Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«12» 12 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.03.01 Эксплуатация объектов сетевой инфраструктуры
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «21» 11 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по выполнению практических работ предназначены для организации работы на практических занятиях по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 3.1 Осуществлять проектирование сетевой инфраструктуры

ПК 3.2 Обслуживать сетевые конфигурации программно-аппаратных средств

ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры

ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем

В рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры» позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры».

Рабочая тетрадь по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры» имеют практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками и выставляются в журнале теоретического обучения.

1. Перечень практических работ
по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 3.1. Эксплуатация технических средств сетевой инфраструктуры	– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – осуществлять диагностику и поиск неисправностей всех компонентов сети; – выполнять действия по устранению неисправностей	ОК 1- 9 ПК 3.1, ПК 3.2, ПК 3.4, ПК 3.5	Практическая работа № 1 Оконцовка кабеля витая пара	2
			Практическая работа № 2 Заделка кабеля витая пара в розетку	2
			Практическая работа № 3 Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену	2
			Практическая работа № 4 Тестирование кабеля	2
			Практическая работа № 5 Поддержка пользователей сети.	2
			Практическая работа № 6 Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	2
			Практическая работа № 7 Выполнение действий по устранению неисправностей	2
			Практическая работа № 8 Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	2
			Практическая работа № 9 Оформление технической документации, правила оформления документов	2
			Практическая работа № 10 Протокол управления SNMP	2
			Практическая работа № 11 Основные характеристики протокола SNMP	2
			Практическая работа № 12 Набор услуг (PDU) протокола SNMP	2
			Практическая работа № 13 Формат сообщений SNMP	2
			Практическая работа № 14 Задачи управления: анализ	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			производительности сети	
			Практическая работа № 15 Задачи управления: анализ надежности сети	2
			Практическая работа № 16 Управление безопасностью в сети.	2
			Практическая работа № 17 Учет трафика в сети	2
			Практическая работа № 18 Средства мониторинга компьютерных сетей	2
			Практическая работа № 19 Средства анализа сети с помощью команд сетевой операционной системы	2
			Практическая работа № 20 Эксплуатация объектов сетевой инфраструктуры	2
Тема 3.2. Эксплуатация систем IP-телефонии	– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – осуществлять диагностику и поиск неисправностей всех компонентов сети; – выполнять действия по устранению неисправностей	ОК 1- 9 ПК 3.1, ПК 3.2, ПК 3.4, ПК 3.5	Практическая работа № 21 Настройка аппаратных IP-телефонов	2
			Практическая работа № 22 Настройка программных IP-телефонов, факсов	2
			Практическая работа № 23 Развертывание сети с использованием VLAN для IP-телефонии	2
			Практическая работа № 24 Настройка шлюза	2
			Практическая работа № 25 Установка, подключение и первоначальные настройки голосового маршрутизатора	2
			Практическая работа № 26 Настройка таблицы пользователей в голосовом маршрутизаторе	2
			Практическая работа № 27 Настройка групп в голосовом маршрутизаторе	2
			Практическая работа № 28 Настройка таблицы маршрутизации вызовов в голосовом	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			маршрутизаторе	
			Практическая работа № 29 Настройка голосовых сообщений в маршрутизаторе	2
			Практическая работа № 30 Настройка программно-аппаратной IP-АТС	2
			Практическая работа № 31 Установка и настройка программной IP-АТС	2
			Практическая работа № 32 Тестирование кодеков. Исследование параметров качества обслуживания	2
			Практическая работа № 33 Мониторинг и анализ соединений по различным протоколам	2
			Практическая работа № 34 Мониторинг вызовов в программном коммутаторе	2
			Практическая работа № 35 Создание резервных копий баз данных	2
			Практическая работа № 36 Диагностика и устранение неисправностей в системах IP-телефонии	2
			Практическая работа № 37 Эксплуатации систем IP-телефонии	2
Тема 3. 3. Инвентаризация технических средств сетевой инфраструктуры, замена расходных материалов и мелкий ремонт периферийного оборудования	– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – осуществлять диагностику и поиск неисправностей всех компонен-	ОК 1- 9 ПК 3.1, ПК 3.2, ПК 3.4, ПК 3.5	Практическая работа № 38 Обследование и модернизация сетевой инфраструктуры	2
			Практическая работа № 39 Замена расходных материалов и мелкий ремонт периферийного оборудования	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
	тов сети; – выполнять действия по устранению неисправностей			

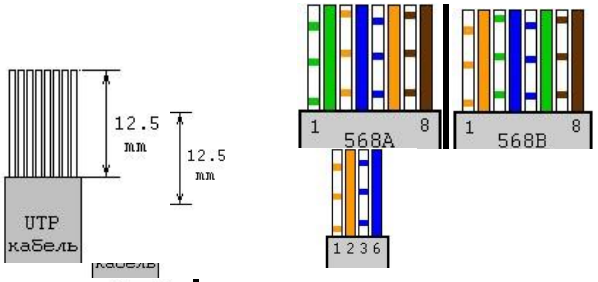
,

2. Описание порядка выполнения практических работ

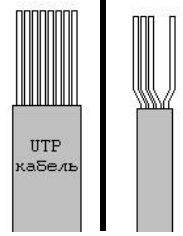
2.1. Практическая работа № 1
Оконцовка кабеля витая пара

Задание:

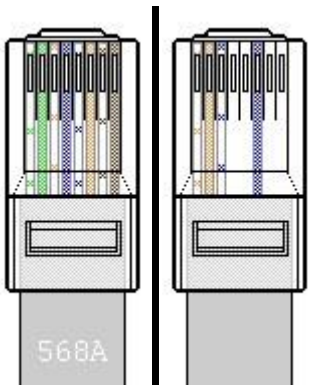
1. Удалите внешнюю оболочку кабеля, на длину 12,5 мм (1/2 дюйма). В обжимном инструменте имеется специальный нож и ограничитель для этой операции.



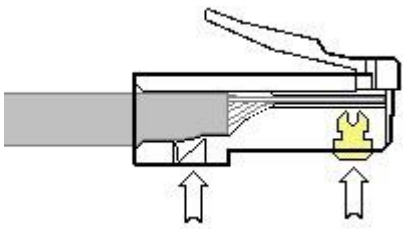
2. Провода зачищать не надо

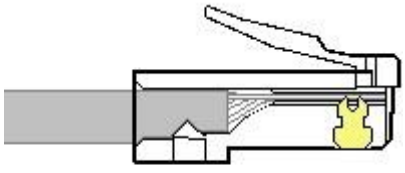


3. Расплетите кабель и расположите провода в соответствии с выбранной вами схемой заделки, причем длина расплетения не должна превышать 12,5 мм.



4. Поверните вилку контактами к себе, как на рисунке, и аккуратно надвиньте на кабель до упора, чтобы провода прошли под контактами.





5. Вилка, с кабелем внутри.
6. Обожмите вилку.

На обжимном инструменте имеется специальное гнездо, в которое вставляется вилка с проводами. И нажатием на ручки инструмента, обжимается.

7. При этом контакты будут утоплены внутрь корпуса и прорежут изоляцию проводов. Фиксатор провода также должен быть утоплен в корпус.

8. Проверить работоспособность кабеля, подключив к компьютеру.

9. Сделайте вывод по работе.

2.2. Практическая работа № 2
Заделка кабеля витая пара в розетку

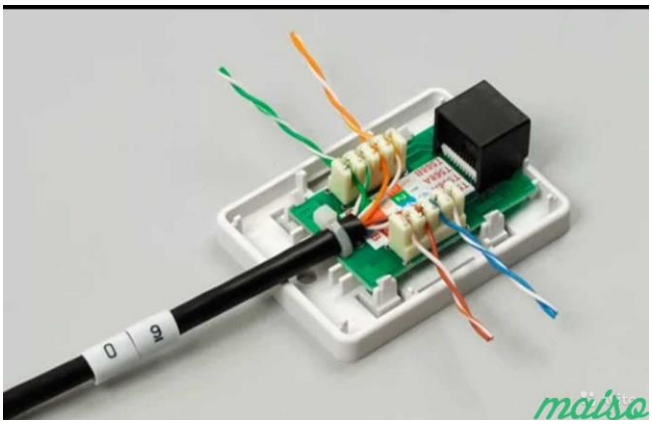
a. Разобрать розетку (рис.1)

.

Рис.1. Состовляющие элементы розетки.

b. Взять телекоммуникационный кабель (с одного конца заделан в патч-панель или разъем RJ-45). c. Разделить проводники по цветовым парам. d. Взять розетку RJ45. e. Разложите витые пары на ножах модуля розетки, сохраняя максимальную целостность свития, согласно указанной на нем цветовой маркировке (рис.1). Стандарт EIA/TIA 568, спецификация EIA/TIA 568B. Рис.1. Раскладка проводников по спецификации EIA/TIA 568B

Б/О Б/С
О С
Б/З Б/К
З К



f. С помощью устройства для заделки витой пары с ударным эффектом Punch Down Tool AMP (кроссовый нож) заделать проводники в розетке AMP.Для этого надавите на проводники до упора. При этом нож модуля прорезает изоляцию и врезается в металл жилы, что гарантирует надежный контакт.

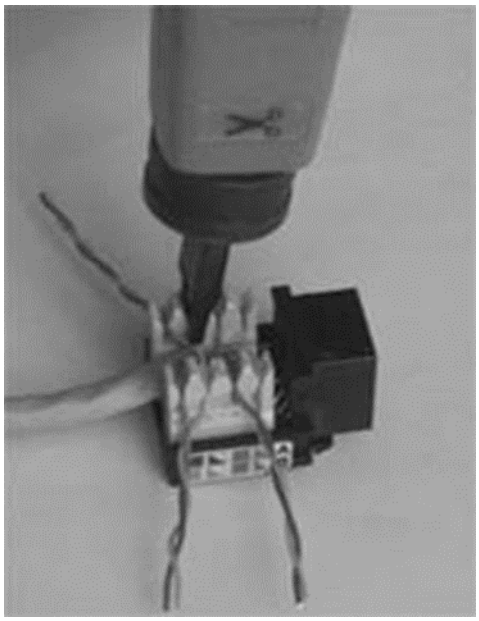


Рис.2. Punch Down Tool AMP

Концы проводников обрезаются одновременно с их заделыванием при помощи Punch Down Tool AMP.

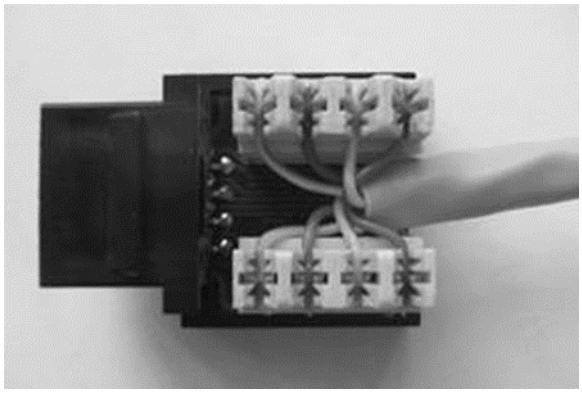


Рис.3. Смонтированная розетка

g. Взять LAN-TESTER Master TX. h. Взять готовый тестовый патч-кордь, закрепить разъем RJ-45 в соответствующем разъеме LAN-TESTER Master TX. Противоположный конец кабеля закрепить в обжатом гнезде (Джеке) розетки. i. Взять LAN-TESTER Remote RX. j. Взять тестовый кабель горизонтальной подсистемы, заделанный с одного конца в Джек розетки, а с другого в патс-панель. Найти по маркеровке кабеля соотствующий разъем патч-панели RJ-45 со стороны ”стены” и соответствующее маркировке гнездо панели RJ-45. Вставить в RJ-45 гнездо панели один конец второго тестового патч-корда , закрепить второй конец этого патч-корда в соответствующем разъеме LAN-TESTER Remote RX. k. Включить LAN-TESTER Master TX, нажав кнопку включения TEST, расположенную на левой боковой стороне корпуса. l. Проверить наличие сигнала по каждому из восьми пинов. Для этого взять LAN-TESTER Remote RX и проверить наличие световых сигналов на каждом из пинов в соответствующем порядке от 1 до 8. m. В случае отсутствия сигнала на каком-либо из пинов повторить обжим Джека розетки RJ-45. В случае, если сигнал все равно отсутствует, еще раз переделать джек.

2.3. Практическая работа № 3
Кроссирование и монтаж патч-панели в коммутаци-онный шкаф, на стену

Задание:

1. Подготовительные работы

Для начала работ необходимо подготовить патч-панель, инструменты и материалы для монтажа — устройство для зачистки витой пары, ударный инструмент для заделки в кросс, кусачки, стяжки и элементы маркировки.

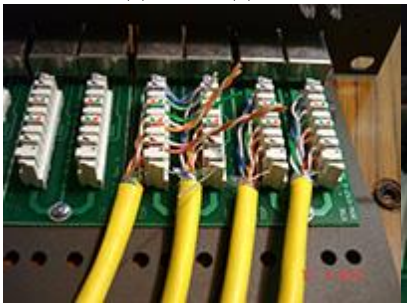
Для более качественной укладки кабеля лучше использовать патч-панель с задним органайзером. Также для удобства коммутации и дальнейшего администрирования рекомендуется использовать держатели кабеля — горизонтальные и вертикальные организаторы. Количество органайзеров выбирается до работ по монтажу ЛВС, исходя из числа портов и наличия другого активного сетевого оборудования.

Предварительно необходимо выбрать место расположения патч-панели в стойке или шкафу и продумать варианты укладки кабельного жгута и монтажа патч-панели.

2. Снятие верхней оболочки кабеля


На этом этапе используется отрегулированный под данный тип кабеля инструмент для зачистки витой пары.
Удалять оболочку кабеля следует не более чем на 30-40 мм. Выполните кольцевую подрезку кабеля, повернув инструмент на 360 градусов вокруг кабеля, и удалите оболочку. Нож инструмента должен полностью прорезать внешнюю оболочку кабеля, не задев изоляцию проводников.

3. Раскладка и заделка кабеля в патч-панели




Заведите жилы обрезанного кабеля на контакты патч-панели в соответствии с цветовой маркировкой портов и выбранным стандартом T568A или T568B. Снимать изоляцию жил не требуется, также важно сохранять целостность свития пар.
С помощью ударного инструмента для заделки забиваем жилы в контактный модуль. При этом нож модуля прорезает изоляцию и врезается в контакт жилы, обеспечивая надежный контакт. Устройство заделки также может содержать в себе нож для автоматической обрезки жил.
Не забудьте закрепить кабели при помощи стяжек, тем самым обеспечив надежную фиксацию и защиту от натяжения и перегибов. Услуга аудита сети поможет выявить все недочеты, сделанные в процессе монтажных работ.

4. Результат смонтированной патч-панели
После монтажа всех кабелей необходимо их аккуратно сгруппировать и закрепить пластиковыми стяжками.
Установите патч-панель в 19" стойку или шкаф. Выполните сертификацию СКС на соответствие категории.



2.4. Практическая работа № 4
Тестирование кабеля

Задание:

1. Проверка кабеля Ethernet с помощью петлевой заглушки

- Подключите петлевую заглушку к одному концу соединителя.
- Вставьте один конец кабеля Ethernet в другой конец соединителя.
- Включите концентратор или коммутатор.
- Вставьте другой конец кабеля Ethernet в порт на концентраторе или коммутаторе.

Загорелся ли индикатор линка на порте после подключения кабеля к порту?
Если индикатор линка не загорелся, проблема в концентраторе или коммутаторе. Если индикатор линка на порте загорелся, кабель прошел проверку целостности.

2. Кабельный тестер

Проверка кабелей UTP

1. Подготовка кабельного тестера к работе
Выберите функцию WIRE MAP (схема разводки проводов) на кабельном тестере.
Убедитесь, что следующие параметры (если таковые имеются) настроены правильно.

Параметр тестера	**Требуемые настройки — неэкранированная витая пара (UTP)**
CABLE (КАБЕЛЬ):	UTP
WIRING (ПРОВОДА):	10BASE-T или EIA/TIA 4PR
CATEGORY (КАТЕГОРИЯ):	CATEGORY 5 (КАТЕГОРИЯ 5)

WIRE SIZE (ДИАМЕТР ПРОВОДА):	AWG 24
CALIBRATE TO CABLE (КАЛИБРОВАТЬ ДЛЯ КАБЕЛЯ)?	NO (НЕТ)
BEEPING (СИГНАЛЫ):	ON или OFF (ВКЛ. или ВЫКЛ.)

Настроив прибор, выйдите из режима настройки.

2. Процедура проверки кабелей

Порядок проверки с использованием кабельного тестера Fluke для локальной сети.

- Вставьте один конец кабеля в разъем RJ-45 тестера с маркировкой «UTP/FTP».
- Вставьте другой конец кабеля в розетку RJ-45 соединителя (с маркировкой «LAN Use»).
- Вставьте идентификатор кабеля (с маркировкой «Net Tool») в другой конец соеднителя.

Ко многим кабельным тестерам прилагаются соединитель и идентификатор кабеля.

Соединитель и идентификатор кабеля

3. Использование функции Wire Map (Схема разводки проводов)

Функцию Wire Map (Схема разводки проводов) и идентификатор кабеля можно использовать для определения прокладки ближнего и дальнего концов кабеля. Один набор номеров, отображаемых на ЖК-экране, соответствует ближнему концу, а другой ряд — дальнему концу.

а. Выполните тест схемы разводки проводов на каждом предоставленном кабеле.

Заполните следующую таблицу на основе результатов проверки каждого кабеля категории 5. Запишите идентификационный номер каждого кабеля и его цвет. Также запишите тип кабеля (прямой или перекрестный), выведенные на экран тестера результаты проверки и описание проблемы.

Номер кабеля	**Цвет кабеля**	**Прямой или перекрестный**	**Отображаемые результаты проверки** (Примечание. Подробное описание результатов теста схемы разводки проводов приведено в руководстве к прибору.)	**Проблема /описание**
			Верхний: Нижний:	
			Верхний: Нижний:	

			Верхний: Нижний:	
			Верхний: Нижний:	
			Верхний: Нижний:	

4. Использование функции определения длины кабелей С помощью функции тестера LENGTH выполните основную проверку ранее использованных кабелей. Внесите в таблицу дополнительную информацию о каждом кабеле.

Номер кабеля	**Длина кабеля**	**Результаты проверки (прошел/не прошел)**

2.5. Практическая работа № 5
Поддержка пользователей сети.

Задание:

1. С разрешения преподавателя включите компьютер, дождитесь завершения загрузки операционной системы Windows (Windows XP, 7).

2. Найдите в вашей сети сетевой адаптер, концентратор (HUB или Switch), модем, волоконнооптический приёмопередатчик, Wi-Fi-роутер, интернет-сервер, файловый сервер, выделенный сервер, рабочую станцию (покажите преподавателю, что вы нашли).

3. Поместите на «Рабочий стол» значок «Сеть» (если его там нет), выполните двойной щелчок по этому значку и ознакомьтесь с содержимым вашей локальной компьютерной сети. Попробуйте определить, какая у вас локальная сеть (по способу взаимодействия компьютеров) – одноранговая или сеть с выделенным сервером?

− *В одноранговой локальной сети все компьютеры равноправны. Общие устройства могут быть подключены к любому компьютеру в сети. Пользователи самостоятельно решают, какие ресурсы своего компьютера (диски, папки, принтеры) сделать доступными для других пользователей сети. Подключенные к сети пользователи могут пользоваться ресурсами компьютера как своими собственными. Основным недостатком таких одно-*

ранговых сетей является слабая защищенность информации от несанкционированного доступа.

- *Если к локальной сети подключено более 10 компьютеров, одноранговая сеть может оказаться недостаточно производительной.*
- *Для увеличения производительности, а также в целях обеспечения большей информационной безопасности один из компьютеров локальной сети может быть выделен в качестве сервера, на котором хранится наиболее важная информация. Правила доступа к этой информации устанавливает один человек – администратор сети.*

Сделайте **Screenshot** (копию экрана) окна «Сетевое окружение» и вставьте его в ваш отчёт.

4. Открывая в окне «Сетевое окружение» папки подключенных к сети ПК, определите, какие ресурсы они предоставляют в совместное использование. Сделайте **Screenshot** окон 2-х папок и вставьте их в ваш отчёт.

5. Выясните, куда входят компьютеры (рабочая группа, домен), определите название рабочей группы или домена, определите имя своего компьютера. Запишите результаты в отчёт. − *свойства папки «Мой компьютер» Имя компьютера.*

6. Определите, есть ли на вашем компьютере сетевые диски и сетевые принтеры.

- ***Сетевые диски*** *— это диски другого компьютера сети, которые данный компьютер воспринимает как своё дополнительное внешнее устройство.*
- ***Сетевые принтеры*** *— это принтеры другого компьютера сети, которые данный компьютер воспринимает как свои дополнительные устройства печати.*

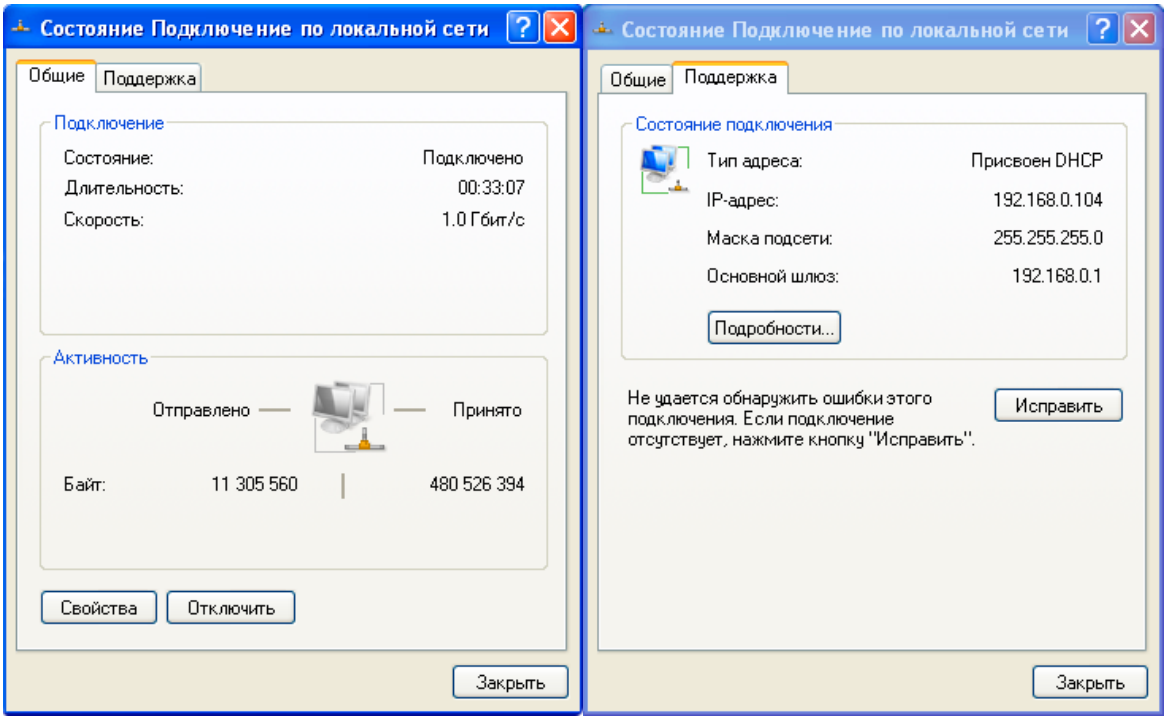
7. Подключите к своему компьютеру сетевой принтер. Какой вид имеет значок сетевого принтера?

- *Найдите в сетевом окружении компьютер преподавателя, выполните двойной щелчок мышью по нему, а затем по значку принтера. Принтер подключится автоматически.*

8. Создайте на сервере, в папке своей группы, которая находится в папке Students, новую папку и назовите её своей фамилией с инициалами, например, Чумак А.А и подключите её к своему компьютеру как сетевой диск. Какой вид имеет значок сетевого диска?

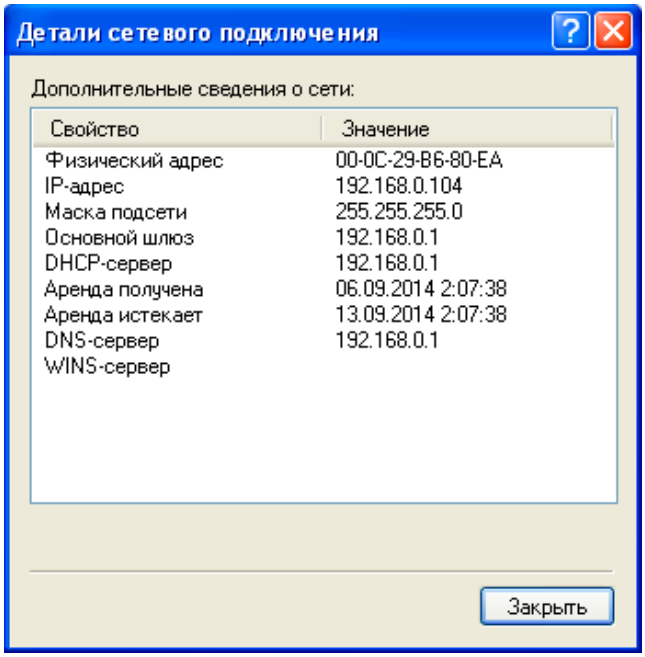
- *Удалить сетевые диски и принтеры можно, воспользовавшись контекстным меню выбранного объекта.*

9. Определите IP адрес вашего персонального компьютера. − *(см. свойства папки Сетевое окружение свойства параметра "Подключение по локальной сети" свойства параметра "Протокол TCP/IP"). Результаты запишите в отчёт. − Можно выполнить двойной щелчок по значку «Сеть» на панели индикации («системный трэй»):*

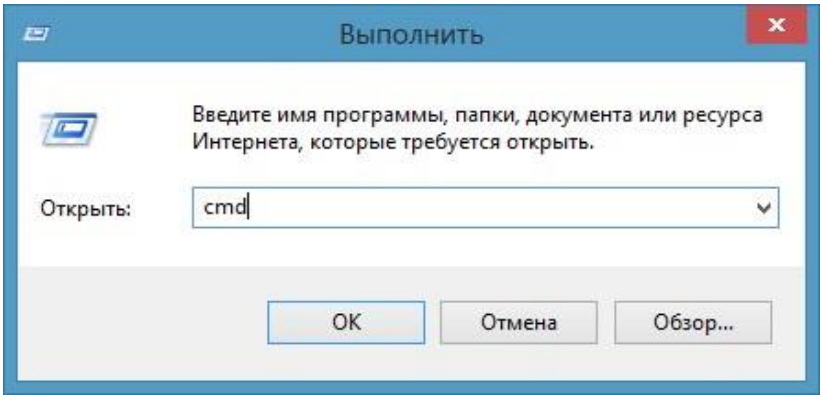


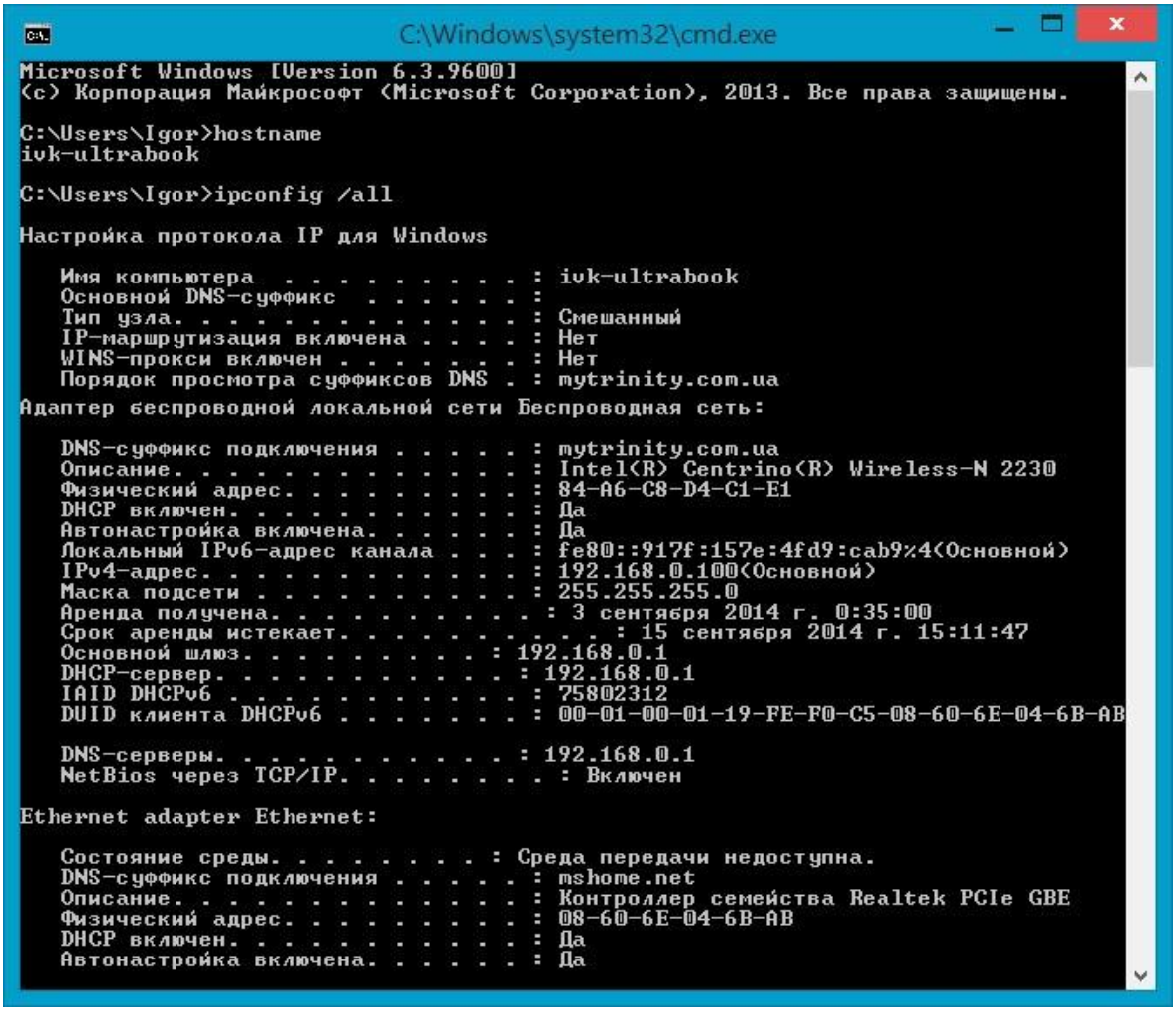
10. Определите физический адрес сетевой карты вашего компьютера

