скобка.

Для дальнейшей детализации перечислений необходимо использовать цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

Пример:

- _____
- _____
  1) _____
  2) _____
- _____

Каждый раздел курсовой работы следует начинать с нового листа (страницы).

В документе большого объема на первом (заглавном) листе помещают содержание, включающее номера и наименования разделов и подразделов с указанием номеров листов (страниц). Содержание включают в общее количество листов данного документа. Слово "Содержание" записывают в виде заголовка (симметрично тексту) с прописной буквы. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы.

Список использованных источников должен быть оформлен в соответствии с ГОСТом 7.1-2003 «Библиографическая запись. Библиографическое описание».

2.1 Изложение текста

Текст документа должен быть кратким, четким и не допускать различных толкований.

При изложении обязательных требований в тексте должны применяться слова "должен", "следует", "необходимо", "требуется, чтобы", "разрешается только", "не допускается", "запрещается", "не следует". При изложении других положений следует применять слова - "могут быть", "как правило", "при необходимости", "может быть", "в случае" и т.д.

При этом допускается использовать повествовательную форму изложения текста документа, например "применяют", "указывают" и т.п.

В тексте должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии – общепринятые в научно-технической литературе.

В тексте не допускается:

- применять обороты разговорной речи, техницизмы, профессионализмы;

- применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова при наличии равнозначных слов и терминов на русском языке;

- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, в расшифровках буквенных обозначений, входящих в формулы и рисунки; применять математический знак минус (-) перед отрицательными значениями величин (следует писать слово «минус»);

- применять без числовых значений математические знаки, например, > (больше), < (меньше), = (равно), ≠ (не равно), а также знака № (номер), % (процент); применять индексы стандартов без

регистрирующего номера; перечень допускаемых сокращений слов установлен в ГОСТ 2.316, ГОСТ 7.12; в тексте следует применять стандартизованные единицы физических величин, их наименование и обозначение, установленные в ГОСТ 8.417;

- если в тексте курсовой работы приводится диапазон числовых значений физической величины, то обозначение единицы физической величины указывается, после последнего числового значения диапазона.

Примеры: 1. От 1 до 5 мм.

2. От плюс 10 до минус 40^0 С.

Недопустимо отделять единицу физической величины от числового значения (переносить их на разные строки или страницы), кроме единиц физических величин, помещенных в таблицах, выполненных машинописным способом.

2.2 Формулы

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено не менее одной свободной строки. Если уравнение не умещается в одну строку, то оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (-), умножения (х), деления (:), или других математических знаков, причем знак в начале следующей строки повторяют. При переносе формулы на знаке, символизирующем операцию умножения, применяют знак «Х».

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они даны в формуле.

Формулы в курсовой работе следует нумеровать порядковой нумерацией в пределах всей курсовой работы арабскими цифрами в круглых скобках в крайнем правом положении на строке.

Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Одну формулу обозначают - (1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула (В.1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой, например (3.1).

После формулы помещают перечень всех принятых в формуле символов с расшифровкой их значений и указанием размерности (если в этом есть необходимость). Буквенные обозначения дают в той же последовательности, в которой они приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

$$PS = \langle F, Z, I \rangle, \qquad (1)$$

где F - рабочая память системы (называемая также базой данных), содержащая текущие данные (элементы рабочей памяти);

Z - база знаний, содержащая множество продукций (правил вида: "условие → действие");

I - интерпретатор (решатель), реализующий процедуры вывода.

Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой.

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула (В. 1). Ссылки в тексте на порядковые номера формул дают в скобках.

Пример -... в формуле (1).

2.3 Иллюстрации и приложения

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в курсовой работе непосредственно после текста, в котором они упоминаются впервые, или на следующей странице.

Иллюстрации могут быть в компьютерном исполнении, в том числе и цветные. На все иллюстрации должны быть даны ссылки в курсовой работе. Чертежи, графики, диаграммы, схемы, иллюстрации, помещаемые в курсовой работе, должны соответствовать требованиям государственных стандартов Единой системы конструкторской документации (ЕСКД).

Допускается выполнение чертежей, графиков, диаграмм, схем посредством использования компьютерной печати.

Фотоснимки размером меньше формата А4 должны быть наклеены на стандартные листы белой бумаги.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается «Рисунок 1». Слово «рисунок» и его наименование располагают посередине строки.

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например - Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например Рисунок 1.1.

Выше и ниже каждой иллюстрации должно быть оставлено не менее одной свободной строки.