− *В окне «Состояние Подключение по локальной сети» нажмите кнопку «Подробности»:*



− ***Второй способ:*** *в «Главном меню» найдите команду «Выполнить», введите «cmd». Откроется окно командного интерпретатора (режим «ДОС»). Введите в этом окне команду «ipconfig /all» и нажмите «Enter».*





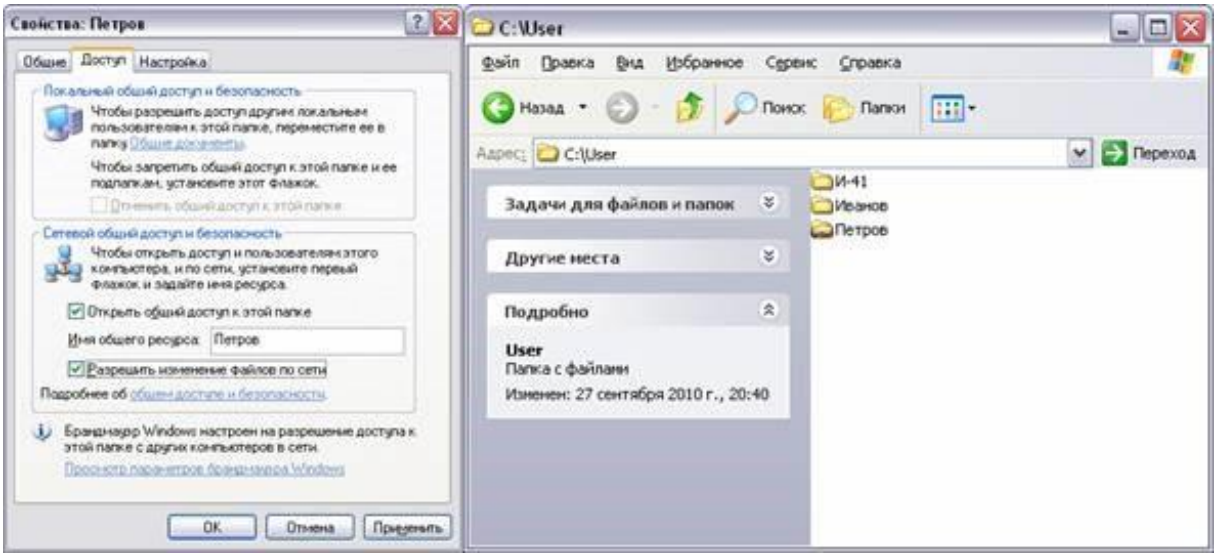
11. Предоставьте в совместное использование свои ресурсы - объявите свой каталог общим, выбрав команду «Доступ» в контекстном меню. − *В папке «Мои документы» создайте каталог с именем, совпадающим с Вашей фамилией.*

− *Задайте тип доступа Полный (команда «Разрешить изменение файлов по сети»).*

− *Обратите внимание на изменение вида значка каталога.*

Сделайте копию экрана и сохраните графический файл с этой копией в этой папке. Обменяйтесь этими файлами с кем-нибудь по сети.

4



12. Сохраните отчёт в СДО

2.6. Практическая работа № 6
Эксплуатация технических средств сетевой инфраструктуры (принтеры, ком-пьютеры, серверы)

Порядок работы

1. Убедитесь в том, что компьютерная система обесточена (при необходимости, отключите систему от сети).
2. Разверните системный блок задней стенкой к себе.
3. По наличию или отсутствию разъемов USB установите форм-фактор материнской платы (при наличии разъемов USB - форм-фактор ATX, при их отсутствии -AT). 4. Установите местоположение и снимите характеристики следующих разъемов:
   - питания системного блока;
   - питания монитора;
   - сигнального кабеля монитора;
   - клавиатуры;
   - последовательных портов; • параллельного порта (если есть);
   - других разъемов.
5. Убедитесь в том, что все разъемы, выведенные на заднюю стенку системного блока, не взаимозаменяемы, то есть каждое базовое устройство подключается одним единственным способом.
6. Изучите способ подключения мыши.
7. Заполните таблицу:

Разъем	Тип разъема	Количество контактов	Примечания

8. Определить наличие основных устройств персонального компьютера.
9. Установите местоположение блока питания, выясните мощность блока питания (указана на ярлыке).
10. Установите местоположение материнской платы.
11. Установите характер подключения материнской платы к блоку питания.
12. Установите местоположение жесткого диска.

Установите местоположение его разъема питания. Проследите направление шлейфа проводников, связывающего жесткий диск с материнской платой.

13. Установите местоположение платы видеоадаптера.
14. При наличии прочих дополнительных устройств выявите их назначение, опишите характерные особенности данных устройств (типы разъемов, тип интерфейса и др.).
15. Заполните таблицу:

Устройство	Характерные особенности	Куда и при помощи чего подключается

2.7. Практическая работа № 7
Выполнение действий по устранению неисправностей

Классификация неисправностей АПС

Для выбора метода диагностики и определения первичных и вторичных симптомов отказа необходимо уметь классифицировать неисправность, т. к. первичный отказ часто вызывает целый спектр отказов вторичных, являющихся следствием первичного и затеняющих причину неисправности.

Предлагаемая классификация охватывает ошибки и отказы, вызванные электронными узлами *системной платы*, как наиболее сложной части PC, и может быть распространена на весь клон IBM PC.

С позиции аппаратных и программных средств, используемых в PC, неисправности подразделяются на аппаратные, программные и аппаратно-программные.

Аппаратные неисправности, т. е. неисправности аппаратных средств, в свою очередь, подразделяются на случайные, мягкие и жесткие ошибки.

К **случайным** ошибкам относят:

1) плавающие ошибки;
2) корректируемые отказы;
3) некорректируемые отказы (технические остановы).

Потенциально, любая неисправность, связанная со случайными ошибками, может привести к жесткой ошибке. Случайная ошибка, приобретшая фактор стабильности и делающая невозможной дальнейшую эксплуатацию системы классифицируется как жесткая, не корректируемая и требует анализа и диагностики неисправности АПС. Нередко, после коррекции условий эксплуатации ВС (температурно-климатические, вибрационные и т. д.), такие ошибки исчезают, но, по истечении некоторого времени, появляются снова. Таким образом, это – не метод устранения ошибок, и задача инженера или техника по ТО – наоборот, *ужесточить условия эксплуатации ВС на время диагностики,* с целью выявления ошибки и выделения отказавшего узла. Наиболее неприятны отказы, связанные с факторами нестабильности и неопределенности – плавающие ошибки.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Запустить программу Everest на тестируемом компьютере и с помощью мастера отчетов (меню «Отчёт») сформировать отчет об аппаратном обеспечении.
3. Заполнить табл. 1.

1. Результаты выполнения работы

№	Наименование компонента системного блока или характеристика	Найденное обозначение или характеристика
1	Тип ЦП, частота	
2	Тип системной платы, форм-фактор	
3	Чипсет системной платы	
4	Тип жесткого диска, объем	
5	Тип сетевого адаптера	
6	Тип видеоадаптера	
7	Тип звукового адаптера	
8	Разъемы ОЗУ	
9	Разъемы расширения системной платы	
10	Объем кэш-памяти процессора	

2.8. Практическая работа № 8
Выполнение мониторинга и анализа работы локальной сети с помощью программ-ных средств.

Задание:

1. Проверка знакомства с процессом наблюдения за сетью

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

2: Изучение средств мониторинга сети
Проведите исследование и найдите три средства мониторинга сети.
Перечислите эти три найденных средства.
Заполните следующую форму для выбранных средств мониторинга сети.

Поставщик	Название продукта	Функциональные возможности

3: Выберите средство мониторинга сети
1: Выберите одно или несколько средств мониторинга из исследования.
Укажите одно или несколько средств из исследования, которые бы вы выбрали для мониторинга сети. Назовите эти средства и объясните свой выбор, перечислив конкретные функциональные возможности, которые по вашему мнению важны.
2: Изучите средство мониторинга сети PRTG.
Перейдите на веб-страницу www.paessler.com/prtg.
В следующих полях приведите примеры некоторых функций PRTG.
3. Какие выводы вы можете сделать на основании проведённого исследования в отношении программного обеспечения для наблюдения за сетью?

2.9. Практическая работа № 9
Оформление технической документации, правила оформления документов

Полное наименование изделия на титульном листе, в основной надписи и при первом упоминании в тексте документа должно быть одинаковым с наименованием его в основном конструкторском документе.
В последующем тексте порядок слов в наименовании должен быть прямой, т.е. на первом месте должно быть определение (имя прилагательное), а затем - название изделия (имя существительное); при этом допускается употреблять сокращенное наименование изделия.
Наименования, приводимые в тексте документа и на иллюстрациях, должны быть одинаковыми.
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 документах должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии - общепринятые в научно-технической литературе.

Если в документе принята специфическая терминология, то в конце его (перед списком литературы) должен быть перечень принятых терминов с соответствующими разъяснениями. Перечень включают в содержание документа.

В тексте документа 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 и термины при наличии равнозначных слов и терминов в русском языке;
- применять произвольные словообразования;
- применять сокращения слов, кроме установленных правилами русской орфографии, соответствующими государственными стандартами, а также в данном документе;
- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, и в расшифровках буквенных обозначений, входящих в формулы и рисунки.

В тексте документа, за исключением формул, таблиц и рисунков, не допускается:

- применять математический знак минус (-) перед отрицательными значениями величин (следует писать слово "минус");
- применять знак "Ø" для обозначения диаметра (следует писать слово "диаметр"). При указании размера или предельных отклонений диаметра на чертежах, помещенных в тексте документа, перед размерным числом следует писать знак "Ø";
- применять без числовых значений математические знаки, например > (больше), <(меньше), =(равно), ≥(больше или равно), ≤(меньше или равно), ≠(не равно), а также знаки № (номер), % (процент);
- применять индексы стандартов, технических условий и других документов без регистрационного номера.

Если в документе приводятся поясняющие надписи, наносимые непосредственно на изготовляемое изделие (например на планки, таблички к элементам управления и
т.п.), их выделяют шрифтом (без кавычек), например ВКЛ., ОТКЛ., или кавычками - если надпись состоит из цифр и (или) знаков.

Наименования команд, режимов, сигналов и т.п. в тексте следует выделять кавычками, например, "Сигнал +27 включено".

Перечень допускаемых сокращений слов установлен в ГОСТ 2.316.

Если в документе принята особая система сокращения слов или наименований, то в нем должен быть приведен перечень принятых сокращений, который помещают в конце документа перед перечнем терминов.

Условные буквенные обозначения, изображения или знаки должны соответствовать принятым в действующем законодательстве и государственных стандартах. В тексте документа перед обозначением параметра дают его пояснение, например "Временное сопротивление разрыву $\sigma_в$".

При необходимости применения условных обозначений, изображений или знаков, не установленных действующими стандартами, их следует пояснять в тексте или в перечне обозначений.

В документе следует применять стандартизованные единицы физических величин, их наименования и обозначения в соответствии с ГОСТ 8.417.

Наряду с единицами СИ, при необходимости, в скобках указывают единицы ранее применявшихся систем, разрешенных к применению. Применение в одном документе разных систем обозначения физических величин не допускается.

В тексте документа числовые значения величин с обозначением единиц физических величин и единиц счета следует писать цифрами, а числа без обозначения единиц физических величин и единиц счета от единицы до девяти - словами. Примеры

1 Провести испытания пяти труб, каждая длиной 5 м.

2 Отобрать 15 труб для испытаний на давление.

Единица физической величины одного и того же параметра в пределах одного документа должна быть постоянной. Если в тексте приводится ряд числовых значений, выраженных в одной и той же единице физической величины, то ее указывают только после последнего числового значения, например 1,50; 1,75; 2,00 м.

Если в тексте документа приводят диапазон числовых значений физической величины, выраженных в одной и той же единице физической величины, то обозначение единицы физической величины указывается после последнего числового значения диапазона. Примеры:

1. От 1 до 5 мм.
2. От 10 до 100 кг.
3. От плюс 10 до минус 40°С.
4. От плюс 10 до плюс 40°С.

Недопустимо отделять единицу физической величины от числового значения (переносить их на разные строки или страницы), кроме единиц физических величин, помещаемых в таблицах, выполненных машинописным способом.

Приводя наибольшие или наименьшие значения величин, следует применять словосочетание "должно быть не более (не менее)".

Приводя допустимые значения отклонений от указанных норм, требований, следует применять словосочетание "не должно быть более (менее)".

Например, массовая доля углекислового натрия в технической кальцинированной соде должна быть не менее 99,4 %.

Числовые значения величин в тексте следует указывать со степенью точности, которая необходима для обеспечения требуемых свойств изделия, при этом в ряду величин осуществляется выравнивание числа знаков после запятой.

Округление числовых значений величин до первого, второго, третьего и т.д. десятичного знака для различных типоразмеров, марок и т.п. изделий одного наименования должно быть одинаковым. Например, если градация толщины стальной горячекатаной ленты 0,25 мм, то весь ряд толщин ленты должен быть указан с таким же количеством десятичных знаков, например 1,50; 1,75; 2,00.

Дробные числа необходимо приводить в виде десятичных дробей, за исключением

размеров в дюймах, которые следует записывать $^1/_4''$; $^1/_2''$ (но не $\frac{1''}{4}$, $\frac{1''}{2}$).

При невозможности выразить числовое значение в виде десятичной дроби, допускается записывать в виде простой дроби в одну строчку через косую черту, например, 5/32; (50А-4С)/(40В+20).

В формулах в качестве символов следует применять обозначения, установленные соответствующими государственными стандартами. Пояснения символов и числовых коэффициентов, входящих в формулу, если они не пояснены ранее в тексте, должны быть приведены непосредственно под формулой. Пояснения каждого символа следует давать с новой строки в той последовательности, в которой символы приведены в формуле. Первая строка пояснения должна начинаться со слова "где" без двоеточия после него.

Пример - Плотность каждого образца, Pкг/м^3, вычисляют по формуле

$$\rho = \frac{m}{V}, \quad (1)$$

где m - масса образца, кг; V- объем образца, м^3.

Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой.

Переносить формулы на следующую строку допускается только на знаках выполняемых операций, причем знак в начале следующей строки повторяют. При переносе формулы на знаке умножения применяют знак "×".

В документах, издаваемых нетипографским способом, формулы могут быть выполнены машинописным, машинным способами или чертежным шрифтом высотой не менее 2,5 мм. Применение машинописных и рукописных символов в одной формуле не допускается.

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).

Ссылки в тексте на порядковые номера формул дают в скобках, например, ... в формуле (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).

Порядок изложения в документах математических уравнений такой же, как и формул.

Примечания приводят в документах, если необходимы пояснения или справочные данные к содержанию текста, таблиц или графического материала.

Примечания не должны содержать требований.

Примечания следует помещать непосредственно после текстового, графического материала или в таблице, к которым относятся эти примечания, и печатать с прописной буквы с абзаца. Если примечание одно, то после слова "Примечание" ставится тире и примечание печатается тоже с прописной буквы. Одно примечание не нумеруют. Несколько примечаний нумеруют по порядку арабскими цифрами. Примечание к таблице помещают в конце таблицы над линией, обозначающей окончание таблицы. Примеры:

Примечание -

_____

_____ _____

Примечания

1

_____ ___

2

_____ ___

В текстовом документе допускаются ссылки на данный документ, стандарты, технические условия и другие документы при условии, что они полностью и однозначно определяют соответствующие требования и не вызывают затруднений в пользовании документом.

Ссылки на стандарты предприятий (СТП) и другую техническую документацию должны быть оговорены в договоре на разработку изделия.

Ссылаться следует на документ в целом или его разделы и приложения. Ссылки на подразделы, пункты, таблицы и иллюстрации не допускаются, за исключением подразделов, пунктов, таблиц и иллюстраций данного документа.

При ссылках на стандарты и технические условия указывают только их обозначение, при этом допускается не указывать год их утверждения при условии записи обозначения с годом утвер-

ждения в конце текстового документа под рубрикой ’’ССЫЛОЧНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ" по форме:

Обозначение документа, на который дана ссылка	Номер раздела, подраздела, пункта, подпункта, перечисления, приложения, разрабатываемого документа, в котором дана ссылка

При ссылках на другие документы в графе "Обозначение документа" указывают также и наименование документа. При ссылках на раздел или приложение указывают его номер.

Задание:
1. Оформить текст используя правила стандартов ЕСКД:

2.10. Практическая работа № 10
Протокол управления SNMP

Для успешного администрирования сети необходимо знать состояние каждого ее элемента с возможностью изменять параметры его функционирования. Обычно сеть состоит из устройств различных производителей и управлять ею было бы нелегкой задачей, если бы каждое из сетевых устройств понимало только свою систему команд. Поэтому возникла необходимость в создании единого языка управления сетевыми ресурсами, который бы понимали все устройства, и который, в силу этого, использовался бы всеми пакетами управления сетью для взаимодействия с конкретными устройствами.

Подобным языком стал SNMP - Simple Network Management Protocol. Разработанный для систем, ориентированных под операционную систему UNIX, он стал фактически общепринятым стандартом сетевых систем управления и поддерживается подавляющим большинством производителей сетевого оборудования в своих продуктах.

В силу своего названия - Простой Протокол Сетевого Управления - основной задачей при его разработке было добиться максимальной простоты его реализации. В результате возник протокол, включающий минимальный набор команд, однако позволяющий выполнять практически весь спектр задач управления сетевыми устройствами - от получения информации о местонахождении конкретного устройства, до возможности производить его тестирование.

Протокол SNMP дает возможность администраторам управлять узлами, такими как серверы, рабочие станции, маршрутизаторы, коммутаторы и устройства безопасности в сети IP. Он позволяет сетевым администраторам контролировать работу сети, выполнять поиск и разрешение сетевых проблем, а также планировать рост сети.

Сегодня SNMP является самым популярным протоколом управления различными коммерческими, университетскими и исследовательскими объединенными сетями.

Применяют SNMP для:

- Получение информации о состоянии сетевого оборудования
- Локализация неполадок в сети
- Удаленное управление узлами сети
- Сбор статистической информации о состоянии сети
- Возможно применение протокола SNMP в областях, не связанных с сетевыми технологиями:
  - Проекты по использованию SNMP в системах управления светофорами
  - Производства, имеющие сеть измерительных приборов, разбросанных географически, нуждающиеся в мониторинге состояния и показаний этих приборов

Основные преимущества протокола SNMP:

- простота;
- доступность;
- независимость от производителей.

Основной концепцией протокола является то, что вся необходимая для управления устройством информация хранится на самом устройстве - будь то сервер, модем или маршрутизатор - в так называемой Административной Информационной Базе (MIB - Management Information Base - RFC 1213).

Применяются базы управляющей информации (MIB) для упрощения. запоминания адреса объектов устройств, определяемых в цифровом формате. Базы MIB описывают структуру управляемых данных на подсистеме устройства; они используют иерархическое пространство имен, содержащее идентификаторы объектов (OID-ы). Каждый OID состоит из двух частей: текстового имени и SNMP адреса в цифровом виде. Базы MIB являются необязательными и выполняют вспомогательную роль по переводу имени объекта из человеческого формата (словесного) в формат SNMP (цифровой). Так как структура объектов на устройствах разных производителей

не совпадает, без базы MIB практически невозможно определить цифровые SNMP адреса нужных объектов.

MIB представляет собой набор переменных, характеризующих состояние объекта управления. Эти переменные могут отражать такие параметры, как количество пакетов, обработанных устройством, состояние его интерфейсов, время функционирования устройства и т.п.

Для того, чтобы проконтролировать работу некоторого устройства сети, необходимо просто получить доступ к его MIB, которая постоянно обновляется самим устройством, и проанализировать значения некоторых переменных.

Модель SNMP состоит из четырех компонентов:

- управляемых узлов;
- станций управления (менеджеров);
- управляющей информации;
- протокола управления.

Агентами в SNMP являются программные модули, которые работают в управляемых устройствах. Агенты собирают информацию об управляемых устройствах, в которых они работают, и делают эту информацию доступной для систем управления сетями (network management systems - NMS) с помощью протокола SNMP.

Управляемое устройство может быть узлом любого типа, находящимся в какой-нибудь сети: это хосты, служебные устройства связи, принтеры, роутеры, мосты и концентраторы, коммутаторы.

При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой системе есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт информацию менеджеру.

Менеджеры SNMP обрабатывают данные о конфигурации и функционировании управляемых систем и преобразуют их во внутренний формат, удобный для поддержания протокола SNMP. Протокол также разрешает активные задачи управления, например, изменение и применение новой конфигурации через удаленное изменение этих переменных. Доступные через SNMP переменные организованы в иерархии. Эти иерархии, как и другие метаданные (например, тип и описание переменной), описываются базами управляющей информации (базы MIB, от англ. Management information base).

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

- Управляемое устройство;
- Агент — программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства;
- Система сетевого управления (Network Management System, NMS) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети.

Управляемое устройство — элемент сети (оборудование или программное средство), реализующий интерфейс управления (не обязательно SNMP), который разрешает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютеры-хосты, принтеры и т. п.

Агентом называется программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства. Агент обладает локальным знанием управляющей информации и переводит эту информацию в специфичную для SNMP форму или из неё (медиация данных).

В состав системы сетевого управления (*NMS*) входит приложение, отслеживающее и контролирующее управляемые устройства. NMS обеспечивают основную часть обработки данных, необходимых для сетевого управления. В любой управляемой сети может быть одна и более NMS.

Детали протокола

SNMP работает на прикладном уровне TCP/IP (седьмой уровень модели OSI). Агент SNMP получает запросы по UDP-порту 161. Менеджер может посылать запросы с любого доступного порта источника на порт агента. Ответ агента будет отправлен назад на порт источника на менеджере. Менеджер получает уведомления (Traps и InformRequests) по порту 162. Агент может генерировать уведомления с любого доступного порта. При использовании TLS или DTLS запросы получаются по порту 10161, а ловушки отправляются на порт 10162.

В SNMPv1 указано пять основных протокольных единиц обмена (protocol data units — PDU). Еще две PDU, GetBulkRequest и InformRequest, были введены в SNMPv2 и перенесены в SNMPv3.

Все PDU протокола SNMP построены следующим образом:

IP header (IP-заголовок)	UDP header (UDP-заголовок)	version (версия)	community (пароль)	PDU-type (PDU-тип)	request-id (id запроса)	error-status (статус ошибки)	error-index (индекс ошибки)	variable bindings (связанные переменные)

Существует семь протокольных единиц обмена SNMP, из которых два основных:

GetRequest

Запрос от менеджера к объекту для получения значения переменной или списка переменных. Требуемые переменные указываются в поле variable bindings (раздел поля values при этом не используется). Получение значений указанной переменной должно быть выполнено агентом как *Атомарная операция* (операции, выполняющиеся как единое целое, либо не выполняющиеся вовсе.). Менеджеру будет возвращен Response (ответ) с текущими значениями.

SetReques

Запрос от менеджера к объекту для изменения переменной или списка переменных. Связанные переменные указываются в теле запроса. Изменения всех указанных переменных должны быть выполнены агентом как атомарная операция. Менеджеру будет возвращен Response с (текущими) новыми значениями переменных.

Ловушки агента SNMP

NMS периодически проводит опрос агентов SNMP, размещенных на управляемых устройствах, запрашивая данные у устройства с помощью запроса get. С помощью этого процесса приложение для управления сетями может собирать информацию для мониторинга транспортной нагрузки и проверять настройки управляемых устройств. Информация может отображаться через графический интерфейс пользователя в системе NMS. Можно вычислить минимальные, средние и максимальные значения, создать графическое представление данных или установить пороговые значения, при превышении которых будут отправляться соответствующие уведомления. Например, система NMS может контролировать использование центрального процессора маршрутизатора Cisco. Диспетчер SNMP осуществляет периодическую выборку значений и представляет эту информацию в графическом виде, чтобы сетевой администратор могу использовать её для вычисления базовых показателей.

Периодический опрос SNMP имеет свои недостатки. Во-первых, существует задержка между временем обнаружения события и временем отправки соответствующего уведомления (путём опроса) системой NMS. Во-вторых, существует компромисс между частотой опроса и использованием пропускной способности.

Чтобы смягчить воздействие этих недостатков, агенты SNMP могут создавать и отправлять ловушки, сообщая системе NMS о некоторых событиях немедленно. Ловушки — это незапрашиваемые сообщения, предупреждающие диспетчера SNMP о каком-либо условии или событии в сети. Примерами условий ловушек, помимо прочего, являются следующие: неправильная аутентификация пользователей, перезапуски, изменение состояния канала (на активное или неактивное), отслеживание MAC-адресов, закрытие подключения TCP, потеря подключения к соседнему узлу или другие важные события. Уведомления, направленные на ловушки, помогают сократить использование ресурсов сети и агентов, устраняя необходимость в некоторых запросах на опрос SNMP.

Версии SNMP

Существует несколько версий SNMP, включая следующие:

SNMPv1 — простой протокол управления сетями, полноценный стандарт Интернета, описанный в документе RFC 1157.

SNMPv2c — описан в серии документов RFC 1901—1908; использует среду администрирования на базе строки сообщества.

SNMPv3 — обеспечивающий взаимодействие протокол на основе стандартов, первоначально определённый в серии документов RFC 2273—2275; обеспечивает защищённый доступ к устройствам с помощью аутентификации и шифрования пакетов в сети. Данная версия протокола включает следующие функции обеспечения безопасности: контроль целостности сообщений для защиты пакетов от искажения при пересылке; аутентификация для подтверждения достоверности источника сообщения и шифрование для предотвращения прочтения содержимого сообщения несанкционированным источником.

В SNMPv1 и SNMPv2c используется модель безопасности на основе сообществ (community). Сообщество диспетчеров, имеющих доступ к базе MIB агента, определяется списком контроля доступа и паролем.

В отличие от SNMPv1, версия SNMPv2c предусматривает механизм массового извлечения записей и более подробное информирование станций управления об ошибках. Механизм массового извлечения получает таблицы и большие объёмы информации, сводя к минимуму затраты времени на двустороннее согласование. Усовершенствованная обработка ошибок в SNMPv2c

предусматривает расширенные коды ошибок для различных условий возникновения ошибок. Эти условия обозначаются одним кодом ошибки в SNMPv1. Коды возврата по ошибке в SNMPv2c включают тип ошибки.

Примечание. SNMPv1 и SNMPv2c включают минимальный набор средств обеспечения безопасности. В частности, SNMPv1 и SNMPv2c не обеспечивают ни аутентификацию источника сообщения управления, ни шифрование. Наиболее обновлённое описание версии SNMPv3 содержится в серии документов RFC 3410—3415. В эту версию протокола добавлены методы обеспечения безопасной передачи наиболее важных данных между управляемыми устройствами.

SNMPv3 предусматривает как модели безопасности, так и уровни безопасности. Модель безопасности — это стратегия аутентификации, настроенная для пользователя и группы, в которой данный пользователь находится. Уровень безопасности характеризует допустимую степень безопасности в модели. Сочетание уровня безопасности и модели безопасности определяет, какой механизм безопасности будет использоваться при обработке пакета SNMP. Доступные модели безопасности — SNMPv1, SNMPv2c и SNMPv3.

Сетевой администратор должен настроить агент SNMP для использования версии SNMP, поддерживаемой станцией управления. Поскольку агент может взаимодействовать с несколькими диспетчерами SNMP, можно настраивать программное обеспечение для поддержки связи с помощью SNMPv1, SNMPv2c или SNMPv3.

6. Порядок выполнения работы

6.1 Собрать схему в соответствии с физической топологией, показанной на рис. 1.

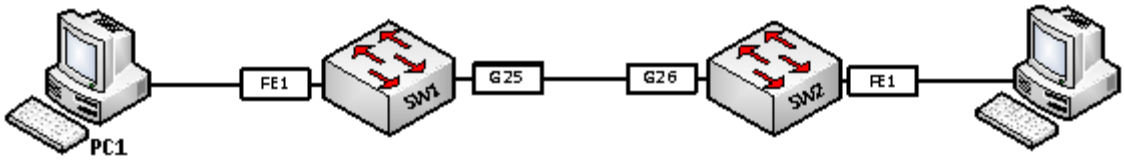


Рисунок 1. (FE1 – Порт Fast Ethernet 1, G25 – Порт Gigabit Ethernet 25).

6.2 Настроить адресацию сети в соответствии с диаграммой сетевого уровня, показанной на рис. 2. Коммутаторы предварительно настроены.

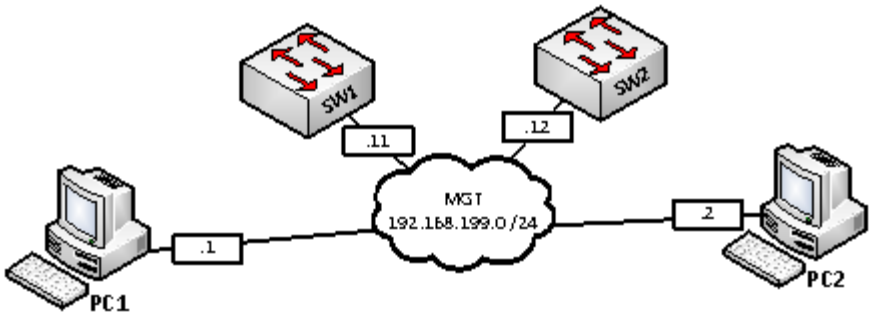


Рисунок 2. Сетевой уровень.

Все устройства в сети должны быть доступны, проверить командой «ping», например с PC1 проверить связь до SW1 командой «ping 192.168.199.11», до SW2 командой «ping 192.168.199.12», до PC2 командой «ping 192.168.199.2», как показано на рис. 3.

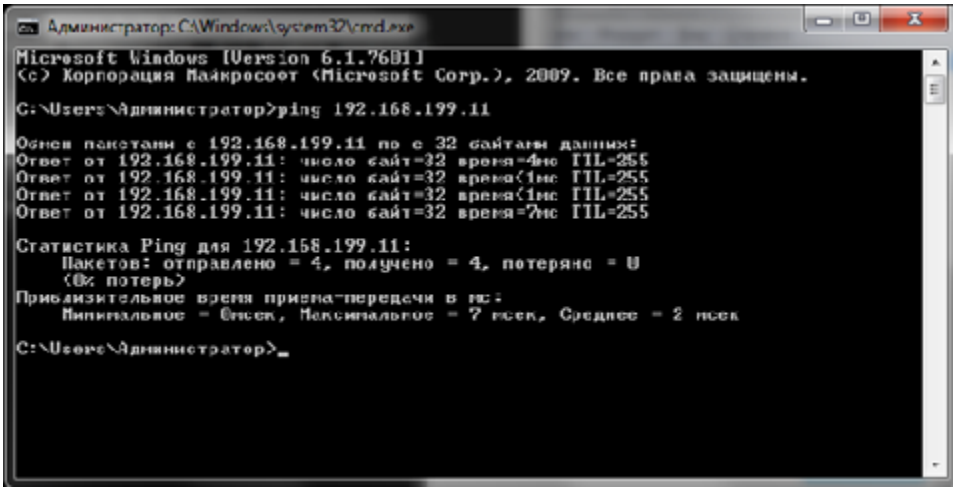
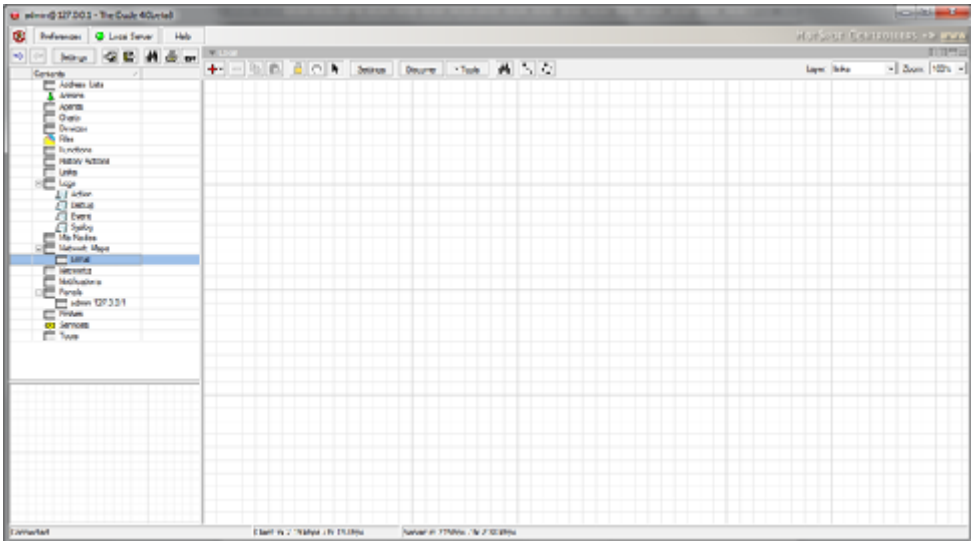
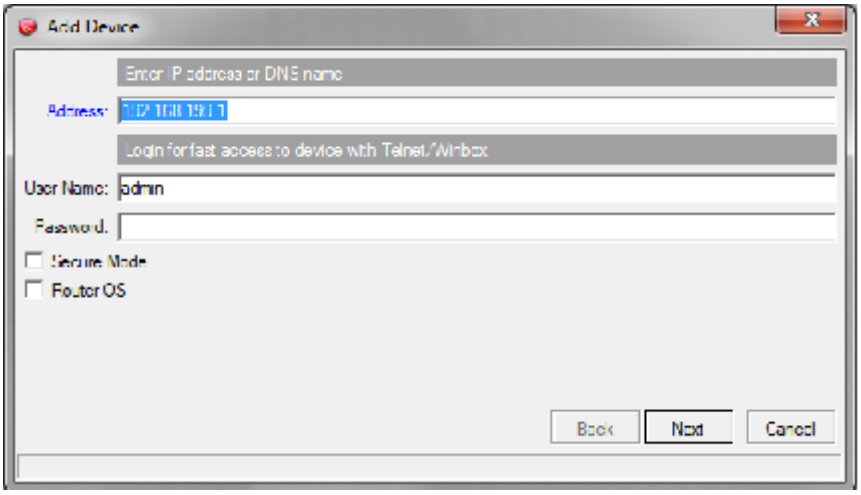


Рисунок 3. Результат проверки связи до SW1.

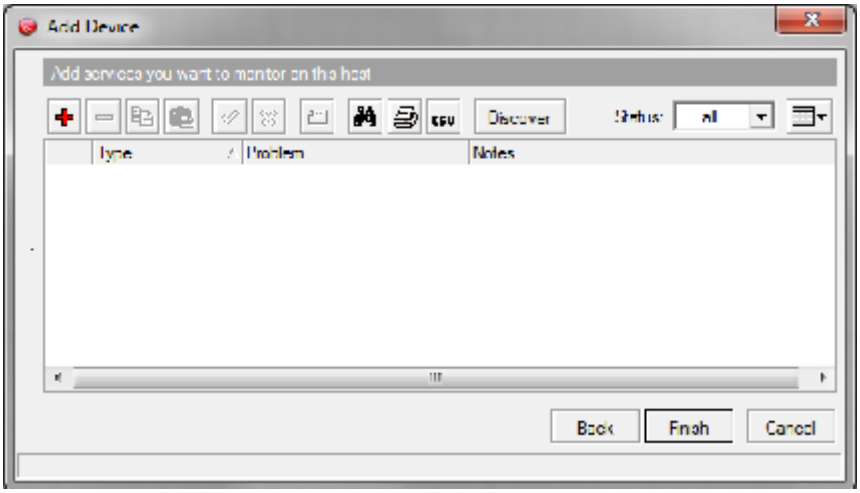
6.3. Произвести настройку SNMP сервера установленного на компьютере, для чего открыть программу «The Dude», в слева в меню выбрать карту сети (Network Maps > Local).



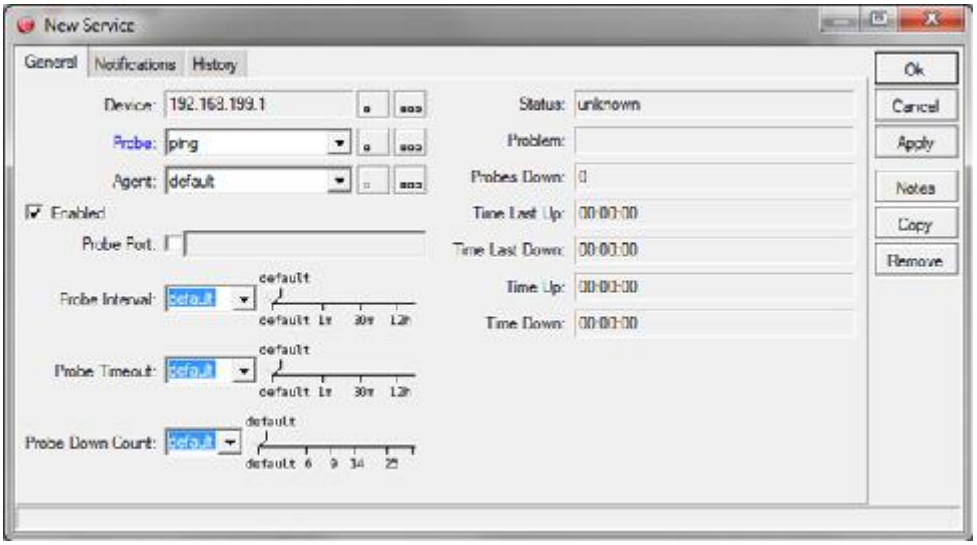
Добавить устройства в соответствии с L1 диаграммой, изображенной на рис. 1. Для этого на панели инструментов нужно нажать красный плюс и выбрать пункт «Device», в открывшемся диалоговом окне ввести IP-адрес нужного устройства и нажать «Next».



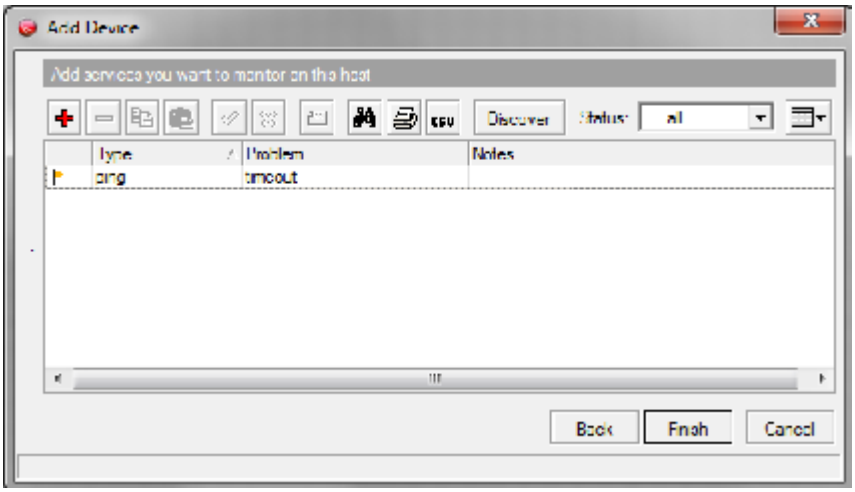
В открывшемся окне выбрать метод проверки работоспособности устройства, для этого нажать красный плюс.



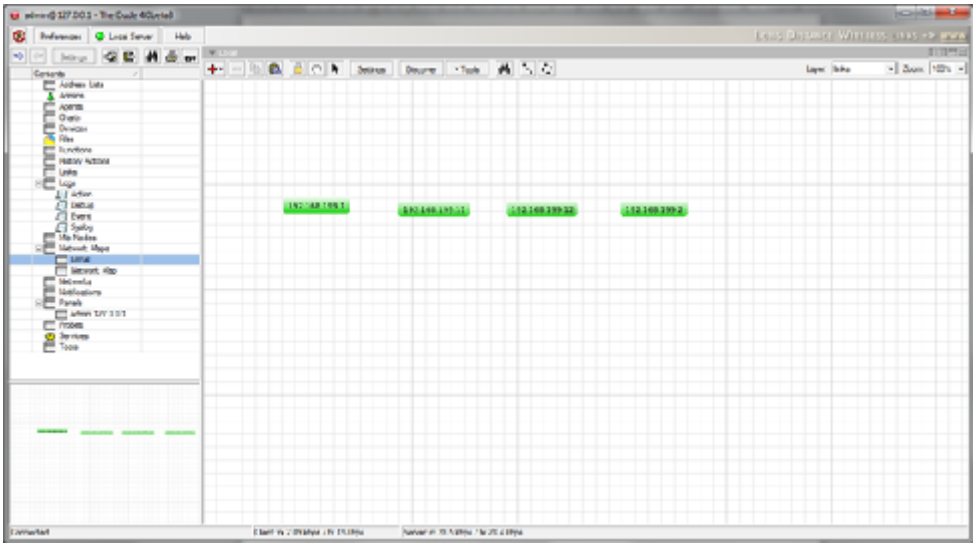
В открывшемся окне из выпадающего списка «Probe» выбрать тип «Ping» и нажать кнопку OK.



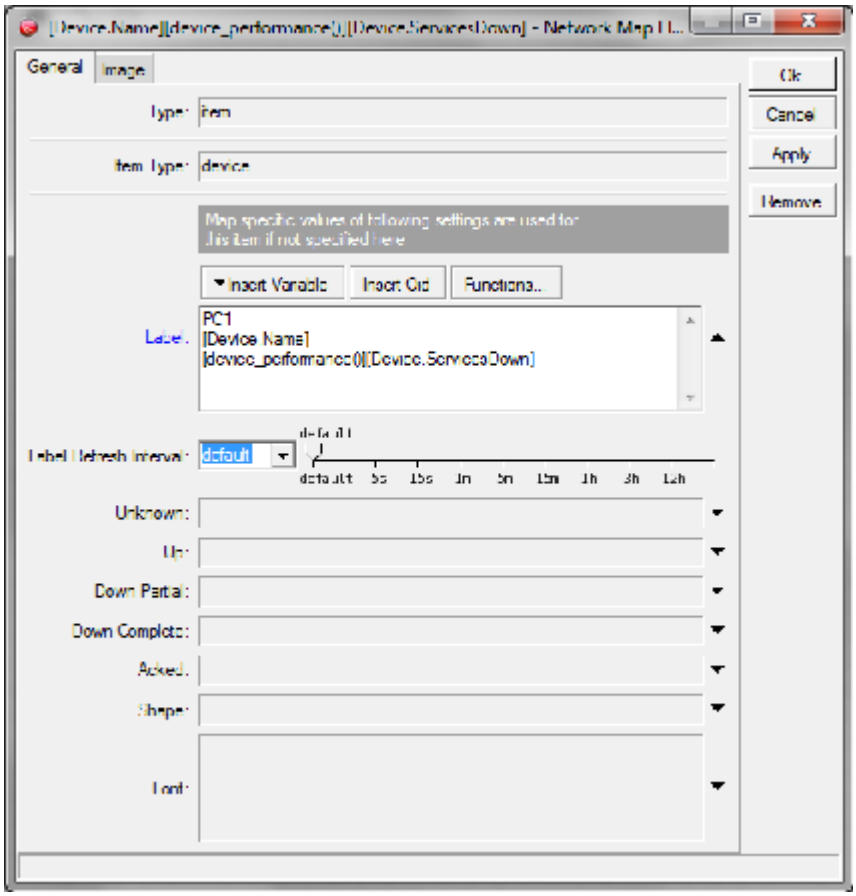
Затем нажать кнопку «Finish».

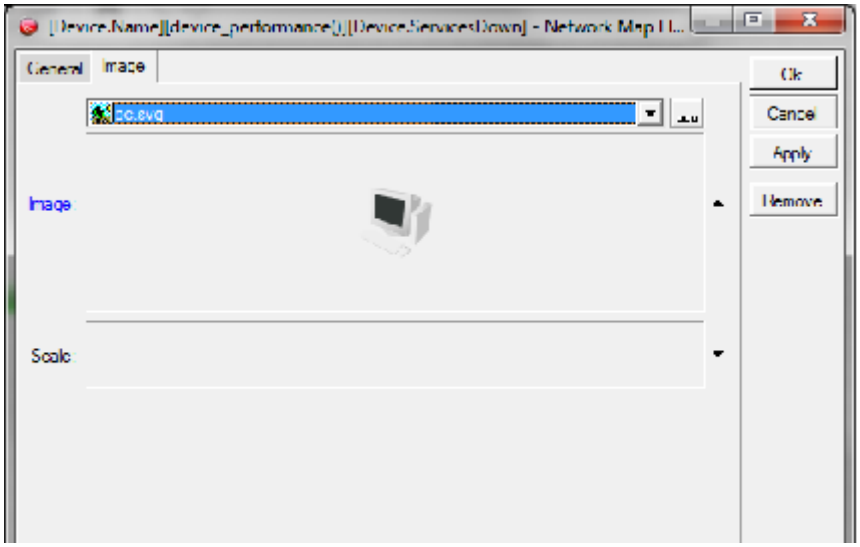


Аналогично добавить коммутаторы SW1, SW2 и PC2.



Производим настройку компьютеров, нажимаем правой кнопкой на PC1 из контекстного меню выбираем «Appearance», в открывшемся окне во кладке «General», в поле «Lable» добавить имя PC1, а на вкладке «Image» из выпадающего списка выбрать «pc.svg» и нажать Ок.





Аналогично выполнить для PC2.

Произвести настройку коммутаторов, для этого на коммутаторе нажать правой кнопкой и выбрать пункт «Appearance», в открывшемся окне во вкладке «Image» из выпадающего списка выбрать «switch.svg». Во вкладке «General» в поле «Lable», ввести параметры за которыми будет производится мониторинг по протоколу SNMP. Для примера следующие OID:

А. 1.3.6.1.2.1.1.1.0 – Запрос по протоколу SNMP на наименование модели устройства.

Б. 1.3.6.1.2.1.1.3.0 – Запрос времени работы устройства с момента последнего включения или сбоя.

В. 1.3.6.1.4.1.171.12.1.1.6.1.0 – Запрос загрузки CPU коммутатора в процентах.

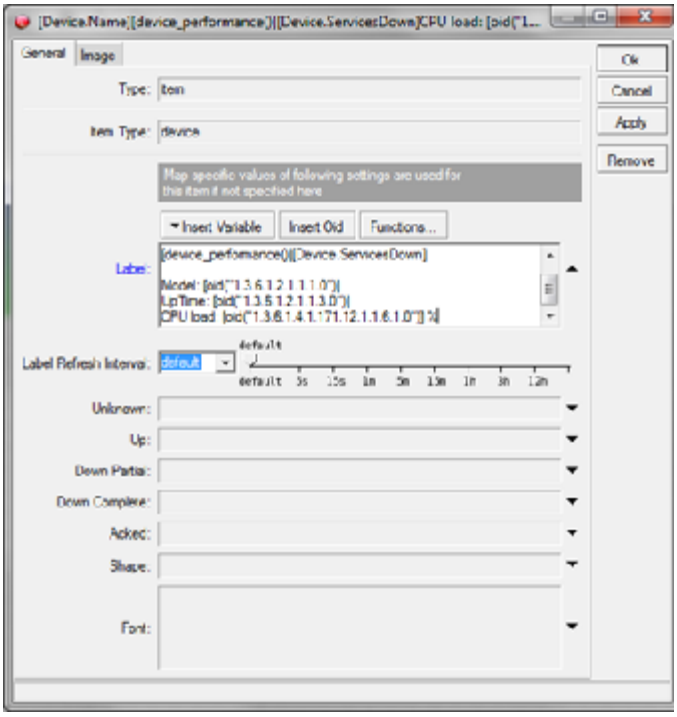
Пример формирования запроса: запрос к конкретному OID осуществляется строкой «[oid("1.3.6.1.4.1.171.12.1.1.6.1.0")]», которая будет выводить значение загрузки CPU одним числом. Для того чтобы данный параметр был интуитивно понятен на создаваемой схеме можно написать следующую строку: «CPU load: [oid("1.3.6.1.4.1.171.12.1.1.6.1.0")] %».

Все запросы могут выглядеть так:

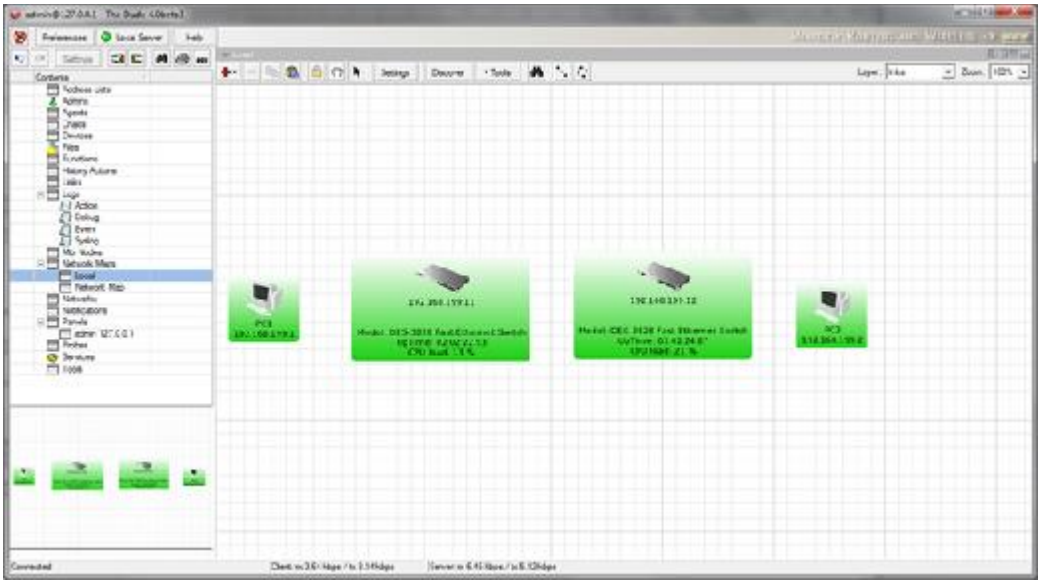
Model: [oid("1.3.6.1.2.1.1.1.0")]

UpTime: [oid("1.3.6.1.2.1.1.3.0")]

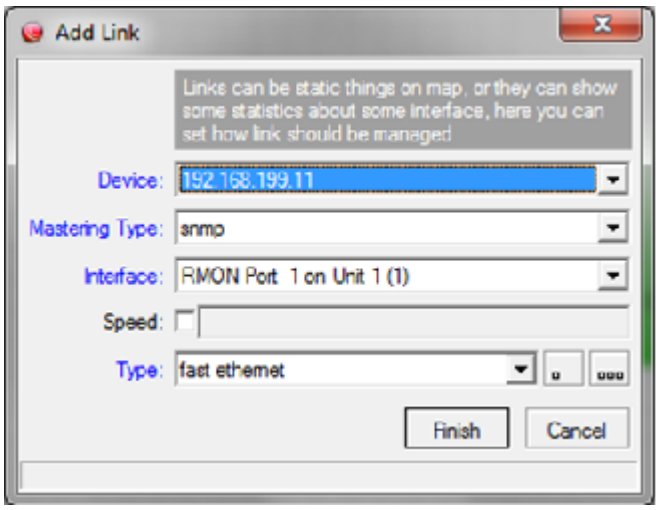
CPU load: [oid("1.3.6.1.4.1.171.12.1.1.6.1.0")] %

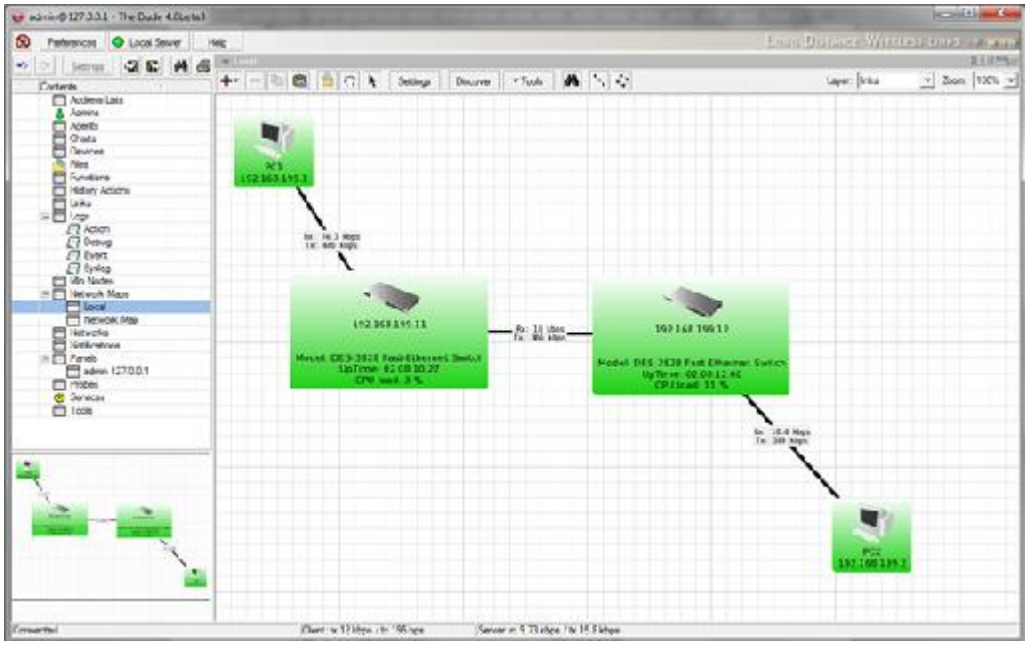


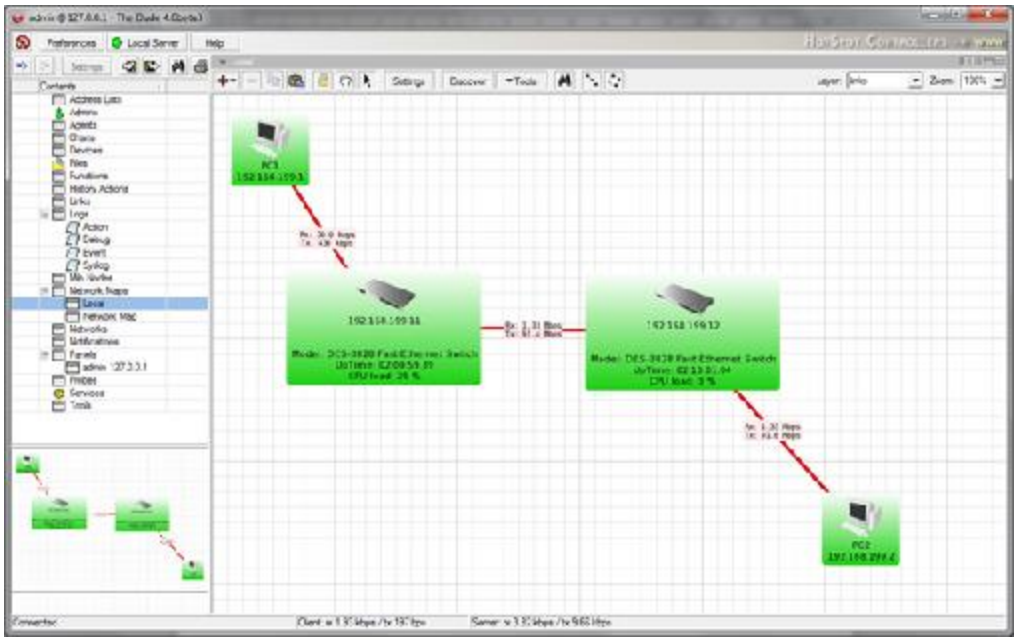
Затем нажать кнопку ОК и сделать аналогичное для коммутатора SW2.