Пример:

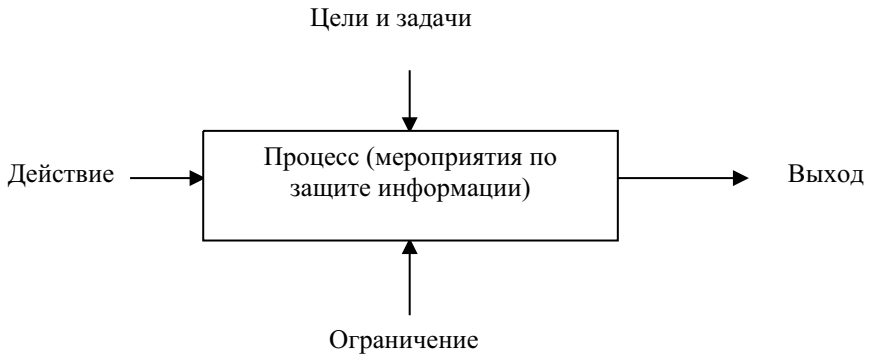


Рисунок 1 – Основные характеристики системы защиты

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст).

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например, Рисунок А.3.

При ссылках на иллюстрации следует писать «... в соответствии с рисунком 2».

Материал, дополняющий текст документа, допускается помещать в приложениях. Приложениями

могут быть, например, графический материал, таблицы большого формата, расчеты, описания аппаратуры и приборов, описания алгоритмов и программ задач, решаемых на ЭВМ и т.д.

Приложение оформляют как продолжение данного документа на последующих его листах или выпускают в виде самостоятельного документа.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова "Приложение" и его обозначения, а под ним в скобках для обязательного приложения пишут слово "обязательное", а для информационного - "рекомендуемое" или "справочное".

Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ь, Ы, Ъ. После слова "Приложение" следует буква, обозначающая его последовательность. Приложения, как правило, выполняют на листах формата А4. Допускается оформлять приложения на листах формата А3, А4 3, А4 4, А2 и А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Пример:

Приложение А

(обязательное)

Все приложения должны быть перечислены в содержании документа (при наличии) с указанием их номеров и заголовков.

2.4 Таблицы

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Слово "Таблица" указывают один раз слева над первой частью таблицы, над другими частями пишут слова "Продолжение таблицы" с указанием номера (обозначения) таблицы. При переносе части таблицы название помещают только над первой частью таблицы, нижнюю горизонтальную черту, ограничивающую таблицу, не проводят.

Таблицу следует располагать в курсовой работе непосредственно после текста, в котором она упоминается впервые, или на следующей странице, а при необходимости, в приложении к документу.

Допускается помещать таблицу вдоль длинной стороны листа документа. На все таблицы должны быть ссылки в отчете. При ссылке следует писать слово «таблица» с указанием ее номера.

Таблицу с большим количеством строк допускается переносить на другой лист (страницу).

При переносе части таблицы на другой лист (страницу) слово «Таблица» и номер ее указывают слева над первой частью таблицы, над другими частями пишут «Продолжение таблицы 1».

Цифровой материал, как правило, оформляют в виде таблиц в соответствии с рисунком 1.

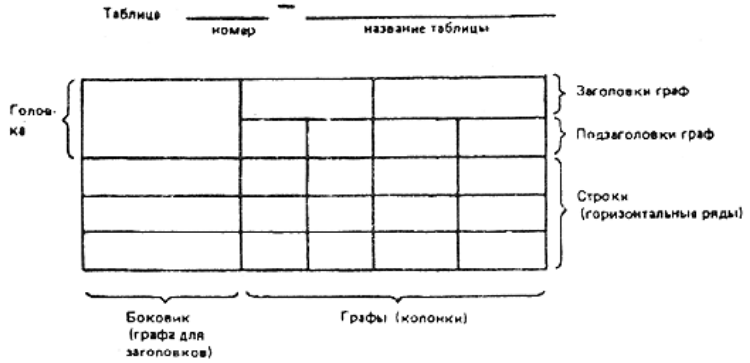


Рисунок 1– Пример таблицы

Если цифровые или иные данные в какой-либо строке таблицы не приводят, то в ней ставят прочерк.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

Если в документе одна таблица, то она должна быть обозначена «Таблица 1» или «Таблица В. 1», если она приведена в приложении В.

Заголовки граф и строк таблицы следует писать с прописной буквы в единственном числе, а подзаголовки граф — со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц

точки не ставят.

Таблицы слева, справа и снизу, как правило, ограничивают линиями. Допускается применять размер шрифта в таблице меньший, чем в тексте.

Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Высота строк таблицы должна быть не менее 8 мм.

Заголовки граф, как правило, записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Если строки или графы таблицы выходят за формат страницы, ее делят на части, помещая одну часть под другой или рядом, при этом в каждой части таблицы повторяют ее головку и боковик. При делении таблицы на части допускается ее головку или боковик заменять соответственно номером граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы. Оформление таблиц в курсовой работе должно соответствовать ГОСТ 1.5 и ГОСТ 2.105.