Настройка связей между устройствами. Для добавления связи необходимо нажать на красный плюс, выбрать «Link» и провести между устройствами в открывшемся окне линию, выбрать параметры в соответствии с тем между какими устройствами настраивается связь. Например, если это связь между PC1 и SW, то необходимо выбрать Device – 192.168.199.11, Mastering Type – snmp, Interface – RMON Port 1 on Unit 1 (1) , Type – Fast Ethernet, затем нажать кнопку «Finish», аналогично добавить связи между SW1-SW2 и SW2-PC2.

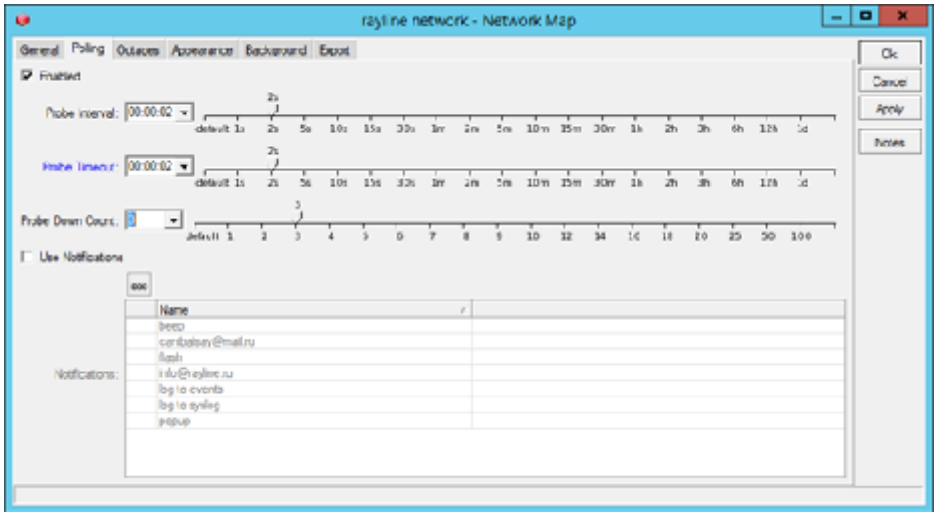

Add Link
Links can be static things on map, or they can show some statistics about some interface, here you can set how link should be managed
Device:
192.168.199.11
Mastering Type:
snmp
Interface:
RMON Port 1 on Unit 1 (1)
Speed:
Type:
fast ethernet
Finish
Cancel





6.4 Проверка выполненной лабораторной работы**.**

1. За всеми устройствами, включенными в сеть, должен выполняться мониторинг, об этом должен свидетельствовать зеленый цвет устройств на карте сети.
2. Мониторинг вышедшего из строя оборудования – для проверки необходимо отключать кабель в разных участках сети и наблюдайте за картой сети, устройства до которых была потеряна связь будут отмечены красным, при возобновлении связи устройства станут опять зелеными. Если устройства не меняют свой цвет, то необходимо уменьшить время опроса оборудования, для этого зайдите в настройки (settings), затем на вкладке Polling выставите время опроса 2 секунды, как показано на рисунке. И затем повторно выполните проверку пункта
3. Между всеми устройствами должен осуществляться мониторинг пропускной способности в реальном времени – об этом свидетельствуют цифры в килобит/с или мегабит/с на связях между устройствами. Для проверки работы запустите тест проверки скорости с компьютеров и наблюдайте за показаниями реальной скорости в системе мониторинга. При проверке скорости между PC1 и PC2 можно видеть изменение скорости в реальном времени, а также наблюдать изменение нагрузки на CPU коммутаторов.



4. Проверка времени работы с момента последнего запуска или сбоя (Uptime)– показывает сколько времени назад было включено устройство. Для проверки, запомните время Uptime на одном из устройств, затем перезагрузите устройство (отключите и подключите питание к коммутатору), после загрузки устройства убедитесь, что счетчик Uptime обнулился и начался новый отсчет времени.

2.11. Практическая работа № 11
Основные характеристики протокола SNMP

Топология

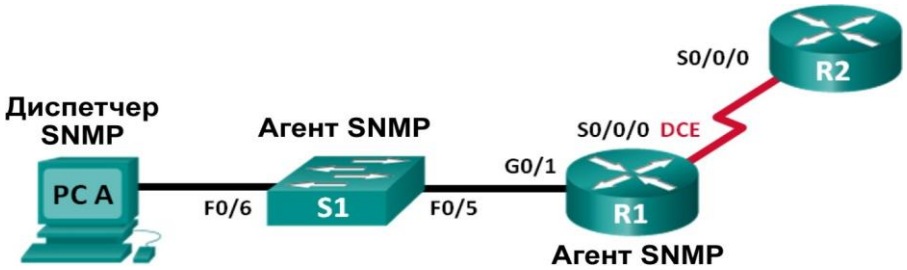


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	192.168.2.1	255.255.255.252	Недоступно
R2	S0/0/0	192.168.2.2	255.255.255.252	Недоступно
S1	VLAN 1	192.168.1.2	255.255.255.0	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

1. Создание сети и настройка базовых параметров устройств

2. Настройка диспетчера и агентов SNMP

3. Преобразование кодов OID с использованием Cisco SNMP Object Navigator

Исходные данные/сценарий

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетями) — это протокол управления сетью и стандарт IETF, который может использоваться как для мониторинга сети, так и для контроля клиентов в ней. SNMP может использоваться для получения и настройки переменных, связанных с состоянием и настройкой сетевых машин, таких как маршрутизаторы и коммутаторы, а также клиентские компьютеры сети. Диспетчер SNMP может опрашивать агенты SNMP для получения данных, либо данные могут автоматически отправляться на диспетчер SNMP путём настройки ловушек на агентах SNMP.

В этой лабораторной работе вы будете должны загрузить, установить и настроить программное обеспечение для управления SNMP с на компьютере ПК A. Вы также настроите маршрутизатор Cisco и коммутатор Cisco в качестве агентов SNMP. После получения сообщений с уведомлением SNMP от агента SNMP вы должны будете преобразовать коды MIB/ID объекта (OID), чтобы получить подробную информацию данных сообщений с помощью Cisco SNMP Object Navigator.

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, а также других версий ОС Cisco IOS. В зависимости от мо-

дели 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. Применение команд **snmp-server** в этой лабораторной работе приведёт к тому, что коммутатор Cisco 2960 сгенерирует сообщение с предупреждением при сохранении файла настройки в NVRAM. Чтобы избежать этого сообщения с предупреждением, убедитесь, что коммутатор использует шаблон **lanbase-routing**. Шаблон IOS контролируется диспетчером базы данных коммутатора (SDM). При изменении предпочтительного шаблона новый шаблон будет использоваться после перезагрузки, даже если настройка не сохраняется.

S1# **show sdm prefer**

Используйте следующие команды для назначения шаблона **lanbase-routing** в качестве шаблона SDM по умолчанию.

S1# **configure terminal**

S1(config)# **sdm prefer lanbase-routing**

S1(config)# **end** S1# **reload**

Необходимые ресурсы:

2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

1 коммутатор (Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный);

1 ПК (с Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

1 ПК (с Windows 7, Vista или XP с доступом к Интернету);

консольные кабели для настройки устройств Cisco IOS через порты консоли;

кабели Ethernet и последовательные кабели в соответствии с топологией.

ПО для управления протоколом SNMP (PowerSNMP Free Manager компании Dart Communications или сервер Syslog SolarWinds Kiwi, ознакомительная версия с испытательным периодом 30 дней)

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: Настройте компьютер.

Шаг 3: Инициализируйте и перезагрузите коммутатор и маршрутизаторы при необходимости.

Шаг 4: Произведите базовую настройку маршрутизаторов и коммутатора. а. Отключите поиск DNS.

Настройте имена устройств в соответствии с топологией.

Настройте IP-адреса в соответствии с таблицей адресации

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

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

Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

Проверьте подключения между устройствами локальной сети с помощью команды ping.

Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка диспетчера и агентов SNMP

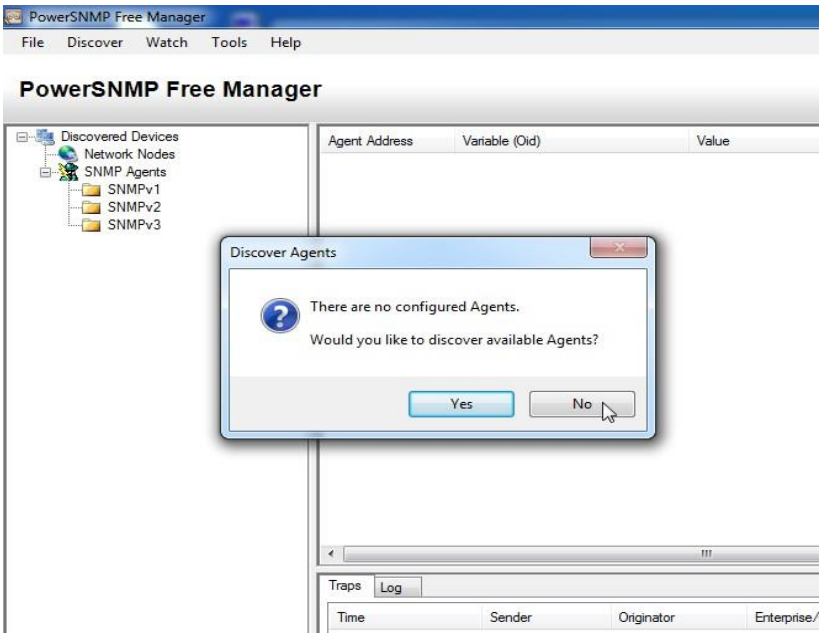
В части 2 вы должны будете установить ПО для управления SNMP и настроить его на ПК A, а также настроить R1 и S1 в качестве агентов SNMP.

Шаг 1: Установите программу управления SNMP.

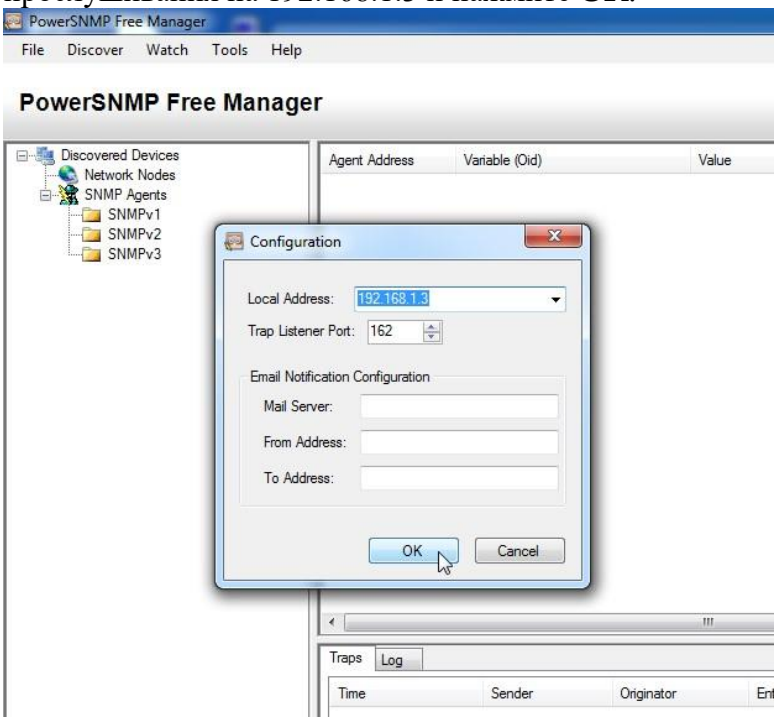
Загрузите и установите бесплатное приложение PowerSNMP Free Manager от компании Dart Communications, перейдя по следующему URL-адресу: http://www.dart.com/snmp-free-manager.aspx.

Запустите программу PowerSNMP Free Manager.

При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No** (Нет). Поиск агентов SNMP осуществляется после настройки SNMP на маршрутизаторе R1. PowerSNMP Free Manager поддерживает SNMP версии 1, 2, и 3. В данной лабораторной работе используется SNMPv2.



Во всплывающем окне настройки (если всплывающее окно не отображается, перейдите во вкладку Tools > Configuration (Инструменты > Настройка)) назначьте локальный IP-адрес для прослушивания на 192.168.1.3 и нажмите **OK**.



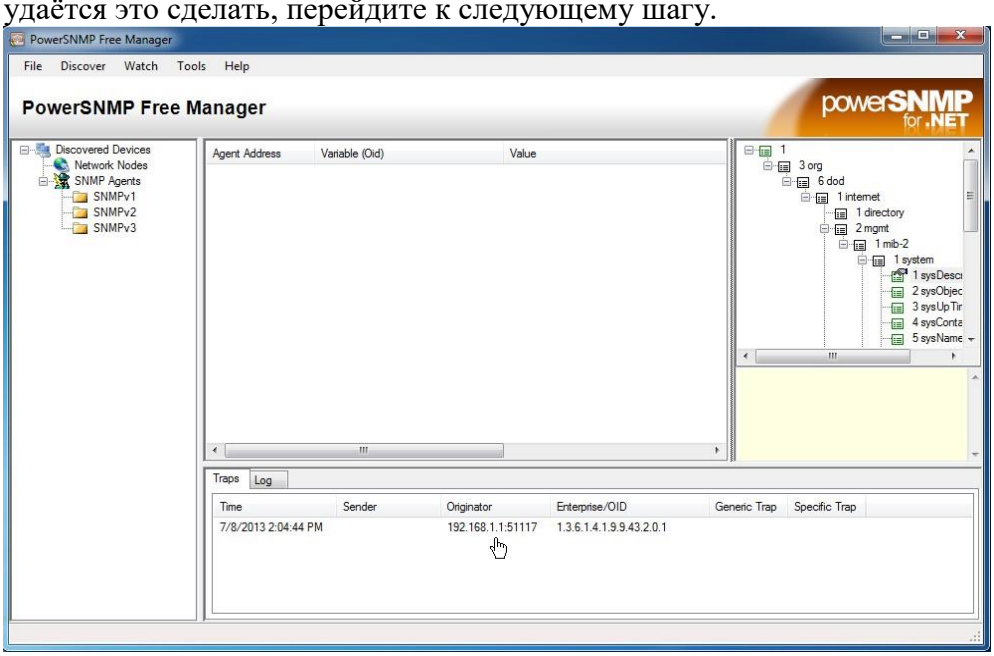
Примечание. При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No** и перейдите к следующему части данной лабораторной работы.

Шаг 2: Настройте агент SNMP.

На маршрутизаторе R1 введите следующие команды в режиме глобальной конфигурации, чтобы настроить его в качестве агента SNMP. В строке 1 ниже строкой сообщества SNMP является **ciscolab** с правами только для чтения, а именованный список доступа SNMP_ACL определяет, какие узлы могут получать данные SNMP от маршрутизатора R1. В строках 2 и 3 команды местоположения и контактной информации агента SNMP предоставляют описательную контактную информацию. В строке 4 указаны IP-адрес узла, который будет получать уведомления SNMP, версия SNMP и строка сообщества. Строка 5 включает все ловушки SNMP по умолчанию; строки 6 и 7 создают именованный список контроля доступа, определяющий, каким узлам разрешено получение информации SNMP от маршрутизатора.

R1(config)# **snmp-server community ciscolab ro SNMP_ACL**
R1(config)# **snmp-server location snmp_manager**
R1(config)# **snmp-server contact ciscolab_admin**
R1(config)# **snmp-server host 192.168.1.3 version 2c ciscolab**
R1(config)# **snmp-server enable traps**
R1(config)# **ip access-list standard SNMP_ACL**
R1(config-std-nacl)# **permit 192.168.1.3**

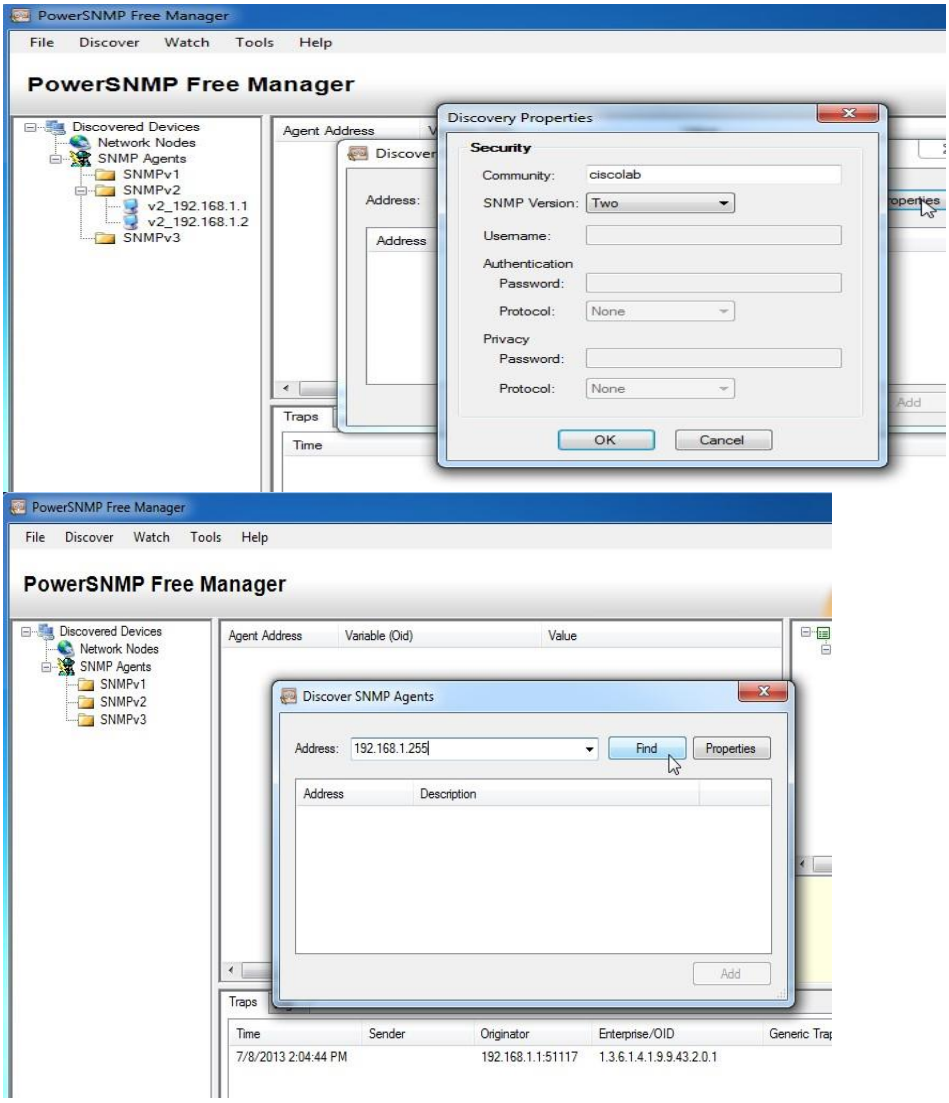
На этом этапе можно заметить, что PowerSNMP Free Manager получает уведомления от маршрутизатора R1. Если уведомления не приходят, вы можете попытаться принудительно установить отправку уведомления SNMP, введя команду **copy run start** на маршрутизаторе R1. Если вам не удаётся это сделать, перейдите к следующему шагу.



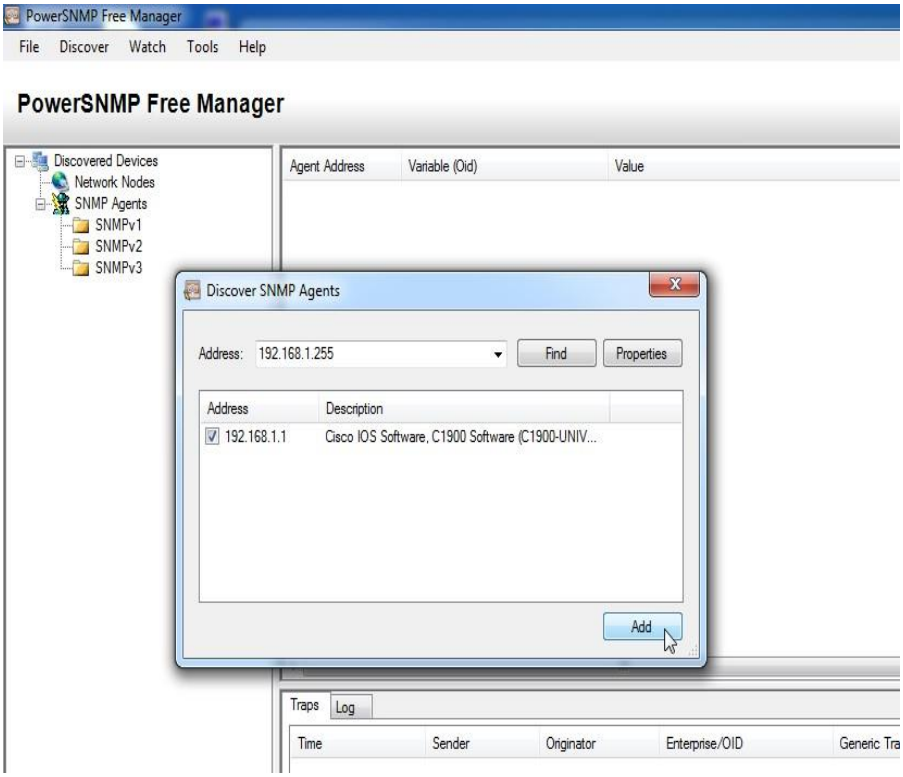
Шаг 3: Выполните обнаружение агентов SNMP.

В программе PowerSNMP Free Manager на компьютере ПК A откройте окно **Discover > SNMP Agents** (Обнаружение > Агенты SNMP). Введите IP-адрес **192.168.1.255**. В том же окне щёлкните

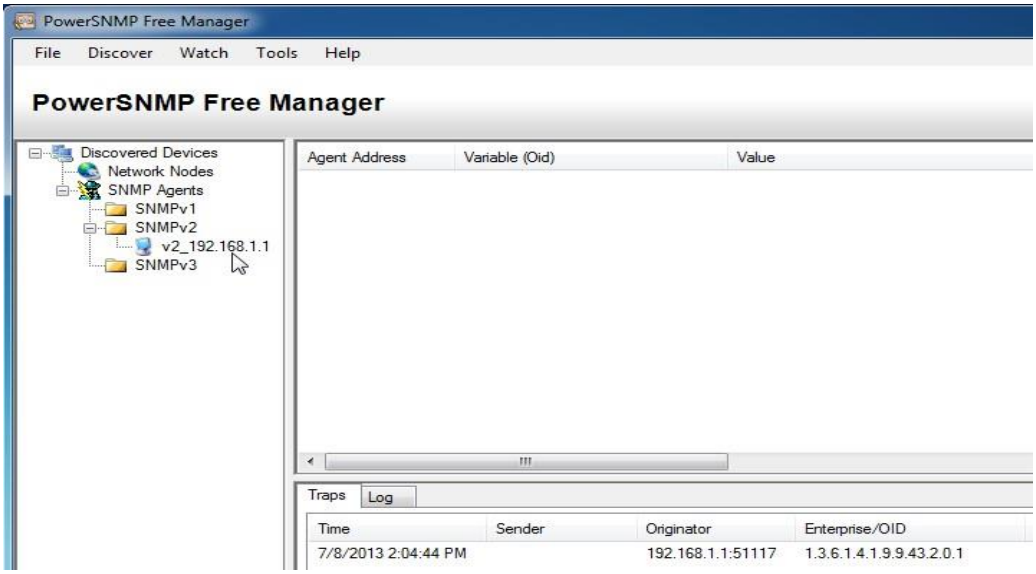
Properties (Свойства) и выберите в поле «Community» (Сообщество) параметр **ciscolab**, а в поле «SNMP Version» параметр **Two** (2), затем щёлкните **OK**. Теперь можете нажать **Find** (Найти) для обнаружения всех агентов SNMP в сети 192.168.1.0. Программа PowerSNMP Free Manager должна обнаружить маршрутизатор R1 по адресу 192.168.1.1. Установите флажок и щёлкните **Add** (Добавить), чтобы добавить маршрутизатор R1 в качестве агента SNMP.


PowerSNMP Free Manager
File Discover Watch Tools Help
PowerSNMP Free Manager
Discovered Devices
Network Nodes
SNMP Agents
SNMPv1
SNMPv2
v2_192.168.1.1
v2_192.168.1.2
SNMPv3
Agent Address
Discover
Address:
Address
Discovery Properties
Security
Community:
ciscolab
SNMP Version:
Two
Username:
Authentication
Password:
Protocol:
None
Privacy
Password:
Protocol:
None
OK
Cancel
Traps
Time
Add

PowerSNMP Free Manager
File Discover Watch Tools Help
PowerSNMP Free Manager
Discovered Devices
Network Nodes
SNMP Agents
SNMPv1
SNMPv2
SNMPv3
Agent Address
Variable (Oid)
Value
Discover SNMP Agents
Address:
192.168.1.255
Find
Properties
Address
Description
Add
Traps
Time
Sender
Originator
Enterprise/OID
Generic Trap
7/8/2013 2:04:44 PM
192.168.1.1:51117
1.3.6.1.4.1.9.9.43.2.0.1



В программе PowerSNMP Free Manager маршрутизатор R1 добавляется в список доступных агентов SNMPv2.



Настройте коммутатор S1 в качестве агента SNMP. Вы можете использовать те же команды **snmpserver**, которые вы использовали для настройки R1.

После завершения настройки коммутатора S1 уведомления SNMP с адреса 192.168.1.2 отображаются в окне «Traps» (Прерывания) программы PowerSNMP Free Manager. В программе PowerSNMP Free Manager добавьте коммутатор S1 в качестве агента SNMP с помощью тех же действий, которые вы выполнили для обнаружения R1.

Часть 3: Преобразование кодов OID с использованием Cisco SNMP Object Navigator

В части 3 принудительно установите отправку уведомлений SNMP на диспетчер SNMP, размещенный на компьютере ПК A. После этого вы должны будете преобразовать полученные коды

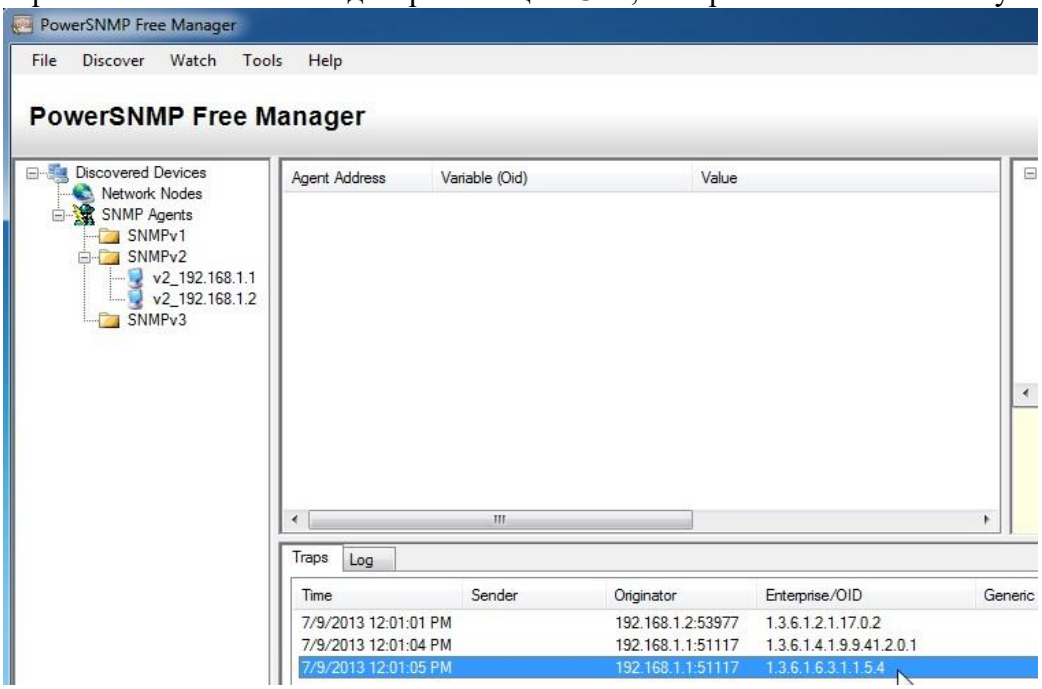
OID в имена, чтобы прочитать сообщения. Коды MIB/OID можно легко преобразовать с помощью средства Cisco SNMP Object Navigator на веб-сайте http://www.cisco.com.