Пример:

Таблица 1 – Результаты структурирования информации

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена информации	Наименование источника информации	№ элемента информации
1	2	3	4	5	6

Продолжение таблицы 1

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена информации	Наименование источника информации	№ элемента информации
1	*2*	*3*	*4*	*5*	*6*

Графическая часть курсовой работы (чертежи, схемы и т. п.) выполняется с соблюдением соответствующих государственных стандартов. Каждое приложение должно начинаться с нового листа с указанием вверху листа по центру слова «Приложение» и иметь тематический заголовок.

3 Организация выполнения и порядок руководства курсовыми работами

Руководство курсовыми работами должно поручаться наиболее квалифицированным преподавателям кафедры, обладающим методическим опытом и научной квалификацией. Для учета специфики курсовых работ по специальностям каждой кафедре необходимо разработать методические указания по выполнению курсовых работ.

Руководство курсовыми работами начинается с выдачи задания студентам. В этот период необходимым условием, обеспечивающим эффективность дальнейшего руководства, является индивидуальная беседа руководителя со студентом по заданию. В ходе беседы руководитель должен выяснить степень подготовленности студента к выполнению данного задания, рекомендовать необходимую литературу и информировать о порядке выполнения задания. В результате индивидуальной беседы может быть уточнена или выбрана студентом другая тема работы.

Задание выдается за подписью руководителя работы, датируется днем выдачи и регистрируется в кафедральном журнале.

В ряде случаев необходимо организовывать на кафедре чтение вводных лекций профессора или одного из опытных руководителей с целью разъяснения значения курсовой работы для данной дисциплины, требований, предъявляемых к работе.

В рамках отведенного для руководства курсовыми работами времени должны регулярно проводиться индивидуальные консультации.

Одной из важных форм руководства является предварительный просмотр выполненной курсовой работы. Если работа содержит экспериментальную часть, то руководитель, прежде всего, должен провести экспертизу этой части, а затем указать все ошибки, неточности по работе в целом.

После проверки выполнения студентом одного этапа работы, руководитель работы разрешает студенту перейти к следующему.

Заведующий кафедрой должен периодически проверять состояние работы, контролировать направленность и методику деятельности отдельных руководителей, давая на заседаниях кафедры соответствующие методические указания.

Работа перед сдачей руководителю подписывается студентом. Если работа удовлетворяет требованиям, предъявляемым к курсовым работам, она допускается к защите, о чем руководитель делает надпись на титульном листе.

4. Защита курсовых работ

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на заседании кафедры, научно-методического семинара кафедры, научной проблемной группы специальной комиссией, состоящей обычно из 3 преподавателей кафедры, при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ могут быть доложены на научных конференциях.

Защита состоит в коротком докладе студента по выполненной работе и в ответах на вопросы присутствующих на защите. Научный руководитель зачитывает отзыв на курсовую работу студента (Приложение Д).

Результаты защиты курсовой работы, согласно действующему Положению о текущем контроле и промежуточной аттестации в СКФУ, оцениваются дифференцированной отметкой по пятибалльной системе. Оценка курсовой работы заносится в зачетную книжку студента и зачетно-экзаменационную ведомость (Приложение Д), составляемую в 2-х экземплярах, один из которых хранится на кафедре в течение всего срока обучения студента, другой представляется в дирекцию факультета.

Защита курсовых работ, предусмотренных учебным планом, проводится не позднее, чем за две недели до начала зачетно-экзаменационной сессии.

Студент, не представивший в установленный срок курсовую работу или не защитивший ее по неуважительной причине, считается имеющим академическую задолженность.

Курсовые работы, представляющие теоретический и практический интерес, следует представлять на конкурс в студенческие научные общества, конференции, отмечать приказом по университету.

Выполненные работы после их защиты должны храниться на кафедре в течение 2 лет, не считая года написания, затем работы, не представляющие для кафедры интерес, уничтожаются по акту.

Итоги выполнения курсовых работ ежегодно обсуждаются на кафедрах и по мере необходимости на

Ученых советах факультетов, а в отдельных случаях и на заседаниях Ученого Совета университета.

Приложение А

(обязательное)

УТВЕРЖДАЮ
Заведующий кафедрой организации и технологии защиты информации канд. техн. наук, доцент
_____ В.И. Петренко
« 10 » сентября 2026 г.