Шаг 1: Удалите текущие сообщения SNMP.

В программе PowerSNMP Free Manager щёлкните правой кнопкой мыши окно **Traps** (Ловушки) и выберите **Clear** (Очистить) для удаления сообщений SNMP.

Шаг 2: Создайте ловушку и уведомление SNMP.

На маршрутизаторе R1 настройте интерфейс S0/0/0 согласно таблице адресации в начале данной лабораторной работы. Перейдите в режим глобальной конфигурации и разрешите интерфейсу отправлять уведомления, создаваемые в случае ловушки SNMP, на диспетчер SNMP на компьютере ПК A. Запомните коды организации/OID, отображаемые в окне ловушек.

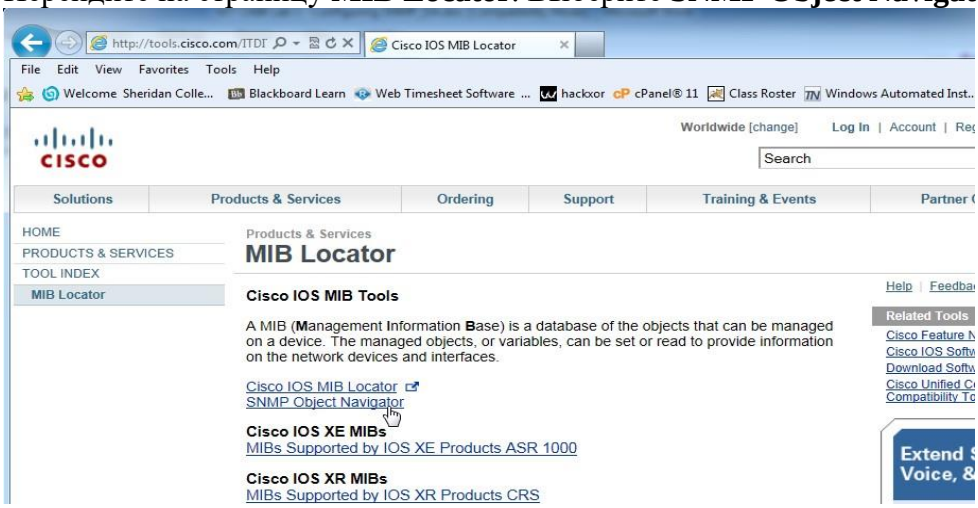


Шаг 3: Декодируйте сообщения MIB/OID SNMP.

На компьютере с доступом к Интернету откройте веб-браузер и перейдите на веб-сайт http://www.cisco.com.

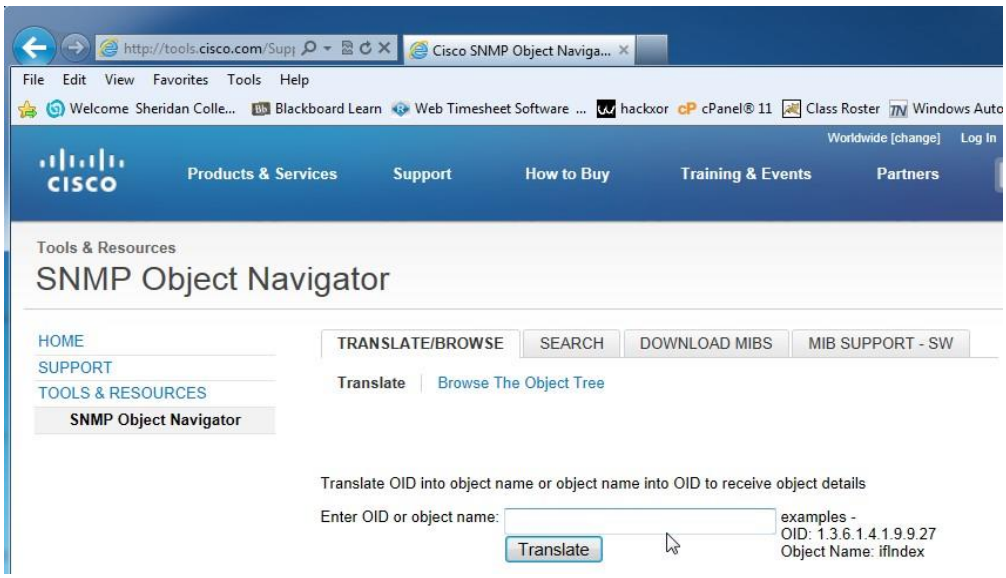
С помощью средства поиска в верхней части окна выполните поиск **SNMP Object Navigator**. Выберите в результатах **SNMP Object Navigator MIB Download MIBs OID OIDs**.

Перейдите на страницу **MIB Locator**. Выберите **SNMP Object Navigator**.



На странице **SNMP Object Navigator** выполните декодирование кода OID из программы

PowerSNMP Free Manager, который был создан в действии 2 части 3 данной лабораторной работы. Введите код OID и выберите **Translate** (Преобразовать).



Запишите коды OID и соответствующие им сообщения, полученные в результате преобразования, ниже.

Вопросы на закрепление

Перечислите несколько потенциальных преимуществ наблюдения за сетью с помощью протокола SNMP.

Почему при работе с SNMPv2 предпочтительно использовать исключительно доступ с правами только для чтения?

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.

2.12. Практическая работа № 12
Набор услуг (PDU) протокола SNMP

Просмотреть трафик клиента или сервера, поступающий от ПК к серверу при запрашивании веб-служб.

Шаг 1. Обзор трафика между клиентом и веб-сервером

а. Войдите в режим моделирования, щелкнув вкладку **Simulation**(моделирование) в правом нижнем углу. Вкладка **Simulation**(моделирование) расположена за вкладкой **Realtime** (в реальном времени) и обозначается символом секундомера.

б. Просмотрите трафик путем создания сложного PDU в режиме моделирования.

1. На **панели "Simulation"** (панель моделирования) выберите команду **Edit Filters** (изменить фильтры) и поставьте флажки в полях TCP и HTTP.
2. Добавьте **Complex PDU** (сложный PDU), щелкнув значок открытого конверта, расположенный над значком режима моделирования.
3. Щелкните External Client (внешний клиент) и сделайте его источником.

в. Укажите параметры **Complex PDU** (сложный PDU), изменив следующие настройки в окне **Create Complex PDU** (создание сложного PDU).

1. Раздел **PDU Settings** (параметры PDU) > **Select Application**(выбор приложения) должно быть установлено **HTTP**.
2. Щелкните имя сервера **ciscolearn.web.com** и сделайте его адресатом.
3. В разделе **Source Port** (порт источника) введите **1000**.
4. В разделе **Simulation Settings** (настройки моделирования) выберите **Periodic Interval** (периодический интервал) и введите **120** секунд.
5. Создайте PDU, щелкнув кнопку **Create PDU** (создать PDU) в окне **Create Complex PDU** (создание сложного PDU).

г. Дважды щелкните **"Simulation Panel"** (панель моделирования), чтобы разблокировать ее из PT-окна. Это позволяет перемещать панель моделирования для просмотра всей топологии сети.

д. Просмотрите поток трафика, нажав кнопку **Auto Capture / Play**(автозахват / воспроизведение) на **"Simulation Panel"** (панель моделирования). Ускорьте анимацию с помощью ползунка управления воспроизведением.
*При появлении окна **Buffer Full** (буфер заполнен) закройте его, щелкнув значок **x**.

Шаг 2. Просмотр информации заголовков пакетов, передаваемых по сети

Проверьте заголовки пакетов, передаваемых между клиентами и сервером.

1. На **"Simulation Panel"** (панель моделирования) и щелкните любую строку в окне Event List (список событий). В рабочей области отобразится конверт, соответствующий этой строке.
2. Щелкните значок в виде конверта в рабочей области, чтобы просмотреть информацию о пакете и заголовке.
3. В окне **OSI Model** (модель OSI) отображается, на каком уровне модели OSI обрабатывается данный пакет.

a. *Обратите внимание, что уровень может быть выше или ниже, в зависимости от принимающего устройства. Коммутатор отображает пакет только до 2-го уровня. Тогда как для ПК и сервера пакеты отображаются вплоть до 4-го уровня.

4. В окне **OSI Model** (модель OSI) прочтите описание пакета.
5. Щелкните **Inbound PDU Details** (сведения о входящих PDU) или **Outbound PDU Details** (сведения о исходящих PDU), чтобы просмотреть информацию о действительно отправленных пакетах.
   *Обратите внимание на MAC-адрес в кадре, IP-адрес в пакете и номера портов источника и назначения в сегменте.
6. Щелкните другие строки списка событий и просмотрите описания.

2.13. Практическая работа № 13
Формат сообщений SNMP

Всю необходимую информацию протокол SNMP получает из базы управляющей информации (ManagementInformationBase, MIB). MIB представляет собой базу данных стандартизированной структуры. База данных имеет древовидную структуру, а все переменные классифицированы по тематике. Каждое поддерево содержит определенную тематическую подгруппу переменных. Наиболее важные компоненты, отвечающие за работу сетевых узлов, объединены в подгруппе MIB-II.

Существуют два типа MIB: стандартные и фирменные. Стандартные MIB определены комиссией по деятельности Интернет (Internet Activity Board, IAB), а фирменные - производителем устройства.

В таблице 1 приведён список наиболее распространенных стандартов баз управляющей информации.

Таблица 1

База	Назначение
MIB-II	Задает множество объектов, которые могут быть использованы для управления сетевыми интерфейсами.
MIB повторителя	Включена в подмножество MIB-II. Устанавливает объекты, которые можно использовать для управления повторителем.
MIB моста	Включена в подмножество MIB-II. Задает объекты данных, которые можно использовать для управления мостом.

RMON MIB	Указывает объекты данных, которые можно использовать для управления сетью в целом, при помощи протокола RMON.

В базах данных, указанных в таблице 1, присутствует множество переменных, которые могут быть полезны для диагностирования сети и сетевых устройств.

Например, используя MIB-II, можно получить сведения об общем количестве пакетов, переданных сетевым интерфейсом, а с помощью MIB повторителя можно узнать информацию о количестве коллизий в порту.

В MIB каждый объект имеет имя и тип. Имя объекта характеризует его положение в дереве MIB. При этом имя дочернего узла включает в себя имя родительского узла и задается целым числом.

Отличия SNMPv 3

SNMP – протокол прикладного уровня. Он предназначен для обмена информацией между сетевыми устройствами. При помощи этого протокола, сетевой администратор может производить анализ сетевого оборудования, находить и решать множество сетевых проблем.

В Декабре 1997 года с выходом SNMPv3, пользователям стали доступны новые службы, такие как: ограничение доступа, защита данных и аутентификация пользователя.

Кроме этого, стоит отметить, что SNMPv3 перенял модульную архитектуру от своих предшественников. Это обеспечивает поддержку предыдущих версий SNMPи, не смотря на то, что SNMPv1 и SNMPv2 не поддерживают аутентификацию и шифрование, у Вас будет возможность управления устройствами, которые поддерживают эти версии.

При создании новой версии разработчики руководствовались следующими принципами:

1. необходимо обеспечить большую безопасность протокола (особенно для операций типа SET);

2. SNMPv3 должен иметь возможность дальнейшего развития и расширения;

3. протокол должен остаться простым и понятным;

4. настройки параметров безопасности SNMPv3 должны быть максимально простыми;

В SNMPv3 уже не применяются термины «агент» и «менеджер», теперь используются термины «сущности». Как и раньше одна сущность находится на управляемом устройстве, а вторая занимается опросом приложений.

У сущностей-агентов и сущностей-менеджеров теперь есть ядро, которое выполняет четыре основные функции (см. Рисунок 1):

1.функции диспетчера;

2.обработка сообщений;

3.функции безопасности;

4.контроль доступа.

Диспетчер– это простая система управления входящим и исходящим трафиком. Для каждого исходящего блока данных (PDU) он определяет тип необходимой обработки (SNMPv1, SNMPv2, SNMPv3) и передает блок данных соответствующему модулю в системе обработки сообщений.

После того как система обработки сообщений вернет сообщение, которое содержит этот блок данных, Диспетчер отправит его на транспортный уровень для последующей передачи. Для входящих сообщений, Диспетчер проводит обратную операцию.

Система обработки сообщений

получает от Диспетчера исходящие блоки данных (PDU), добавляет к ним подходящий заголовок и возвращает их обратно Диспетчеру.

Система безопасности

отвечает за шифрование и аутентификацию. Все исходящие сообщения перед отправкой сначала передаются из системы обработки сообщений в систему безопасности, где все шифруются поля в заголовке сообщения, блок данных (PDU), генерируется код аутентификации и добавляется к заголовку сообщения.

После этого сообщение передается обратно в систему обработки сообщений. Точно такая же операция, но в обратном порядке производится для всех входящих сообщений.

Система контроля доступа

управляет службами аутентификации для контроля доступа к MIB исходя из содержимого блоков данных. (PDU). Теоретически, система контроля доступа может работать с самыми разными моделями контроля доступа, но на данный момент в RFC 2275 описана только одна модель – VACM (View-BasedAccessControlModel)

Таблица 2 - Основные методы SNMP

Метод	Для чего применяется	Поддерживается
GET	Используется менеджером для получения данных из MIB. Размер сообщения ограничен возможностями агента.	SNMPv1-3
GET-NEXT	Метод позволяет последовательно выполнить набор команд иполучить набор значений из MIB	SNMPv1-3
GET-BULK	Используется менеджером для получения сразу большого количества данных из MIB. Размер сообщения отсылаемого агентом не ограничен.	SNMPv2, SNMPv3
SET	Используется менеджером для установки значений в MIB агента	SNMPv1-3
GET-RESPONSE	SNMPv1-3	
TRAP	Используется агентом чтобы послать сигнал менеджеру	SNMPv1-3

NOTIFICATION	SNMPv2, SNMPv3	
INFORM	Используется менеджером для отсылки сигнала другому менеджеру	SNMPv2, SNMPv3
REPORT	SNMPv2, SNMPv3	

При помощи этих команд и стандартной базы MIB можно получить самую разнообразную информацию.

Например: количество принятых и отправленных пакетов по TCP, IP, UDP или ICMP. А еще можно узнать о количестве ошибок, которые были обнаружены во времяотправки или получения пакетов.

При разработке SNMPv3 немало внимания было уделено безопасности протокола. Теперь стала поддерживаться модель, ориентированная на пользователя (User-BasedSecurityModel сокр. USM< см. RFC 3414>) благодаря которой стало возможным добавление модулей аутентификации и шифрованиябез смены базовой архитектуры.*

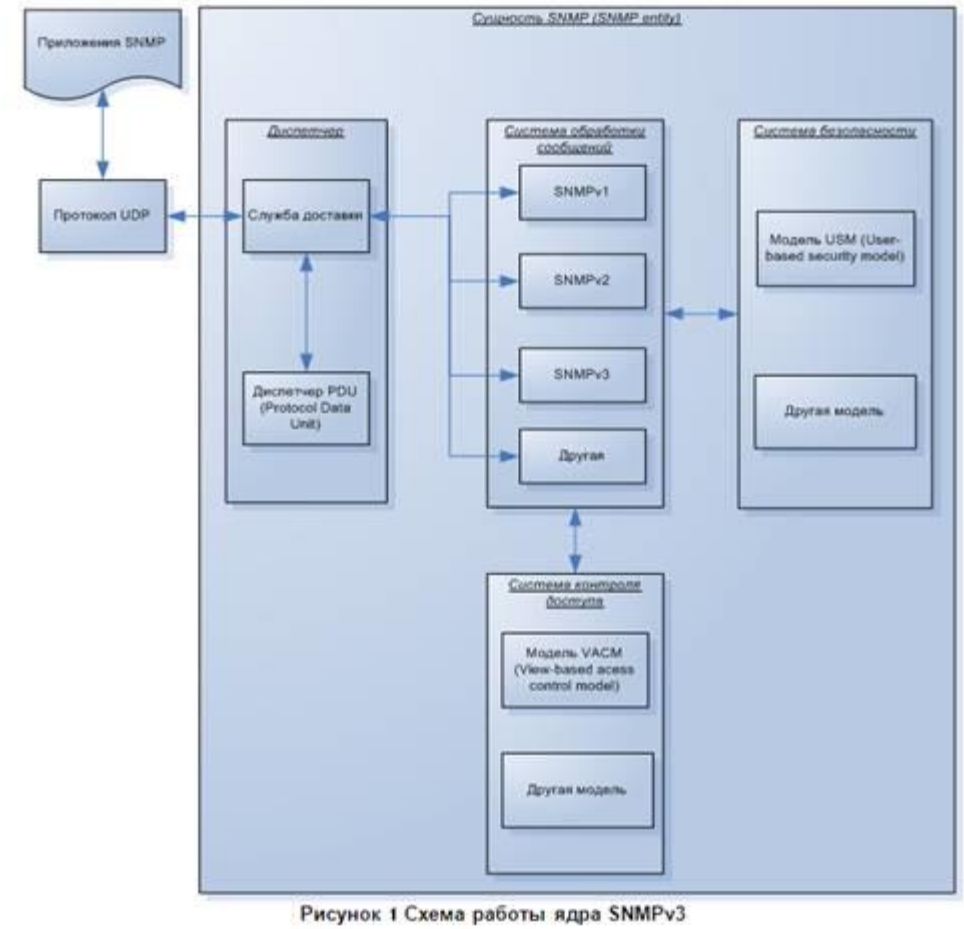


Рисунок 1 Схема работы ядра SNMPv3

3.2Безопасность в SNMPv 3

Модель USM включает в себя модуль аутентификации, модуль шифрования и модуль контроля времени. При этом, модуль аутентификации и шифрования занимаются защитой данных, а модуль контроля времени синхронизирует время между сущностями SNMP.

Основные проблемы, которые необходимо было решить при помощи модели USM:

Изменение данных сущностями не прошедшими аутентификацию;

1. Возможность откладывания каких-либо действий на неопределенное время или повторение одних и тех же действий с произвольными интервалами;

2. Возможность заблокировать обмен данными между сущностями;

3. Возможность перехвата трафика при передаче между сущностями;

4. Возможность «маскарада», т.е. сущность не прошедшая аутентификацию, могла прикинуться сущностью прошедшей аутентификацию.

Проблему решили следующим образом: для каждого сетевого устройства пароль преобразуется в некоторый уникальный ключ. Это обеспечивает дополнительную безопасность т.к. даже в том случае, если ключ будет перехвачен, злоумышленник получит доступ только к одному сетевому устройству. Для шифрования пароля используется алгоритм MD5, но разработчики видимо решили, что это не обеспечит достаточной сохранности пароля и поэтому блок PDU дважды хэшируется при помощи двух разных ключей, которые в свою очередь генерируются из закрытого ключа. Позже, первые 12 октетов используются как код аутентификации сообщения, который добавляется к сообщению. Такой же процесс приходится производить на другой стороне, но только в обратном порядке. Несмотря на всю сложность и энергоемкость процесса передачи данных между сущностями SNMP, по мнению разработчиков, алгоритм шифрования (DES) на самом деле не обеспечивает достаточной защиты информации, поэтому в дальнейшем предполагается использовать другие алгоритмы. Например, алгоритм Диффи-Хиллмана (Diffie-Hillman)

Разработчиками предусмотрено 3 уровня безопасности:

1. noAuthNoPriv – пароли передаются в открытом виде, конфиденциальность данных отсутствует.

2. authNoPriv – аутентификация без конфиденциальности. Большинство пользователейиспользует именно этот уровень т.к уровень защищенности в нем уже достаточно высок, а сетевые устройства не перегружаются шифрованием данных.

3. authPriv – аутентификация и шифрование. Максимальный уровень защищенности.

Как правило, покупатели сначала выбирают второй уровень безопасности и лишь немногие из них, потом начинают использовать третий. Одной из причин, по которой не используется третий уровень, является то, что он перегружает сетевые устройства.

На данный момент закончена разработка новой спецификации DataOverCableServiceInterfaceSpecification<см. стандарт RFC 3256> , а для управления ключами многие пользователи уже используют алгоритмы Диффи-Хиллмана (Diffie-Hillman) и Kerberosвместо DES.Скорее всего, это означает, что скоро можно будет ожидать выход новой версии протокола SNMP.

Интернет - гигантская сеть. Напрашивается вопрос, как она сохраняет свою целостность и функциональность без единого управления? Если же учесть разнородность ЭВМ, маршрутизаторов и программного обеспечения, используемых в сети, само существование Интернет представится просто чудом. Так как же решаются проблемы

управления в Интернет? Отчасти на этот вопрос уже дан ответ - сеть сохраняет работоспособность за счет жесткой протокольной регламентации. "Запас прочности" заложен в самих протоколах. Функции диагностики возложены, как было сказано выше, на протокол ICMP. Учитывая важность функции управления, для этих целей создано два протокола SNMP (Simple Network Management Protocol, RFC-1157, -1215, -1187, -1089, std-15 разработан в 1988 году) и CMOT (Common Management Information services and protocol over TCP/IP, RFC-1095, в последнее время применение этого протокола ограничено). Обычно управляющая прикладная программа воздействует на сеть по цепочке SNMP-UDP-IP-Ethernet. Наиболее важным объектом управления обычно является внешний порт сети (gateway) или маршрутизатор сети. Каждому управляемому объекту присваивается уникальный идентификатор.

Протокол SNMP работает на базе транспортных возможностей UDP (возможны реализации и на основе TCP) и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении в сети Интернет. Протокол определяет формат данных, а их обработка и интерпретация остаются на усмотрение управляющих станций или менеджера сети. SNMP-сообщения не имеют фиксированного формата и фиксированных полей. При своей работе SNMP использует управляющую базу данных (MIB - management information base, RFC-1213, -1212, std-17).

Алгоритмы управления в Интернет обычно описывают в нотации ASN.1 (Abstract Syntax Notation). Все объекты в Интернет разделены на 10 групп и описаны в MIB: система, интерфейсы, обмены, трансляция адресов, IP, ICMP, TCP, UDP, EGP, SNMP. В группу "система" входит название и версия оборудования, операционной системы, сетевого программного обеспечения и пр.. В группу "интерфейсы" входит число поддерживаемых интерфейсов, тип интерфейса, работающего под IP (Ethernet, LAPB etc.), размер дейтограмм, скорость обмена, адрес интерфейса. IP-группа включает в себя время жизни дейтограмм, информация о фрагментации, маски субсетей и т.д. В TCP-группу входит алгоритм повторной пересылки, максимальное число повторных пересылок и пр.. Ниже приведена таблица (3) команд (pdu - protocol data unit) SNMP:

Таблица 3 - Команды SNMP

Команда SNMP	Тип PDU	Назначение
GET-request		Получить значение указанной переменной или информацию о состоянии сетевого элемента;
GET_next_request		Получить значение переменной, не зная точного ее имени (следующий логический идентификатор на дереве MIB);
SET-request		Присвоить переменной соответствующее значение. Используется для описания действия, которое должно быть выполнено;
GET response		Отклик на GET-request, GET_next_request и SET-request. Содержит также информацию о состоянии (коды ошибок и другие данные);
TRAP		Отклик сетевого объекта на событие или на изменение состояния.
GetBulkRequest		Запрос пересылки больших объемов данных, например, таблиц.
InformRequest		Менеджер обращает внимание партнера на определенную информацию в MIB.

SNMPv3-Trap	Отклик на событие (расширение по отношению v1 и v2).
Report	Отчет (функция пока не задана).

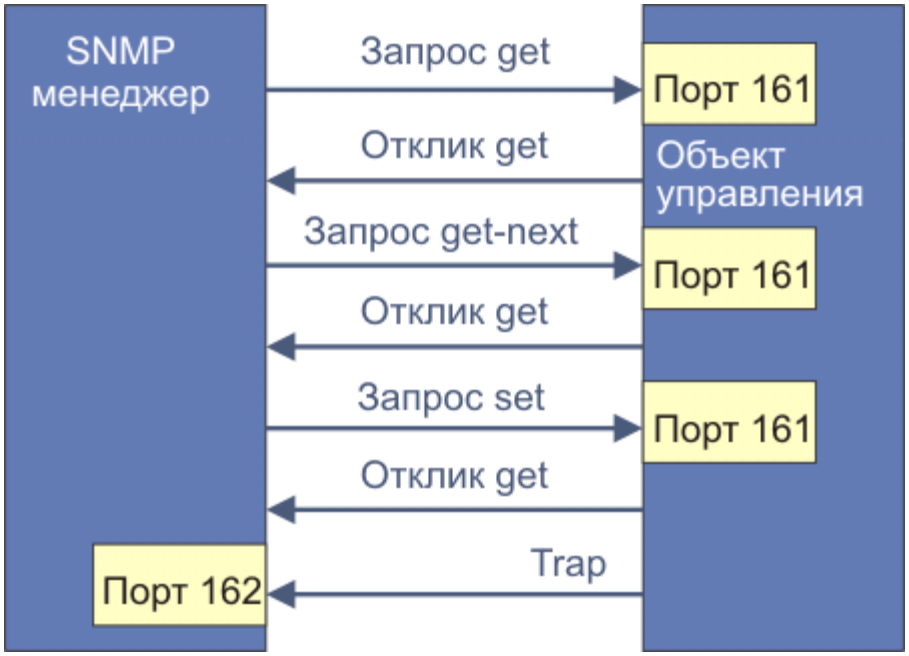


Рис. 2 - Схема запросов/откликов SNMP

Формат SNMP-сообщений, вкладываемых в UDP-дейтограммы, имеет вид (рис. 4.4.13.2):

Рис. 3 - Формат SNMP-сообщений, вкладываемых в UDP-дейтограммы

Поле версия содержит значение, равное номеру версии SNMP минус один. Поле пароль (community - определяет группу доступа) содержит последовательность символов, которая является пропуском при взаимодействии менеджера и объекта управления. Обычно это поле содержит 6-байтовую строку public, что означает общедоступность. Для запросов GET, GET-next и SET значение идентификатора запроса устанавливается менеджером и возвращается объектом управления в отклике GET, что позволяет связывать в пары запросы и отклики. Поле фирма (enterprise) = sysobjectid объек-

та. Поле статус ошибки характеризуется целым числом, присланным объектом управления:

Таблица 4. Номера и назначения используемых портов

Назначение	Порт	Пояснение
SNMP	161/TCP	Simple Network Management Protocol
SNMP	162/TCP	Trap
SMUX	199/TCP	SNMP Unix Multiplexer
SMUX	199/UDP	SNMP Unix Multiplexer
synoptics-relay	391/TCP	SynOptics SNMP Relay Port
synoptics-relay	391/UDP	SynOptics SNMP Relay Port
Agentx	705/TCP	AgentX
snmp-tcp-port	1993/TCP	cisco SNMP TCP port
snmp-tcp-port	1993/UDP	cisco SNMP TCP port

Таблица 5 - Коды ошибок

Статус ошибки	Имя ошибки	Описание
	Noerror	Все в порядке;
	Toobig	Объект не может уложить отклик в одно сообщение;
	Nosuchname	В операции указана неизвестная переменная;
	badvalue	В команде set использована недопустимая величина или неправильный синтаксис;
	Readonly	Менеджер попытался изменить константу;
	Generr	Прочие ошибки.

Если произошла ошибка, поле индекс ошибки (error index) характеризует, к какой из переменных это относится. error index является указателем переменной и устанавливается объектом управления не равным нулю для ошибок badvalue, readonly и nosuchname. Для оператора TRAP (тип PDU=4) формат сообщения меняется. Таблица типов TRAPпредставлена ниже (4.4.13.4):

Таблица 6 - Коды TRAP

Тип TRAP	Имя TRAP	Описание
	Coldstart	Установка начального состояния объекта.
	Warmstart	Восстановление начального состояния объекта.
	Linkdown	Интерфейс выключился. Первая переменная в сообщении идентифицирует интерфейс.
	Linkup	Интерфейс включился. Первая переменная в сообщении идентифицирует интерфейс.
	Authenticationfailure	От менеджера получено snmp-сообщение с неверным паро-

	лем (community).
EGPneighborloss	R$GP-партнер отключился. Первая переменная в сообщении определяет IP-адрес партнера.
Entrprisespecific	Информация о TRAP содержится в поле специальный код.

Для тип TRAP 0-4 поле специальный код должно быть равно нулю.

Поле временная метка содержит число сотых долей секунды (число тиков) с момента инициализации объекта управления. Так прерывание coldstart выдается объектом через 200 мс после инициализации.

В последнее время широкое распространение получила идеология распределенного протокольного интерфейса DPI (Distributed Protocol Interface). Для транспортировки snmp-запросов может использоваться не только UDP-, но и TCP-протокол. Это дает возможность применять SNMP-протокол не только в локальных сетях. Форматы SNMP-DPI-запросов (версия 2.0) описаны в документе RFC-1592. Пример заголовка snmp-запроса (изображенные поля образуют единый массив; см. рис. 4.4.13.3):

Рис. 4 - Формат заголовка SNMP-запроса

Поле Флаг=0x30 является признаком ASN.1-заголовка. Коды Ln - представляют собой длины полей, начинающиеся с байта, который следует за кодом длины, вплоть до конца сообщения-запроса (n - номер поля длины), если не оговорено другое. Так L1 - длина пакета-запроса, начиная с T1 и до конца пакета, а L3 - длина поля пароля. Субполя Tn - поля типа следующего за ними субполя запроса. Так T1=2 означает, что поле характеризуется целым числом, а T2=4 указывает на то, что далее следует пароль (поле community, в приведенном примере = public). Цифры под рисунками означают типовые значения субполей. Код 0xA - является признаком GET-запроса, за ним следует поле кода PDU (=0-4, см. табл. 4.4.13.1)

Блок субполей идентификатора запроса служит для тех же целей, что и другие идентификаторы - для определения пары запрос-отклик. Собственно идентификатор за-

проса может занимать один или два байта, что определяется значением $L_{из}$. СО - статус ошибки (СО=0 - ошибки нет); ТМ - тип MIB-переменной (в приведенном примере = 0x2B); ИО - индекс ошибки. Цифровой код MIB-переменной отображается последовательностью цифровых субполей, характеризующих переменную, например: переменная 1.3.6.1.2.1.5 (в символьном выражении iso.org.dod.internet.mgmt.mib.icmp) характеризуется последовательностью кодов 0x2B 0x06 0x01 0x02 0x01 0x05 0x00.

Начиная с января 1998 года, выпущен набор документов, посвященных SNMPv3 . В этой версии существенно расширена функциональность (см. таблицу 1 тип PDU=5-8), разработана система безопасности.

В данной версии реализована модель, базирующаяся на процессоре SNMP (SNMP Engene) и содержащая несколько подсистем (дипетчер, система обработки сообщений, безопасности и управления доступом, см. рис. 4.4.13.4).

Перечисленные подсистемы служат основой функционирования генератора и обработчика команд, отправителя и обработчика уведомлений и прокси-сервера (Proxy Forwarder), работающих на прикладном уровне. Процессор SNMP идентифицируется с помощью snmpEngineID.

Обеспечение безопасности модели работы SNMP упрощается обычно тем, что обмен запросами-откликами осуществляется в локальной сети, а источники запросов-откликов легко идентифицируются.

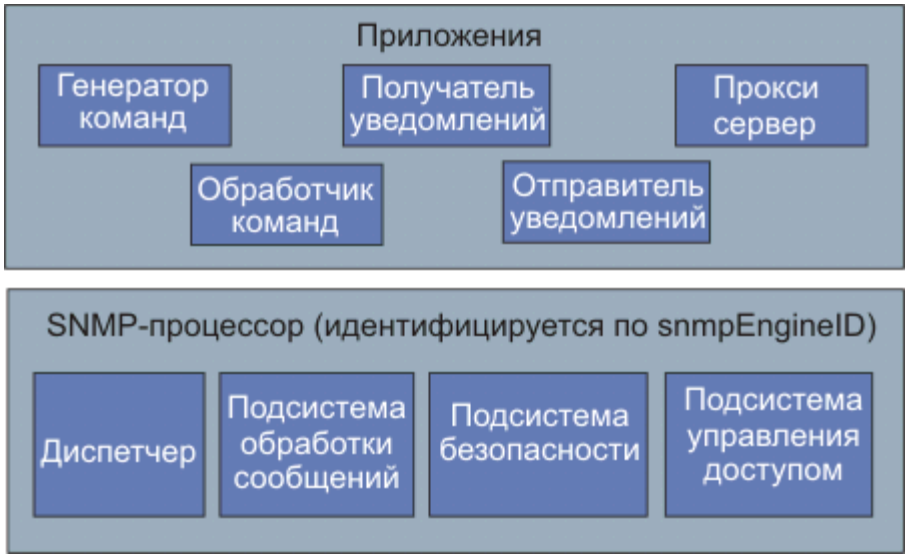


Рис. 5 - Архитектура сущности SNMP (SNMP-entity)

Компоненты процессора SNMP перечислены в таблице 4.4.13.5 (смотри RFC 2571 и - 2573)

Таблица 7 - Компоненты процессора SNMP

Название компонента	Функция компонента
Диспетчер	Позволяет одновременную поддержку нескольких версий SNMP-

	сообщений в процессоре SNMP. Этот компонент ответственен за прием протокольных блоков данных (PDU), за передачу PDU подсистеме обработки сообщений, за передачу и прием сетевых SNMP-сообщений
Подсистема обработки сообщений	Ответственна за подготовку сообщений для отправки и за извлечение данных из входных сообщений
Подсистема безопасности	Предоставляет услуги, обеспечивающие безопасность: аутентификацию и защищенность сообщений от перехвата и искажения. Допускается реализация нескольких моджелей безопасности
Подсистема управления доступом	Предоставляет ряд услуг авторизации, которые могут использоваться приложениями для проверки прав доступа.
Генератор команд	Инициирует SNMP-запросы Get, GetNext, GetBulk или Set, предназначенные для локальной системы, которые могут использоваться приложениями для проверки прав доступа.
Обработчик команд	Воспринимает SNMP-запросы Get, GetNext, GetBulk или Set, предназначенные для локальной системы, это индицируется тем, что contextEngeneID в полученном запросе равно соответствующему значению в процессоре SNMP. Приложение обработчика команд выполняет соответствующие протокольные операции, генерирует сообщения отклика и посылает их откправителю запроса.
Отправитель уведомлений	Мониторирует систему на предмет выявления определенных событий или условий и генерирует сообщения Trap или Inform. Источник уведомлений должен иметь механизм определения адресата таких сообщений, а также параметров безопасности
Получатель уведомлений	Прослушивает сообщения уведомления и формирует сообщения-отклики, когда приходит сообщение с PDU Inform
Прокси-сервер	Переадресует SNMP-сообщения. Реализация этогог модуля является опционной

На рис. 6 показан формат сообщений SNMPv3, реализующий модель безопасности UBM (User-Based Security Model).

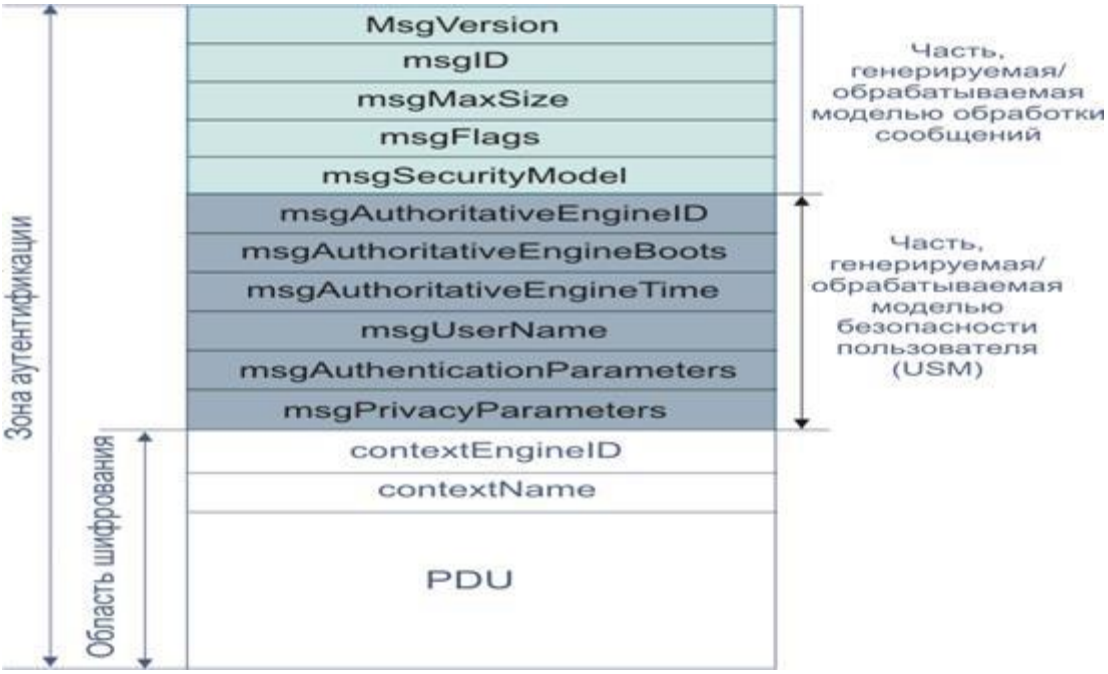


Рис.6 - Формат сообщений SNMPv3 с UBM

Первые пять полей формируются отправителем в рамках модели обработки сообщений и обрабатываются получателем. Следующие шесть полей несут в себе параметры безопасности. Далее следует PDU (блок поля данных) с contextEngeneID и contextName .

· msgVersion (для SNMPv3)=3

· msgID - уникальный идентификатор, используемый SNMP-сущностями для установления соответствия между запросом и откликом. Значение msgID лежит в диапазоне 0 - (2^{31} -1)

· msgMaxSize - определяет максимальный размер сообщения в октетах, поддерживаемый отправителем. Его значение лежит в диапазоне 484 - (2^{31} -1) и равно максимальному размеру сегмента, который может воспринять отправитель.

· msgFlags - 1-октетная строка, содержащая три флага в младших битах: reportableFlag, privFlag, authFlag . Если reportableFlag=1, должно быть прислано сообщение с PDU Report; когда флаг =0, Report посылать не следует. Флаг reportableFlag=1 устанавливается отправителем во всех сообщениях запроса (Get, Set) или Inform. Флаг устанавливается равным нулю в откликах, уведомлениях Trap или сообщениях Report. Флаги privFlag и authFlag устанавливаются отправителем для индикации уровня безопасности для данного сообщения. Для privFlag=1 используется шифрование, а для authFlag=0 - аутентификация. Допустимы любые комбинации значений флагов кроме privFlag=1 AND authFlag=0 (шифрование бех аутентификации).

· msgSecurityModel - идентификатор со значением в диапазоне 0 - (2^{31} -1), который указывает на модель безопасности, использованную при формировании данного сообщения. Зарезервированы значения 1 для SNMPv1,2 и 3 - для SNMPv3.

Модель безопасности USM (User-Based Security Model) использует концепцию авторизованного сервера (authoritative Engene). При любой передаче сообщения одна или две сущ-

ности, передатчик или приемник, рассматриваются в качестве авторизованного SNMP-сервера. Это делается согласно следующим правилам:

· Когда SNMP-сообщение содержит поле данных, которое предполагает отклик (например, Get, GetNext, GetBulk, Set или Inform), получатель такого сообщения считается авторизованным.

· Когда SNMP-сообщение содержит поле данных, которое не предполагает посылку отклика (например, SNMPv2-Trap, Response или Report), тогда отправитель такого сообщения считается авторизованным.

Таким образом, сообщения, посланные генератором команд, и сообщения Inform, посланные отправителем уведомлений, получатель является авторизованным. Для сообщений, посланных обработчиком команд или отправителем уведомлений Trap, отправитель является авторизованным. Такой подход имеет две цели:

· Своевременность сообщения определяется с учетом показания часов авторизованного сервера. Когда авторизованный сервер посылает сообщение (Trap, Response, Report), оно содержит текущее показание часов, так что неавторизованный получатель может синхронизовать свои часы. Когда неавторизованный сервер посылает сообщение (Get, GetNext, GetBulk, Set, Inform), он помещает туда текущую оценку показания часов места назначения, позволяя получателю оценить своевременность прихода сообщения.

· Процесс локализации ключа, описанный ниже, устанавливает единственного принципала, который может владеть ключем. Ключи могут храниться только в авторизованном сервере, исключая хранение нескольких копий ключа в разных местах.

Когда исходящее сообщение передается процессором сообщений в USM, USM заполняет поля параметров безопасности в заголовке сообщения. Когда входное сообщение передается обработчиком сообщений в USM, обрабатываются значения параметров безопасности, содержащихся в заголоке сообщения. В параметрах безопасности содержатся:

· msgAuthoritativeEngeneID - snmpEngeneID авторизованного сервера, участвующего в обмене. Таким образом, это значение идентификатора отправителя для Trap, Response или Report или адресата для Get, GetNext, GetBulk, Set или Inform.

· msgAuthoritativeEngeneBoots - snmpEngeneBoots авторизованного сервера, участвующего в обмене. Объект snmpEngeneBoots является целым в диапазоне 0 - (2^{31} -1). Этот код характеризует число раз, которое SNMP-сервер был перезагружен с момента конфигурирования.

· msgAuthoritativeEngeneTime - nmpEngeneTime авторизованного сервера, участвующего в обмене. Значение этого кода лежит в диапазоне 0 - (2^{31} -1). Этот код характеризует число секунд, которое прошло с момента последней перезагрузки. Каждый авторизованный сервер должен инкрементировать этот код один раз в секунду.

· msgUserName - идентификатор пользователя от имени которого послано сообщение.

· msgAuthenticationParameters - нуль, если при обмене не используется аутентификация. В противном случае - это аутентификационный параметр.

· msgPrivacyParameters - нуль - если не требуется соблюдения конфимденциальности. В противном случае - это параметр безопасности. В действующей модели USM используется алгоритм шифрования DES.

Механизм аутентификации в SNMPv3 предполагает, что полученное сообщение действительно послано принципалом, идентификатор которого содержится в заголовке сообщения, и он не был модифицирован по дороге. Для реализации аутентификации каждый из принципалов, участвующих в обмене должен иметь секретный ключ аутентификации, общий для всех участников (определяется на фазе конфигурации системы). В посылаемое сообщение отправитель должен включить код, который является функцией содержимого сообщения и секретного ключа. Одним из принципов USM является прверка своевременности сообщения (смотри выше), что делает маловероятной атаку с использованием копий сообщения.

Система конфигурирования агентов позволяет обеспечить разные уровни доступа к MIB для различных SNMP-менеджеров. Это делается путем ограничения доступа некоторым агантам к определенным частям MIB, а также с помощью ограничения перечня допустимых операций для заданной части MIB. Такая схема управления доступом называется VACM (View-Based Access Control Model). В процессе управления доступом анализируется контекст (vacmContextTable), а также специализированные таблицы vacmSecurityToGroupTable, vacmTreeFamilyTable и vacmAccessTable.

SNMP-протокол служит примером системы управления, где для достижения нужного результата выдается не команда, а осуществляется обмен информацией, решение же принимается "на месте" в соответствии с полученными данными. Внедрены подсистемы аутентификации, информационной безопасности и управления доступом.

Структура SNMP MIB

Обрабатываемый агентом список объектов и их типов закладывается в него разработчиком, а станция управления получает эту информацию с помощью MIB (Management Information Base). MIB - текстовый файл, описывающий доступные объекты и их типы на языке, определяемом стандартом SMI (Structure and Identification of Management Information). Агент не использует этот файл при работе. MIB делится на модули, некоторые модули принимаются в виде стандартов, некоторые модули создаются разработчиками оборудования.

Разработчик управляемого оборудования (разработчик агента) должен предоставить список поддерживаемых агентом модулей. При описании модуля указывается какие объекты обязательны для реализации, а какие - нет. При описании агента можно указывать какие модули он поддерживает, в каком объеме и с какими модификациями.

На сегодня существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

База данных MIB-II не дает детальной статистики по характерным ошибкам кадров Ethernet, кроме этого, она не отражает изменение характеристик во времени, что часто интересует сетевого администратора.

Эти ограничения были впоследствии сняты новым стандартом на MIB — RMON MIB, который специально ориентирован на сбор детальной статистики по протоколу Ethernet, к тому же с поддержкой такой важной функции, как построение агентом зависимостей статистических характеристик от времени.

3.3 Недостатки протокола SNMP

Протокол SNMP служит основой многих систем управления, хотя имеет несколько принципиальных недостатков, которые перечислены ниже.

· Отсутствие средств взаимной аутентификации агентов и менеджеров. Единственным средством, которое можно было бы отнести к средствам аутентификации, является использование в сообщениях так называемой «строки сообщества» — «community string». Эта строка передается по сети в открытой форме в сообщении SNMP и служит основой для деления агентов и менеджеров на «сообщества», так что агент взаимодействует только с теми менеджерами, которые указывают в поле community string ту же символьную строку, что и строка, хранящаяся в памяти агента. Это, безусловно, не способ аутентификации, а способ структурирования агентов и менеджеров. Версия SNMP v.2 должна была ликвидировать этот недостаток, но в результате разногласий между разработчиками стандарта новые средства аутентификации хотя и появились в этой версии, но как необязательные.

· Работа через ненадежный протокол UDP (а именно так работает подавляющее большинство реализаций агентов SNMP) приводит к потерям аварийных сообщений (сообщений trap) от агентов к менеджерам, что может привести к некачественному управлению. Исправление ситуации путем перехода на надежный транспортный протокол с установлением соединений чревато потерей связи с огромным количеством встроенных агентов SNMP, имеющихся в установленном в сетях оборудовании. (Протокол CMIP изначально работает поверх надежного транспорта стека OSI и этим недостатком не страдает.) Разработчики платформ управления стараются преодолеть эти недостатки. Например, в платформе HP OV Telecom DM TMN, являющейся платформой для разработки многоуровневых систем управления в соответствии со стандартами TMN и ISO, работает новая реализация SNMP, организующая надежный обмен сообщениями между агентами и менеджерами за счет самостоятельной организации повторных передач сообщений SNMP при их потерях.

Практическое задание

Расшифровать вышеприведенные сообщения управляющего протокола, в соответствии с поставленными ниже в пп. 1…18 вопросами.

1. Фирму-поставщика оборудования сетевых интерфейсов

2. MAC-адреса источника и назначения

3. Тип протокола, обслуживаемого данным Ethernet-кадром

4. Версию протокола сетевого уровня

5. Приоритет сетевого уровня для данной дейтаграммы

6. Длину пакета сетевого уровня (в байтах)

7. Время жизни данной дейтаграммы

8. Протокол транспортного уровня (Dec’код и название)

9. Сетевой адрес отправителя

10. Сетевой адрес назначения

11. Транспортный порт отправителя

12. Транспортный порт получателя

13. Тип и версию протокола прикладного уровня

14. Длину дейтаграммы транспортного уровня (в байтах)

15. Тип и класс тэга протокола прикладного уровня

16. Длину сообщения протокола прикладного уровня

17. Длину и содержимое поля Community

18. Тип PDU и его длину (в байтах)

18.1. Для PDU типа Get-Request

18.1.1. Значение идентификатора запроса - RequestID

18.1.2. Значения полей ErrorStatus и Errorlndex

18.1.3. Длину поля, содержащего набор запрашиваемых характеристик

18.1.4. Перечень запрашиваемых характеристик (атрибутов) управляемого объекта*

18.2. Для PDU типа GetResponse

18.2.1. Значение идентификатора запроса – RequestID

18.2.2. Значения полей ErrorStatus и Errorlndex

18.2.3. Длину поля, содержащего набор характеристик управляемого объекта

18.2.4. Перечень характеристик (атрибутов) управляемого объекта*

18.2.5. Значения характеристик (атрибутов) управляемого объекта*

2.14. Практическая работа № 14
Задачи управления: анализ производительности сети

Задание 1. Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам. Для этого в командной строке введите имя утилиты без параметров и дополните **/?**.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname. Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5. Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

a) aspu.ru

b) mathmod.aspu.ru

c) yarus.aspu.ru

Задание 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера. Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотрите локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и

протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
7. Всегда ли можно узнать символьное имя узла по его ip-адресу?
8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

2.15. Практическая работа № 15
Задачи управления: анализ надежности сети

2.16. Практическая работа № 16
Управление безопасностью в сети

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсе-ти	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка базовых мер безопасности на маршрутизаторе

Часть 3. Настройка базовых мер безопасности на коммутаторе

Общие сведения/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к

устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы разрешать SSH-соединения для удаленного управления. Кроме того, вы должны будете настроить основные эффективные меры обеспечения безопасности через интерфейс командной строки операционной системы Cisco IOS. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они правильно внедрены и работают без ошибок.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образом или аналогичная модель)

1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)

1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)

Консольные кабели для настройки устройств Cisco IOS через консольные порты

Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Выполните настройку маршрутизатора и коммутатора.

Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.

Назначьте устройству имя в соответствии с таблицей адресации.

Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблице адресации.

Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

R1(config)# **service password-encryption**

Шаг 2: Установите более надежные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надежных паролей. В рекомендациях должны быть определены сочетания в пароле букв, цифр и специальных символов и его минимальная длина.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями.

R1(config)# **enable secret Enablep@55**

Установите минимальную длину 10 символов для всех паролей. R1(config)# **security passwords min-length 10**

Шаг 3: Разрешите подключения по протоколу SSH.

В качестве имени домена укажите **CCNA-lab.com**.

R1(config)# **ip domain-name CCNA-lab.com**

Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 15).

R1(config)# **username SSHadmin privilege 15 secret Admin1p@55**

Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.

R1(config-line)# **login local**

R1(config-line)# **exit**

Создайте ключ шифрования RSA с длиной 1024 бит.

R1(config)# **crypto key generate rsa modulus 1024**

Шаг 4: Обеспечьте защиту консоли и линий VTY.

Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения в случае отсутствия активности в течение заданного времени. Если сетевой администратор вошел в систему сетевого устройства, а потом был внезапно вынужден покинуть рабочее место, то по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведенные ниже команды обеспечивают закрытие сеанса линии связи через пять минут отсутствия активности.

R1(config)# **line console 0**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **line vty 0 4**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **exit**

R1(config)#

Команда, приведенная ниже, не разрешает вход в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль. Низкое значение этого таймера установлено специально для данной лабораторной работы.

R1(config)# **login block-for 30 attempts 2 within 120** Что означает **2 within 120** в приведенной выше команде?

_ неудачные попытки в течение 120 секунд

Что означает **block-for 30** в приведенной выше команде?

заблокировать на 30 секунд

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные администратором, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol
Embedded-Service-Engine0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Serial0/0/0 unassigned YES NVRAM administratively down down Serial0/0/1
unassigned YES NVRAM administratively down down R1#

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet.

Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.

Нет, Telnet не был активирован во время настройки маршрутизатора.

С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH.

Разрешает ли R1 подключение по протоколу SSH? _____Да.

Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.

Что произошло после ввода неправильных данных для входа в систему во второй раз?

Маршрутизатор отклоняет входящие соединения по протоколу SSH.

Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере команда **show login** была введена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет разрешать попытки входа в систему в течение еще 14 секунд.

R1# **show login**

A default login delay of 1 second is applied.
No Quiet-Mode access list has been configured.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 120 seconds or less, logins will be disabled for 30 seconds.
Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 14 seconds.
Denying logins from all sources.

R1#

По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **Admin1p@55**.

Что отобразилось после успешного входа в систему?

Баннер MOTD и интерпретатор

Войдите в привилегированный режим EXEC и введите в качестве пароля **Enablep@55**.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Нет, так как login block-for защищает вход в консоль, а не в _ привилегированный режим EXEC.
Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.
Часть 3: Настройка базовых мер безопасности на коммутаторе
Шаг 1: Зашифруйте открытые пароли.
S1(config)# **service password-encryption**
Шаг 2: Установите более надежные пароли на коммутаторе.
Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями по установке надежного пароля.
S1(config)# **enable secret Enablep@55**
Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960 недоступна.
Шаг 3: Разрешите подключения по протоколу SSH.
В качестве имени домена укажите **CCNA-lab.com**.
S1(config)# **ip domain-name CCNA-lab.com**
Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к коммутатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 1).
S1(config)# **username SSHadmin privilege 1 secret Admin1p@55**
Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.
S1(config)# **line vty 0 15**
S1(config-line)# **transport input ssh**
Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.
S1(config-line)# **login local**
S1(config-line)# **exit**
Создайте ключ шифрования RSA с длиной 1024 бит.
S1(config)# **crypto key generate rsa modulus 1024**
Шаг 4: Обеспечьте защиту консоли и линий VTY.
Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.
S1(config)# **line console 0**
S1(config-line)# **exec-timeout 10 0** S1(config-line)# **line vty 0 15**
S1(config-line)# **exec-timeout 10 0**
S1(config-line)# **exit**
S1(config)#
Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа в течение 120 секунд. Низкое значение этого таймера установлено специально для данной лабораторной работы.
S1(config)# **login block-for 30 attempts 2 within 120** S1(config)# **end**
Шаг 5: Убедитесь, что все неиспользуемые порты отключены.
По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты. а. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.
S1# **show ip interface brief**
Interface IP-Address OK? Method Status Protocol

```
Vlan1              192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down    FastEthernet0/20
unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down    GigabitEthernet0/2
unassigned      YES unset  down                  down
S1#
```

Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**.

```
S1(config)# interface range f0/1–4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

Убедитесь, что все неактивные интерфейсы отключены администратором.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
```

FastEthernet0/15 unassigned YES unset administratively down down
FastEthernet0/16 unassigned YES unset administratively down down
FastEthernet0/17 unassigned YES unset administratively down down
FastEthernet0/18 unassigned YES unset administratively down down
FastEthernet0/19 unassigned YES unset administratively down down
FastEthernet0/20 unassigned YES unset administratively down down
FastEthernet0/21 unassigned YES unset administratively down down
FastEthernet0/22 unassigned YES unset administratively down down
FastEthernet0/23 unassigned YES unset administratively down down
FastEthernet0/24 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down GigabitEthernet0/2 unassigned YES unset administratively down down S1#

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

Убедитесь, что протокол Telnet на коммутаторе отключен.

Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.

Появился ли баннер после успешного входа в систему? _____

Войдите в привилегированный режим EXEC, используя **Enablep@55** в качестве пароля.

Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вопросы для повторения

В части 1 для консоли и линий VTY в вашей базовой конфигурации была введена команда **password cisco**. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?

При подключении через консольный порт будет запрошен именно этот пароль "cisco".

Распространяется ли команда **security passwords min-length 10** на настроенные ранее пароли, содержащие меньше десяти символов?

Нет.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам 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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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 определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

2.17. Практическая работа № 17
Учет трафика в сети

Порядок выполнения работы:

1. Установить на компьютер программу WinPcap и оболочку к ней Wireshark либо iris, либо esa. Запустить сеанс перехвата пакетов. Запустить для интенсивной генерации кадров браузер и откройте в нем любой сайт по выбору.
2. Установить какой тип кадров Ethernet в данной сети.
3. На основании собранной статистики определить к коммутационному оборудованию какого типа подключен ваш компьютер.

Разберитесь, какие типы оборудования могут в принципе использоваться в вашей сети.

Сортируйте пакеты по адресам отправителя и получателя. Определите, какие группы кадров по адресам присутствуют в собранной статистике. Это поможет сделать выводы.

Поможет также знание собственного IP адреса.

2.18. Практическая работа № 18
Средства мониторинга компьютерных сетей

Задание:

Изучить аппаратные и программные средства мониторинга сети, функциональное использование приборов мониторинга сети (теоретический материал).

Разработать презентацию по теме занятия.

Письменно ответить на вопросы:

1. Опишите группы оборудования для диагностики и сертификации кабельных систем.
2. Опишите по одному прибору из каждой группы приборов мониторинга сети.
3. Опишите основные электромагнитные характеристики кабельных систем.
4. Какую информацию можно получить с помощью программ для мониторинга сети?
5. Опишите группу агентов SNMP.

6. Опишите группу агентов RMON. Заполните отчет, покажите результат работы преподавателю, защитите работу.

2.19. Практическая работа № 19
Средства анализа сети с помощью команд сетевой операционной системы

Краткие теоретические и справочно-информационные материалы по теме занятия.

Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, который дает базу для измерения реакции сети на изменения и перегрузки. Чтобы осуществить сетевую передачу, нужно проверить корректность подключения клиента к сети, наличие у клиента хотя бы одного протокола сервера, знать IP-адрес компьютеров сети и т. д. Поэтому в сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок. Утилиты запускаются из сеанса интерпретатора команд Windows XP (Пуск -> Выполнить -> cmd).

1. Сетевые утилиты

1.1. Утилита *hostname*

Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды *hostname:*

C:\DocumentsandSettings\Администратор>hostname

1.2. Утилита *ipconfig*

Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую конфигурацию IP-адресов компьютеров сети. Синтаксис утилиты *ipconfig:*

ipconfig [/all | /renew [адаптер] | */release* [адаптер]],

где *all* - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-

маршрутизации и др. Без этого параметра команда *ipconfig* выводит только IP-адреса, маску подсети и основной шлюз;

/renew [адаптер] - обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol - автоматическая настройка IPадресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров;

/release [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты *ipconfig /release,* IP-адрес становиться доступен для назначения другому компьютеру.

Запущенная без параметров, команда *ipconfig* выводит полную конфигурацию TCP/IP, включая IP адреса и маску подсети.

Пример использования *ipconfig* без параметров:

C:\Documents and Settings\Администратор>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

DNS-суффикс этого подключения . . :
IP-адрес . . . . . : 10.10.11.70

Маска подсети . . . . . : 255.255.252.0
Основной шлюз . . . . . : 10.10.10.1

1.3. Утилита *net view*

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты *netview*:

*net view [\\компьютер | /domain[:*домен]]; *net view /network:nw* [\\компьютер]

где *компьютер* - задает имя компьютера для просмотра общих ресурсов;

*/domain[:*домен] - задает домен (рабочую группу), для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;

/network:nw - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети NetWare. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.

Вызванная без параметров, утилита выводит список компьютеров в текущем домене (рабочей группе).

Пример с параметром *компьютер:*

C:\DocumentsandSettings\Администратор>netview \\- /Domain:Lab-261
Общие ресурсы на \\-

Имя общего ресурса Тип Используется как Комментарий

NONE (H) Диск
Команда выполнена успешно.

1.4.Утилита *ping*

Проверяет соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *ping:*

ping [-t] [-a] [-n счетчик] [-l *длина] [-f]* [-i *ttl]* [-v *тип] [-r счетчик]* [*-s число] [[-j список комп] | [-k список комп]] [-w интервал] список назн,* где *-t* - повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;

-a - разрешает имя компьютера в адрес;

-n счетчик - передается число пакетов ECHO, заданное параметром. По умолчанию - 4;

-l *длина* - отправляются пакеты типа ECHO, содержащие порцию данных заданной длины. По умолчанию - 32 байта, максимум - 65500; -f - отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;

-i *ttl* - устанавливает время жизни пакетов TTL (Time To Live); -v *тип* - устанавливает тип службы (Type Of Service) пакетов; *-r счетчик* - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;

-s число - задает число ретрансляций на маршруте, где делается отметка времени;

-j список комп - направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно
9;

-k список комп - направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;

-список назн - указывает список компьютеров, которым направляются запросы;

Пример использования утилиты ping с параметром *список назн:*

C:\Documents and Settings\Администратор>ping 10.10.10.1

Обмен пакетами с 10.10.10.1 по 32 байт:

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128 Статистика Ping для 10.10.10.1:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс:

Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

1.5. Утилита netstat

Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *netstat:*

netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал],

где *-a* - выводит все подключения и сетевые порты. Подключения сервера обычно не
выводятся;

-e - выводит статистику Ethernet. Возможна комбинация с ключом *-s;*

-n - выводит адреса и номера портов в шестнадцатеричном формате (а не имена); *s* - выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (InternetControl Message Protocol) и IP. Ключ *-p* может быть использован для указания подмножества стандартных протоколов;

-p протокол - выводит соединения для протокола, заданного параметром. Параметр может иметь значения *tcp* или*udp.* Если используется с ключом *-s* для вывода статистики по отдельным протоколам, то параметр может принимать значения *tcp, udp, icmp* или *ip; -r* - выводит таблицу маршрутизации; *интервал* - обновляет выведенную статистику с заданным в секундах интервалом. Нажатие клавиш CTRL+Сстанавливает обновление статистики. Если этот параметр пропущен, *netstat* выводит сведения о текущей конфигурации один раз.

1.6. Утилита *tracert*

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью посылки эхо-пакетов протокола ICMP с различными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета.

Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP «Time Exceeded». Утилита *tracert* определяет

маршрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное допустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «TimeExceeded», полученных от промежуточных маршрутизаторов. Однако некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты*tracert.* Синтаксис утилиты *tracert:*

tracert [-d] [-h макс_узл] [-j список компьютеров] [-w интервал] точка назн,

где *-d* - отменяет разрешение имен компьютеров в их адреса;

-h макс_узл - задает максимальное количество ретрансляций, используемых при поиске точки назначения;

-j список компьютеров - задает список_компьютеров для свободной маршрутизации;

-w интервал - задает интервал в миллисекундах, в течение которого будет ожидаться ответ; *точка назн* - указывает имя конечного компьютера.

Пример использования утилиты *tracert:*

C:\DocumentsandSettings\Администратор>tracert 10.10.10.1

Трассировка маршрута к 10.10.10.1 с максимальным числом прыжков 30

1 <1 мс <1 мс <1 мс 10.10.10.1 Трассировка завершена.

1.7.Утилита *net use*

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты *net use:*

*net use [устройство | *] [\\компьютер\ресурс[\том]] [пароль | *]] [/user:[домен\]имя пользователя] [[/delete] | [/persistent:{yes | no}]] net use устройство [/home[пароль | *]] [/delete: {yes | no}] net use [/persistent:{yes | no}],*

где *устройство* - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

компьютер\ ресурс - указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов; *\том* - задает имя тома системы Novell NetWare. Для подключения к серверамNovell NetWare должна быть запущена служба клиента сети Novell NetWare (для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server); *пароль* - задает пароль, необходимый для подключения к общему ресурсу;

* - выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;

/user - задает другое имя пользователя для подключения к общему ресурсу; *домен* - задает имя другого домена. Если домен не указан, используется текущий домен; *имя пользователя* - указывает имя пользователя для подключения;

/delete - отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения;

/home - подключает пользователя к его основному каталогу;

/persistent -управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными; *yes* - сохраняет все существующие соединения и восстанавливает их при следующем
подключении; *no* - не сохраняет выполняемые и последующие подключения. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ */delete*. Вызванная без параметров утилита *net use* извлекает список сетевых подключений. Пример вызова команды *net use:*

C:\Documents and Settings\Администратор>net use

1.8.Утилита*Netshare*

Управление общими ресурсами. При вызове команды *netshare* без параметров выводятся сведения обо всех общих ресурсах локального компьютера. **Синтаксис**

net share [*имя_ресурса*] **net share** [*имя_ресурса=диск***:***путь* [{**/users:***число*|**/unlimited**}] [**/remark:"***текст***"**]
[**/cache:** {**manual**|**automatic**|**no**}]]**netshare** [*имя_ресурса* [{**/users:***число*|**unlimited**}] [**/remark:"***текст***"**]
[**/cache:** {**manual**|**automatic**|**no**}]] **net share** [{*имя_ресурса*|*диск***:***путь*} **/delete**]

Параметры *имя_ресурса*- Сетевое имя общего ресурса. Команда **net share** *имя_ресурса* выводит сведения об отдельном ресурсе. *диск***:***путь*- Абсолютный путь к папке, которую требуется сделать общей. **/users:***число*- Максимальное количество пользователей, которым разрешен одновременный доступ к общему ресурсу.

/unlimited- Отмена ограничения на число пользователей, которым разрешен одновременный доступ к общему ресурсу.

/remark:"*текст***"**-Добавление описательного комментария к ресурсу. Текст следует заключать в кавычки.

/cache:automatic- Включение автономного кэширования клиентов с автоматической реинтеграцией.

/cache:manual- Включение автономного кэширования клиентов с реинтеграцией вручную.

/cache:no- Оповещение клиента о невозможности автономного кэширования.

/delete- Отмена общего доступа к ресурсу. **net help** *команда* -
Отображение справки для указанной команды **net**.

Заметки

- Чтобы предоставить общий доступ к папке, имя которой содержит пробелы, заключите диск и путь к папке в кавычки (например **"C:\Новая папка"**).
- При запросе списка всех общих ресурсов компьютера выводятся: имя общего ресурса, имена устройств или путь, связанный с устройством, а также комментарий к этому ресурсу.
- Когда общий ресурс создается на сервере, его конфигурация сохраняется. После остановки службы «Сервер» все общие ресурсы отключаются, но после следующего запуска службы «Сервер» они будут восстановлены. Имена общих ресурсов, заканчивающиеся знаком **$**, не отображаются при обзоре локального компьютера с удаленного компьютера.

Примеры

Чтобы вывести сведения об общих ресурсах компьютера, введите: **net share**
Чтобы сделать папку «C:\Данные» общим ресурсом и включить примечание к нему, введите:

net shareОбщиеДанные=c:\Данные /remark:"Для отдела 123"

Чтобы отменить общий доступ к ресурсу Общие Данные, созданному в предыдущем примере, введите: **net shareОбщиеДанные /delete**

Чтобы сделать папку «C:\Список рисунков» общим ресурсом Список, введите: **net share**

Список="c:\Список рисунков"

3. Рекомендации и замечания

На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику локальных сетей. Они позволяют минимизировать усилия по поиску и исправлению ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество программ этогонаправления: Monitor It, Nautilus NetRanger, CiscoWorks2000, ServiceSentinel и д.р. Они распространяются через Internet на условиях freeware. Windows NT Server обладаетвстроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

(При выполнении консольных команд сделать скриншот экрана и сохранить в Вашей папке в документе WORD!)

2. Получите имя своего компьютера;
3. Выведите список доступных сетевых ресурсов своего компьютера;
4. Спросив у соседа слева имя компьютера, просмотрите его общие ресурсы;
5. Получив свой IP адрес, «опросите» его. Сначала с минимальным размером пакета, затем с максимально возможным;
6. Используя ранее полученное от соседа слева имя компьютера, определите его IP адрес;
7. Используя IP адрес полученный в предыдущем пункте, проверьте подключение к нему, используя число ретрансляций на маршруте, где делается отметка времени, равное количеству его общих сетевых ресурсов;
8. Просмотрите список всех сетевых портов на вашем компьютере и сосчитайте количество открытых (прослушиваемых);
9. Определите маршрут до сайта yandex.ru, с максимальным числом прыжков, равным значению полученному в предыдущем пункте;
10. Очистите текущую конфигурацию DHCP, затем обновите еѐ;
11. Изучив утилиту **netsh**, измените с ее помощью свой IP адрес на статический – 192.168.1., маска подсети – 255.255.255.0;
12. Проверьте подключение к IP адресу из п.2.5;
13. Используя **netsh**, верните свой IP адрес на получение по DHCP;
14. Сделайте диск C:\ общим сетевым ресурсом, используя в качестве имени Фамилию, а в качестве комментария строку «Моя первая Шара»;
15. Выведите список общих сетевых ресурсов соседа слева;

16. Подключите созданный соседом ресурс в качестве сетевого диска «Z:»;
17. Выведите список подключений вашего компьютера;
18. Отключите сетевой диск «Z:» ;
19. Сделайте выводы;

2.20. Практическая работа № 20
Эксплуатация объектов сетевой инфраструктуры

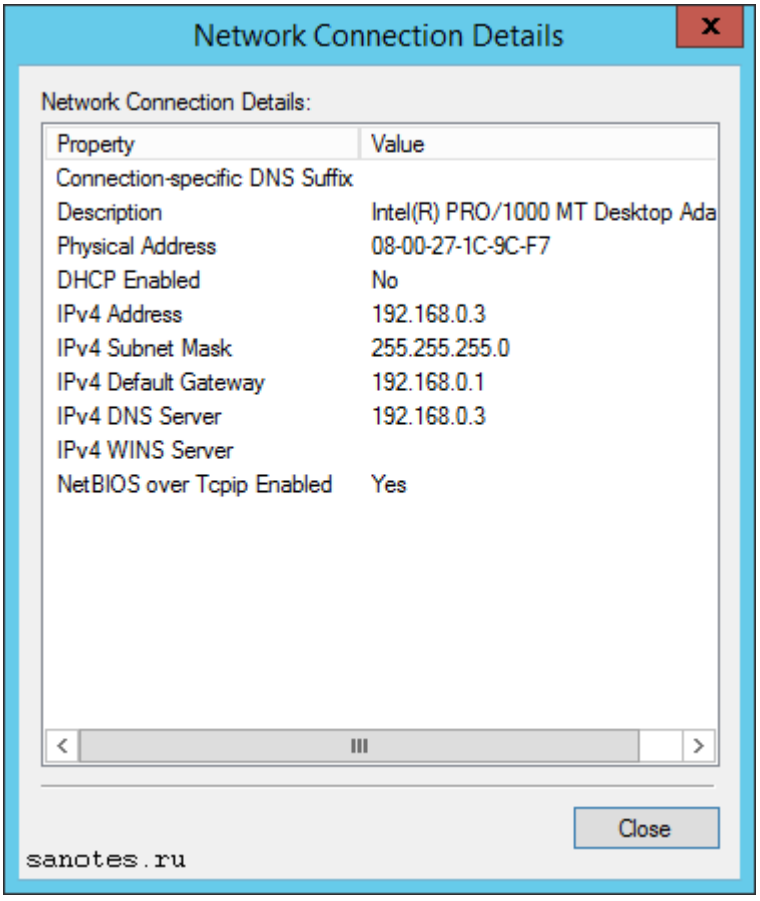
1) Основной контроллер домена, ОС — Windows Server 2016 R2 with GUI.

2) Дополнительный контроллер домена (на случай выхода из строя основного), ОС — Windows Server 2016 R2 Core.

3) Контроллер домена только для чтения (RODC), находящийся в филиале компании за vpn-каналом, ОС — Windows Server 2012 R2 Core.

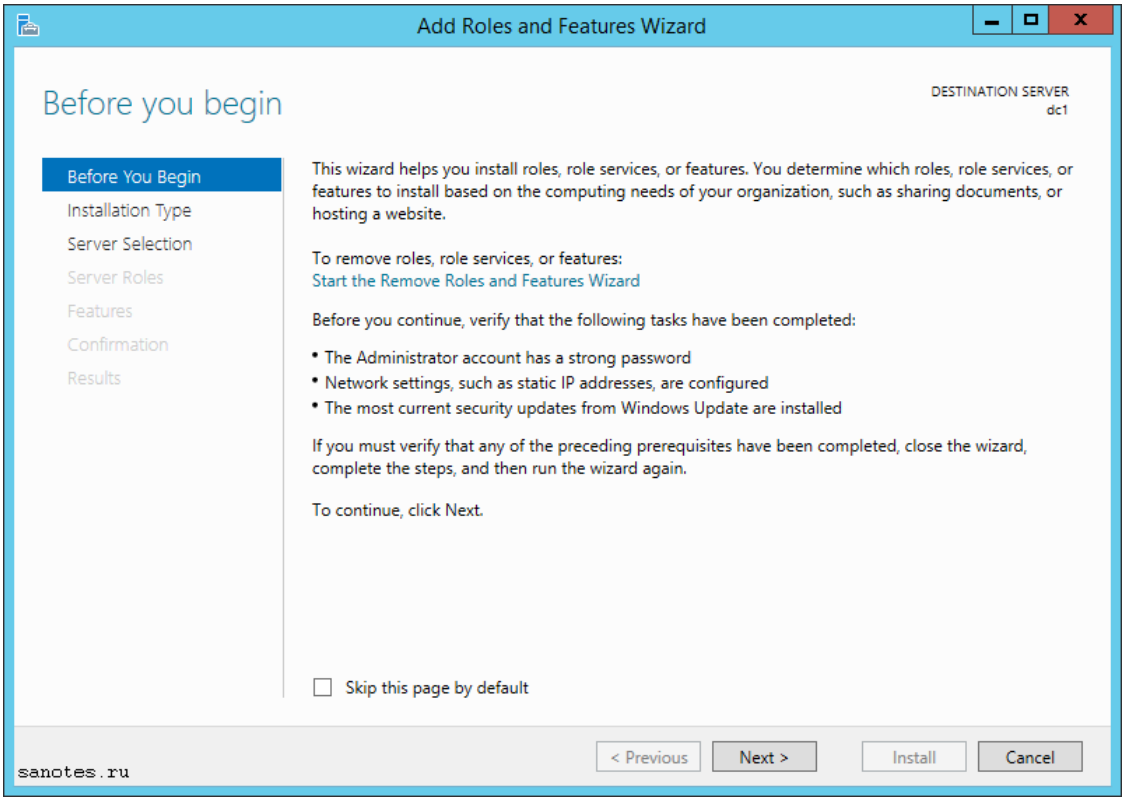
Шаг 1: Установка первого контроллера домена. Подготовка.

Перед запуском мастера ролей, серверу необходимо задать сетевое имя и настроить ip-адрес. Настройки TCP/IP укажем как на скриншоте ниже.

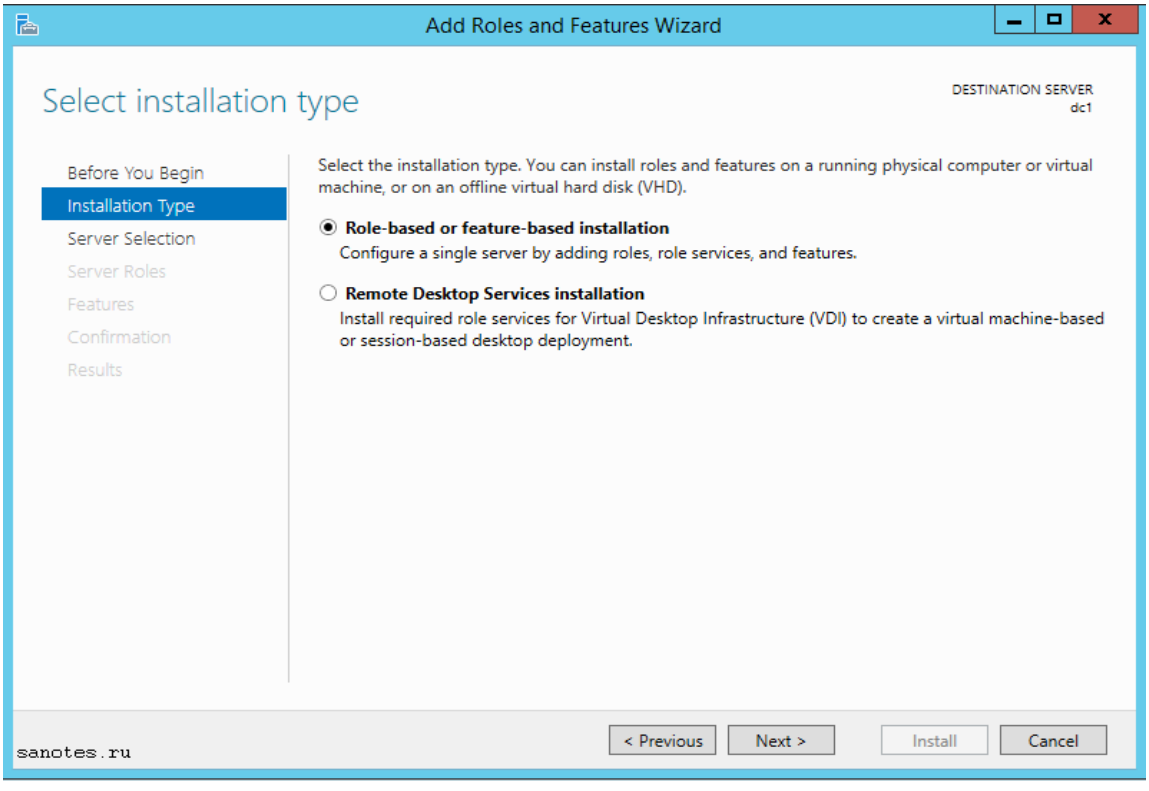


Запускаем диспетчер сервера — **Server Manager -> Dashboard -> Configure this local server -> Add Role and Features Wizard.** На первом экране мастер нам сообщает, что перед тем как продолжить, должен быть установлен сложный пароль администрато-

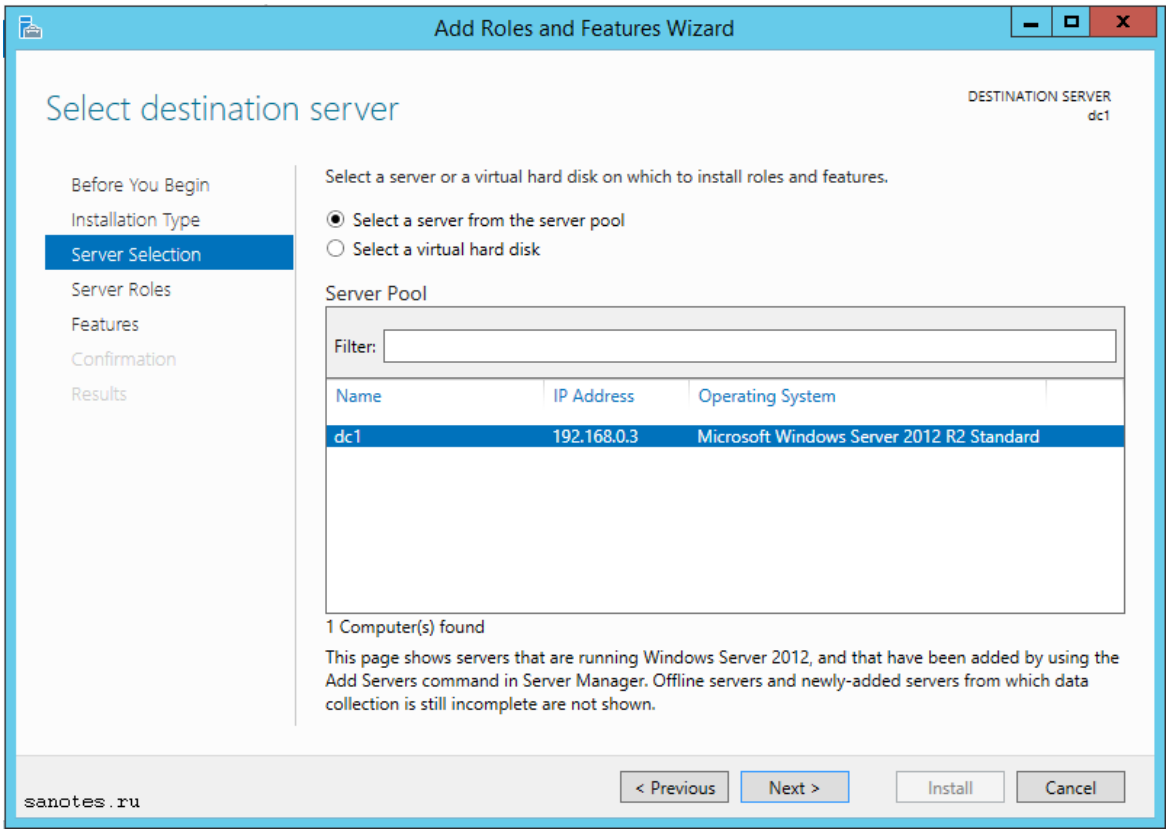
ра, в настройках сети указан статический ip-адрес, установлены последние обновления. Если все это сделано, то нажимаем Next.



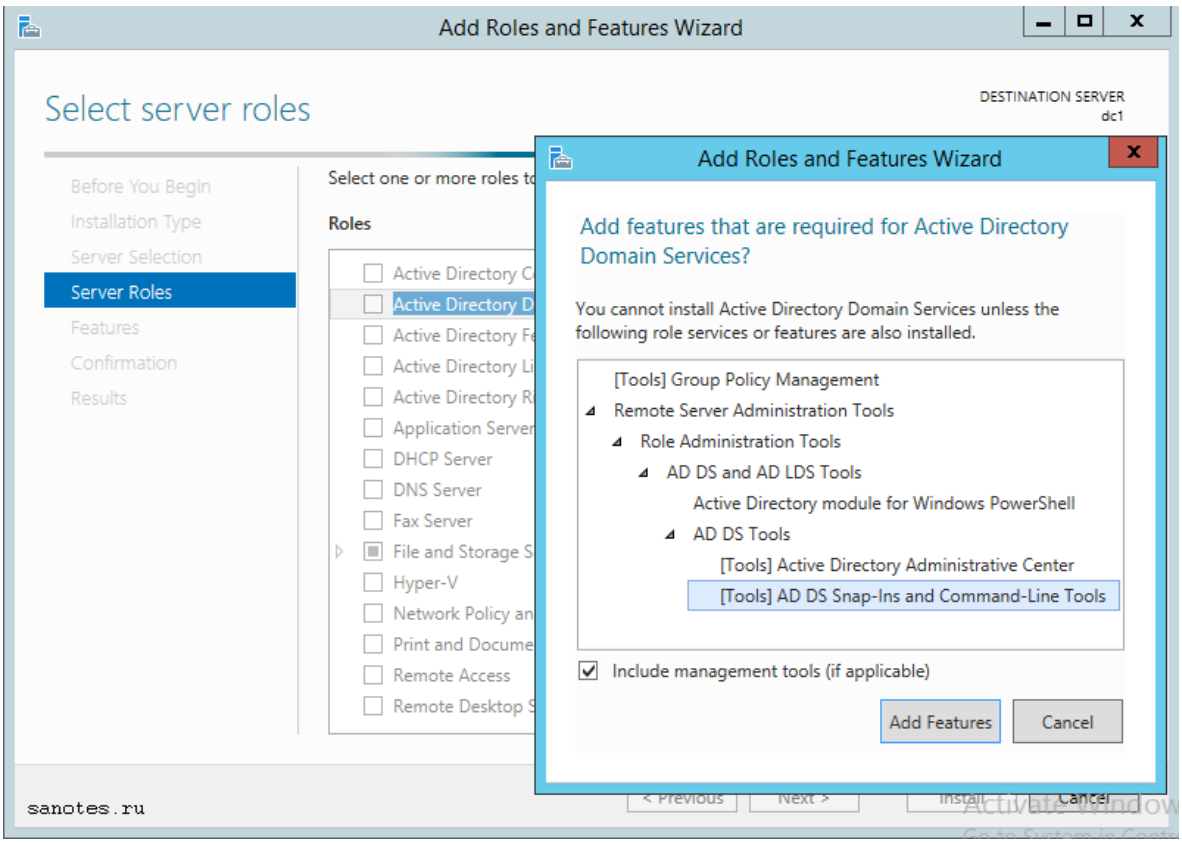
На следующем экране, выбираем первый пункт **Role-based or feature-based installation** (Базовая установка ролей и компонентов). Второй пункт **Remote Desktop Service installtion** предназначен исключительно для установки роли удаленных рабочих столов.