Факультет	математики и компьютерных наук имени профессора Н.И. Червякова
Кафедра	Организации и технологии защиты информации
Направление	Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации

ЗАДАНИЕ
на курсовую работу

студента Перевязки Владислава Сергеевича
(фамилия, имя, отчество)
по дисциплине Защищенные информационные системы

1. Тема работы Разработка проекта системы охранно-пожарной сигнализации офиса
2. Цель
3. Задачи
4. Перечень подлежащих разработке вопросов:
а) по теоретической части
б) по аналитической части

5. Исходные данные:

а) по литературным источникам

б) по вариантам, разработанным преподавателем

в) иное

6. Список рекомендуемой литературы

7. Контрольные сроки представления отдельных разделов курсовой работы:

25 % - “ 28 ” сентября 2020г.

50 % - “ 11 ” октября 2020 г.

75 % - “ 18 ” октября 2020 г.

100 % - “ 01 ” ноября 2020 г.

8. Срок защиты студентом курсовой работы “05” ноября 2026 г.

Дата выдачи задания “ 10 ” сентября 2026 г.

Руководитель курсовой работы

кандидат. техн. наук, доцент. _____ Р.Ю. Стадников

(ученая степень, звание) *(личная подпись)* *(инициалы, фамилия)*

Задание принял(а) к исполнению студент(ка) очной формы обучения

1 курса ИНБ-м-о-13-1 группы _____ В.С. Перевязко

(личная подпись) *(инициалы, фамилия)*

Приложение Б

(обязательное)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК ИМЕНИ ПРОФЕССОРА Н.И. ЧЕРВЯКОВА

КУРСОВАЯ РАБОТА

по дисциплине
«Защищенные информационные системы»
на тему:
«РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ОФИСА»

Выполнил:
Перевязка Владислав Сергеевич
студент 1 курса группы ИНБ-м-о-26-1
направления «Информационная безопасность»
очной формы обучения
_____
(подпись)

Руководитель работы:
Стадников Роман Юрьевич
кандидат техн. наук,
доцент кафедры ОТЗИ

Работа допущена к защите_____ _____
(подпись руководителя) (дата)
Работа выполнена и
защищена с оценкой _____ Дата защиты_____

Члены комиссии: _____ _____ _____
_____ _____ _____
_____ _____ _____
(должность) (подпись) (И.О. Фамилия)

Ставрополь, 2026 г.

Приложение В

(обязательное)

Содержание

Приложение Г

(обязательное)

Список использованных источников

В.1 Нормативно-руководящие документы

1 ГОСТ Р 51275-99. Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения. – Введ.01.01.2000. – М.: Изд.стандартов, 2012.

2 ГОСТ Р 50739-95. Средства Вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введ.01.01.96. – М.: Изд.стандартов, 2012.

В.2 Книги с различным количеством авторов:

- количество авторов не более трех:

3 Завгородний В.А. Комплексная защита информации в компьютерных системах. – М.: Логос, 2013. – 264 с.

- количество авторов не более четырех:

4 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. – 336 с.

- количество авторов более четырех:

5 Сотрудничество /И.И.Иванов,П.П.Петров,С.С.Сидоров и др:АН СССР. ИПМ. – Киев; Наук.думка, 2016. – 270 с.

В.3 Тезисы доклада, сообщения, доклад, другие материалы совещаний (конференций)

6 Росенко А.П., Евстафиади С.П., Феник Е.В. Структура Нейросетевой экспертной системы защиты информации // Сборник трудов научно-практической конференции «Проблемы физико-математических наук». Материалы 48 научно-методической конференции «Университетская наука – региону» – Ставрополь: Изд-во СГУ, 2013. – С.199–202.

В.4 Статьи из журналов и периодических сборников, продолжающихся сборников, ежегодников:

- статья в книге и сборнике:

7 Соколов Н.В., Шангин А.П. Защита информации в компьютерных сетях и системах. – М.: ДМК, 2012. – С.234–256.

- статья на депоненте:

8 Лисипин Л.Г., Медведев А.И. Определение характеристик/ ЦНИИ. –М., 1933. –18 с. –Деп.в ЦНИИНТИ 27.02.03; № 13924.

В.5 Источники из Интернета

9 Сердюк В.А. Новое поколение систем обнаружения и предотвращения информационных атак. – http://www.infoforum.ru/.

Приложение Д

(обязательное)

Отзыв

на курсовую работу студента/ки ___курса

Ф.И.О.

тема

Актуальность: курсовая работа посвящена ……

В первой главе ….

Вторая глава ….

Выводы, сделанные в Заключении, соответствуют целям, поставленным во Введении.

Проанализирован ….объем литературы…

За время работы студент/ка проявил/а себя как…..

Таким образом, работа выполнена на … уровне, соответствует требованиям, предъявляемым к курсовым работам, и заслуживает … оценки.

Научный руководитель
степень, звание, должность
место работы Ф.И.О.

Печать

"…."……..202…г.