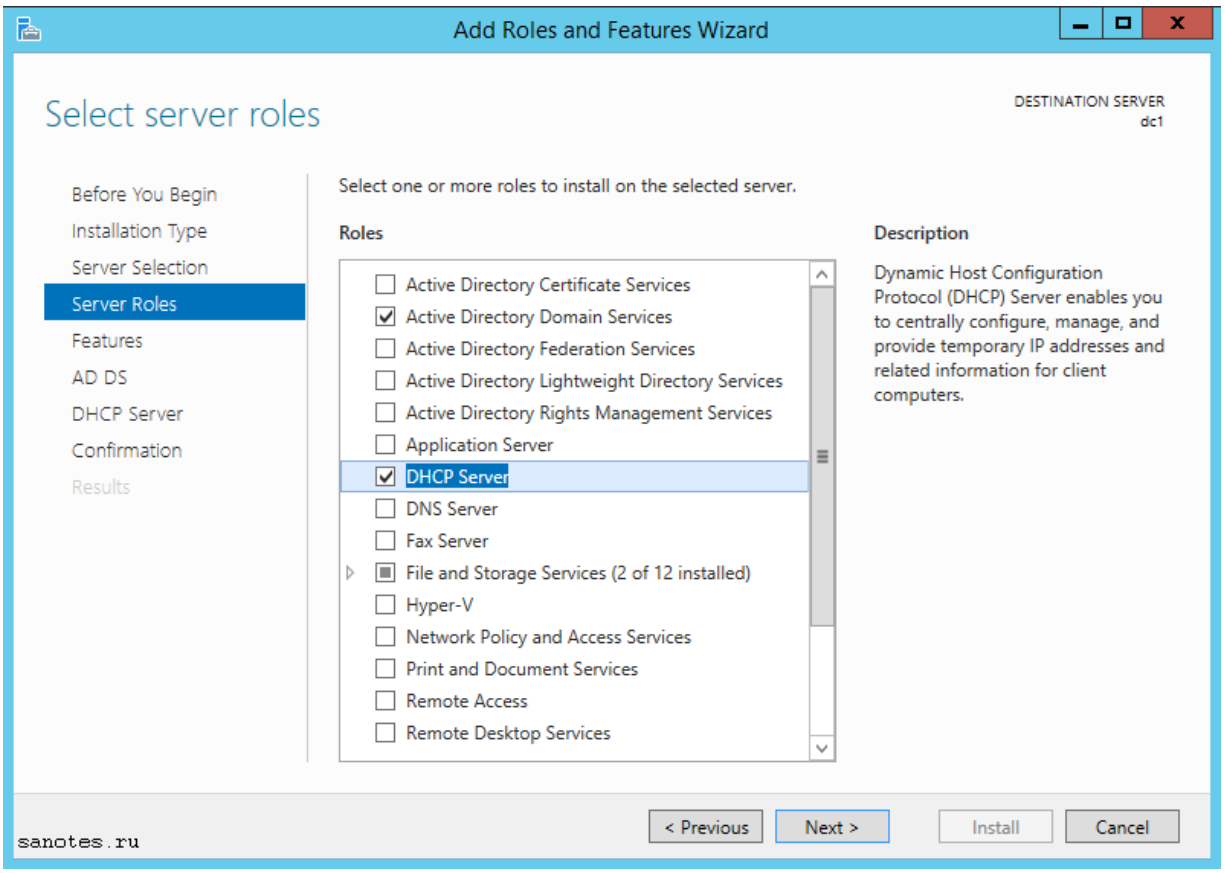
На экране **Select Destination server** диспетчер предлагает нам, выбрать сервер из пула или расположенный на VHD-диске. Поскольку у нас пока только один локальный сервер, то нажимаем Next.



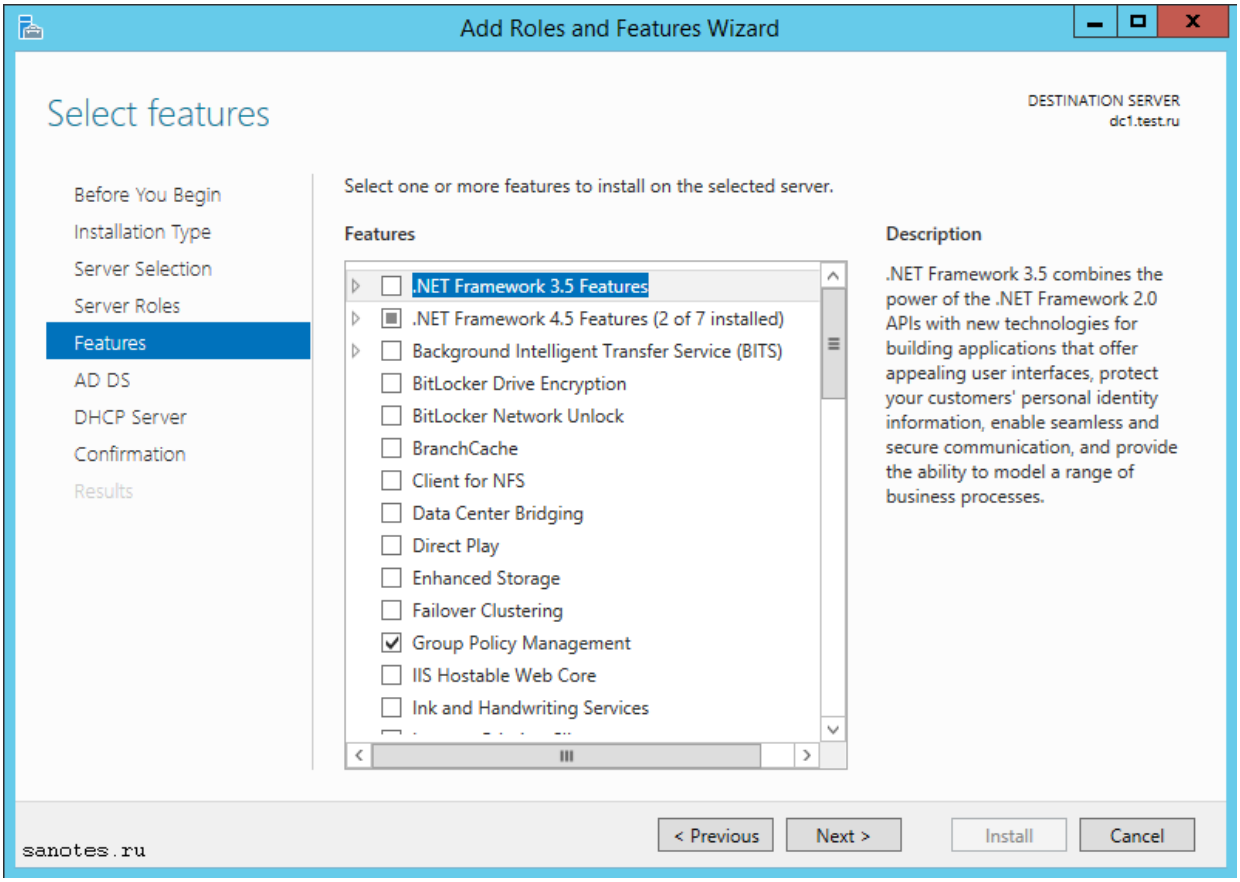
Выбираем **Active Directory Domain Services** (Доменные службы Active Directory), после чего появится окно с предложением добавить роли и компоненты, необходимые для установки роли AD. Нажимаем кнопку Add Features и затем Next.



Обычно, на серверах с AD DS имеет смысл, параллельно разворачивать DHCP Server, поэтому отмечаем его для установки так же. Соглашаемся с установкой компонент. Нажимаем Next.



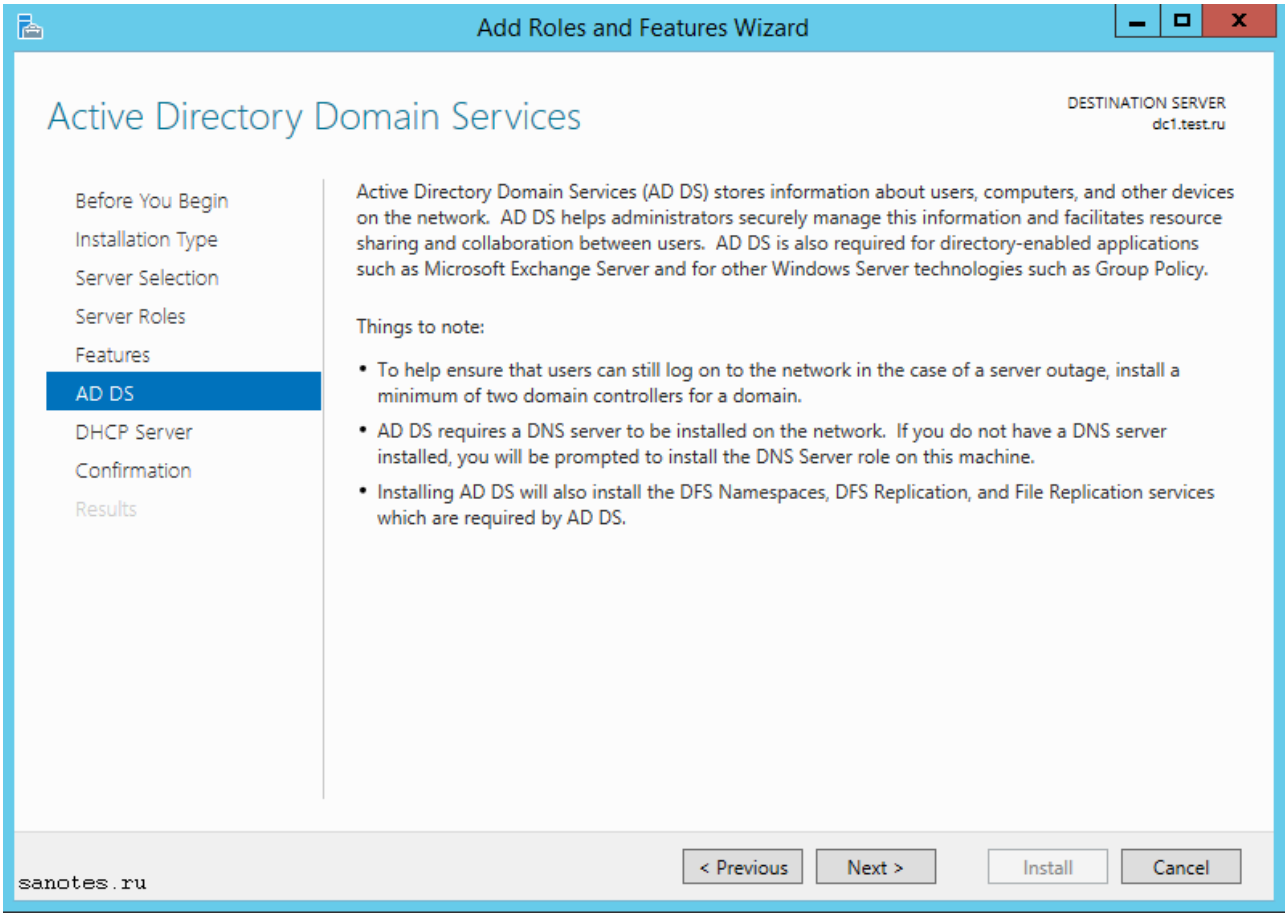
На экране **Features** предлагается выбрать дополнительные компоненты. На контроллере домена ничего экстраординарного обычно не требуется, поэтому нажимаем Next.



На завершающих этапах подготовки к установке, на вкладке AD DS, мастер даст нам некоторые пояснения, а именно, в случае, если основной контроллер будет не доступен, то рекомендуется в одном домене держать как минимум два контроллера.

Службы **Active Directory Domain Services** требуют установленного в сети DNS-сервера. В случае если он не установлен, то роль DNS Server будет предложена для установки.

Так же, службы **Active Directory Domain Services** требуют установки дополнительных служб пространства имен, файловой и DFS репликации **(DFS Namespace, DFS Replication, File Replication)**. Нажимаем Next.



На последнем экране **Confirm installation selection** (Подтверждение устанавливаемых компонентов), можно экспортировать конфигурацию в xml-фаил, который поможет быстро установить еще один сервер с идентичными настройками. Для этого потребуется на новом сервере, используя PowerShell, ввести следующую команду:

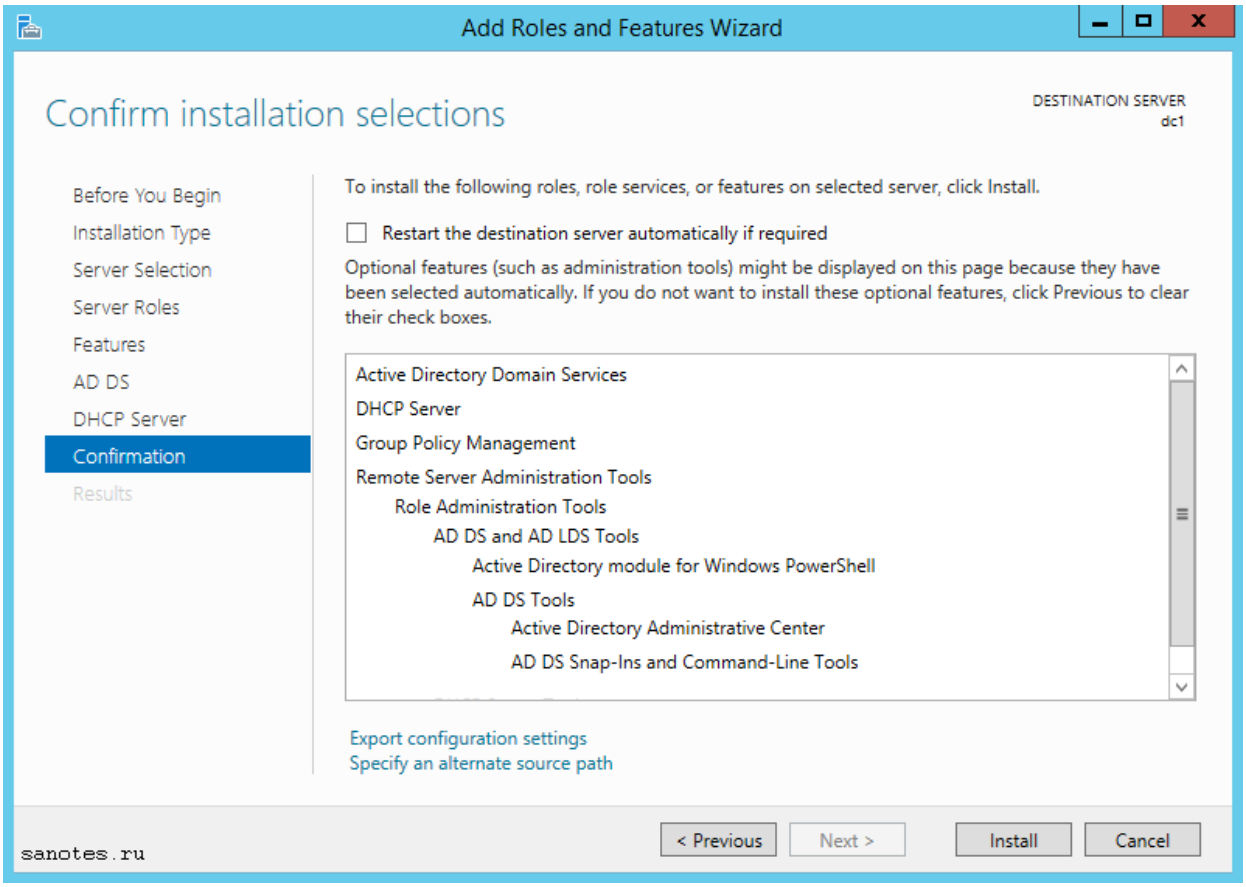
```
Install-WindowsFeature –ConfigurationFilePath
D:\ConfigurationFiles\DeploymentConfigTemplate.xml
```

или если требуется задать новое имя серверу, набираем:

```
Install-WindowsFeature –ConfigurationFilePath
```

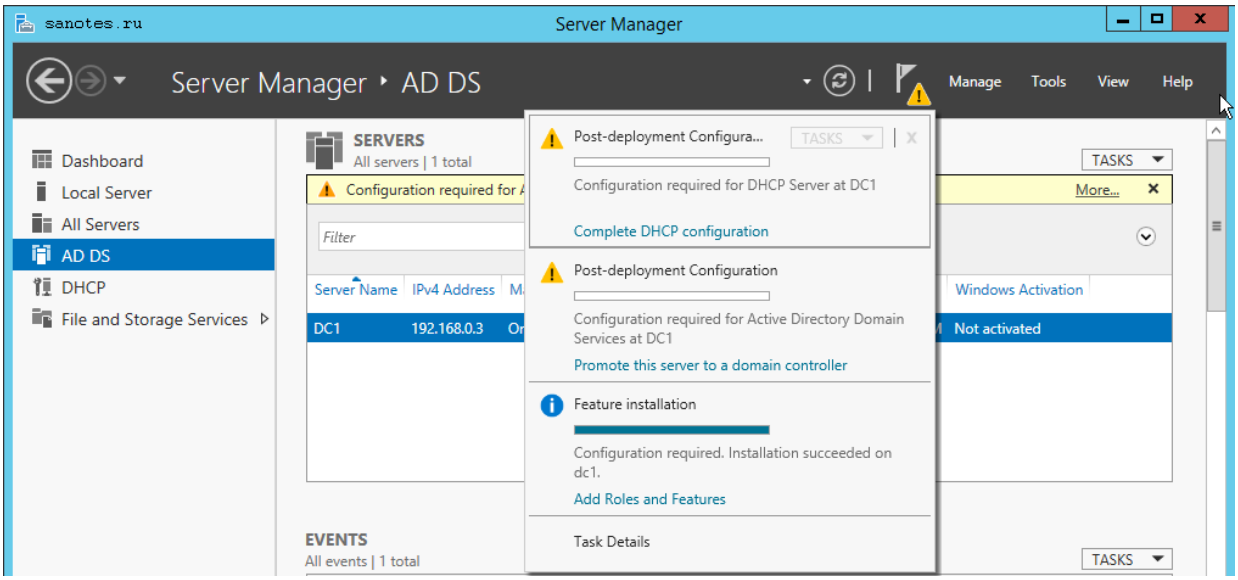
D:\ConfigurationFiles\ADCSConfigFile.xml -ComputerName $servername

В конце нажимаем Install. Дожидаемся окончания процесса установки.



Шаг 2: Установка первого контроллера домена. Настройка служб Active Directory, DNS, DHCP.

Теперь нажимаем на значок треугольника с восклицательным знаком и выбираем сначала **Promote this server to domain controller** (Повысить этот сервер до контроллера домена). Позже запустим процесс развертывания DHCP-сервера.



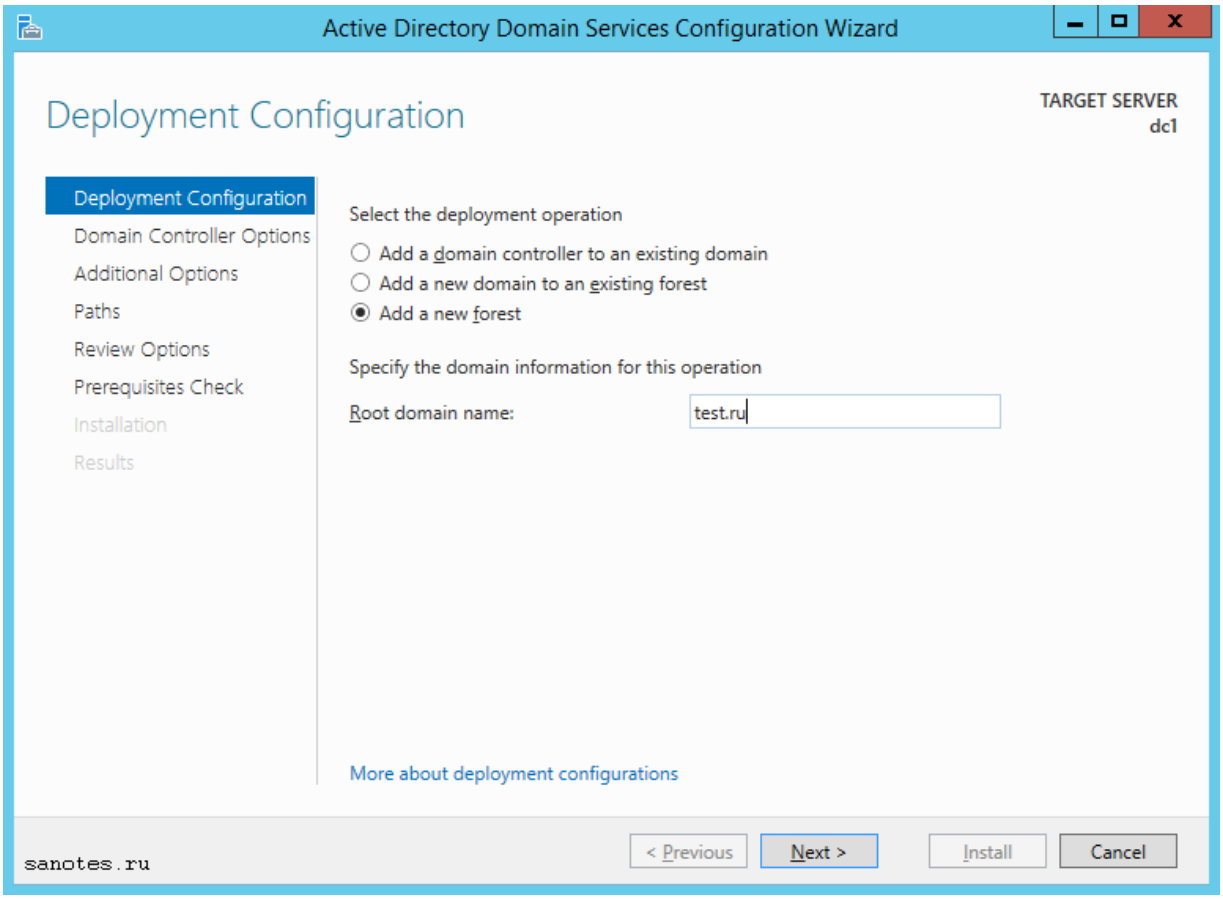
Запустится мастер **Active Directory Domain Services Configuration Wizard** (Мастер конфигурации доменных служб Active Directory). Доступно, три варианта развертывания, если:

Add New Forest — создать новый корневой домен в новом лесу. Используется для новой «чистой» установки Active Directory; (например 'test.ru')

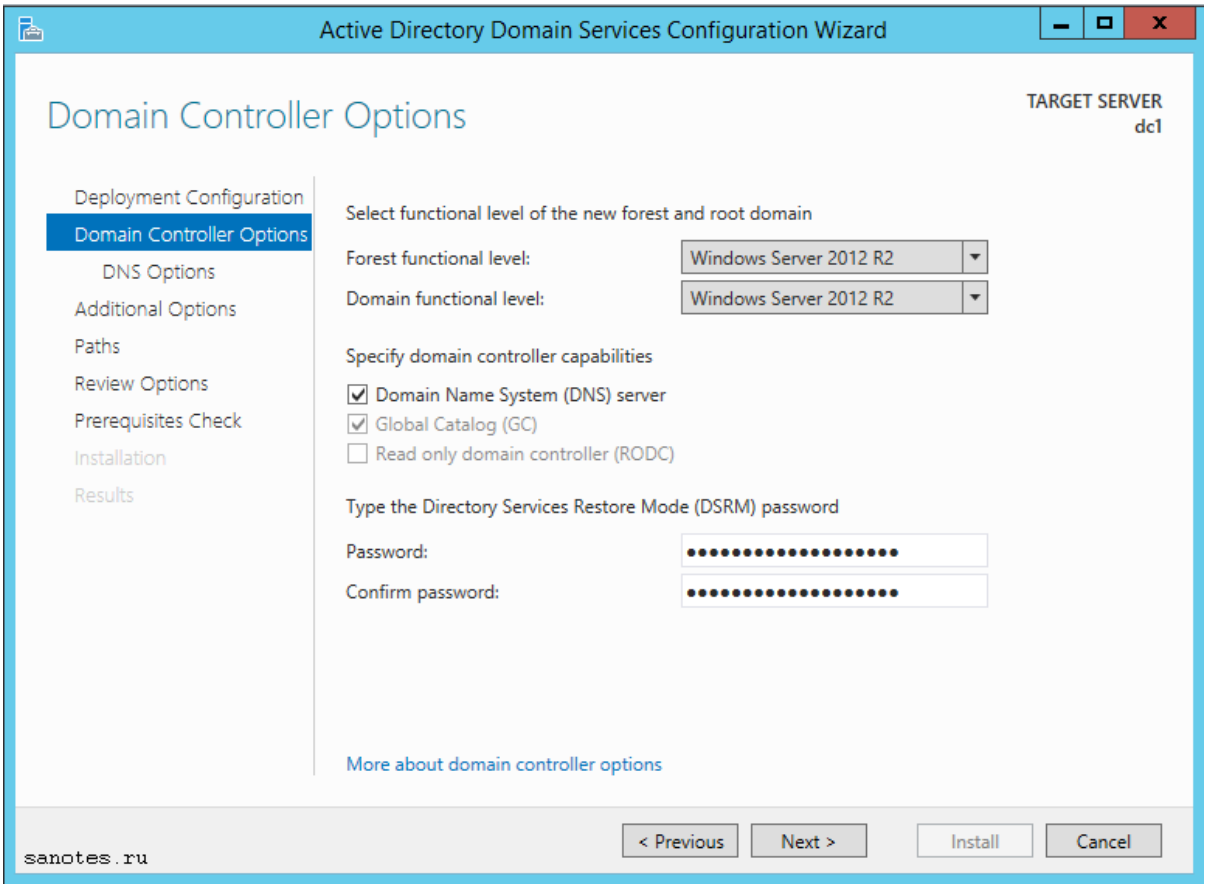
Add a new domain to an existing forest — добавить новый домен в существующем лесу, возможные варианты: *Tree Domain* - корневой домен нового дерева в существующем лесу (например 'test2.ru' параллельно с 'test.ru') или *Child Domain* — дочерний домен в существующем лесу (например 'corp.test.ru')

Add a domain controller to an existing domain — добавить дополнительный контроллер домена в существующем домене, используется для резервного или филиального домена.

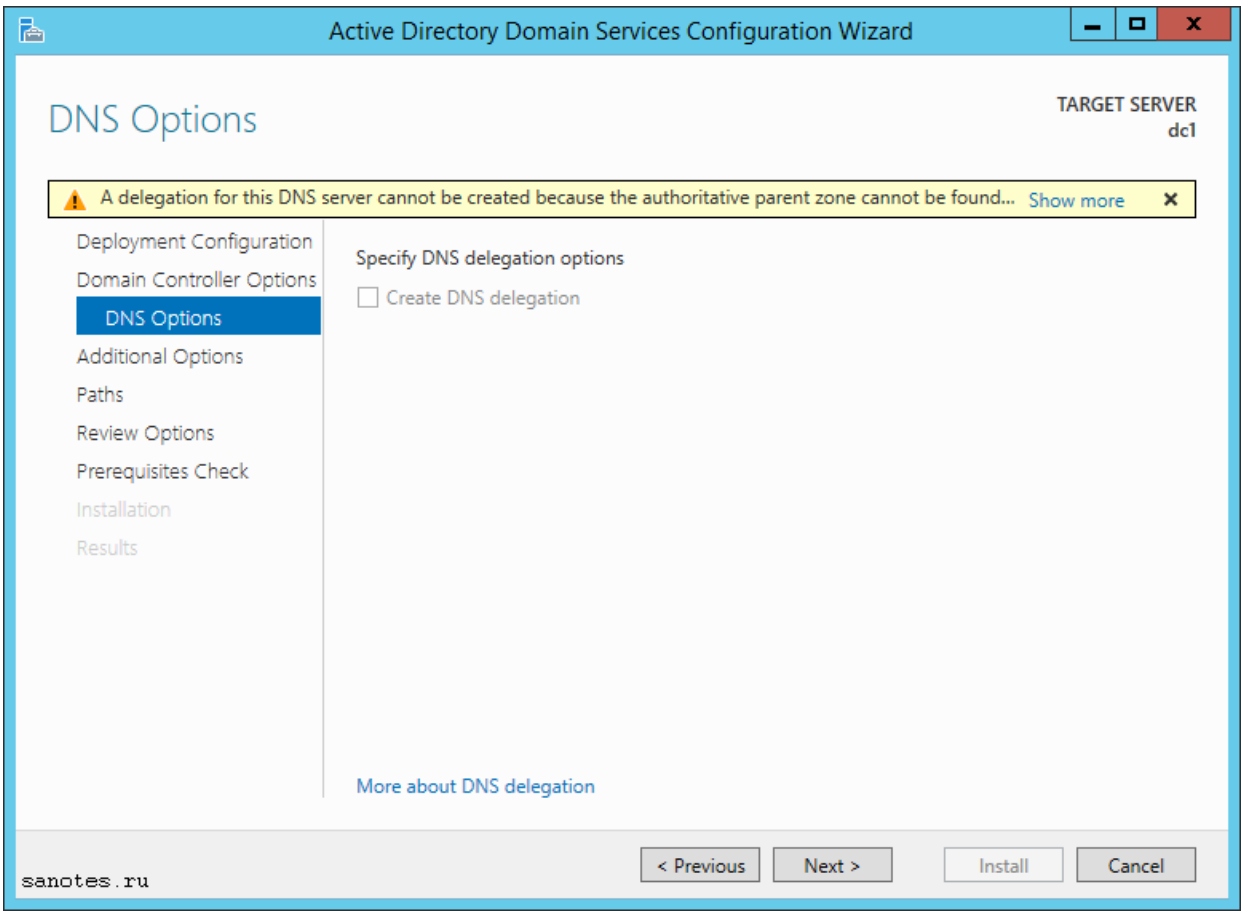
Выбираем вариант **Add New Forest**, задаем корневое имя домена, нажимаем Next.



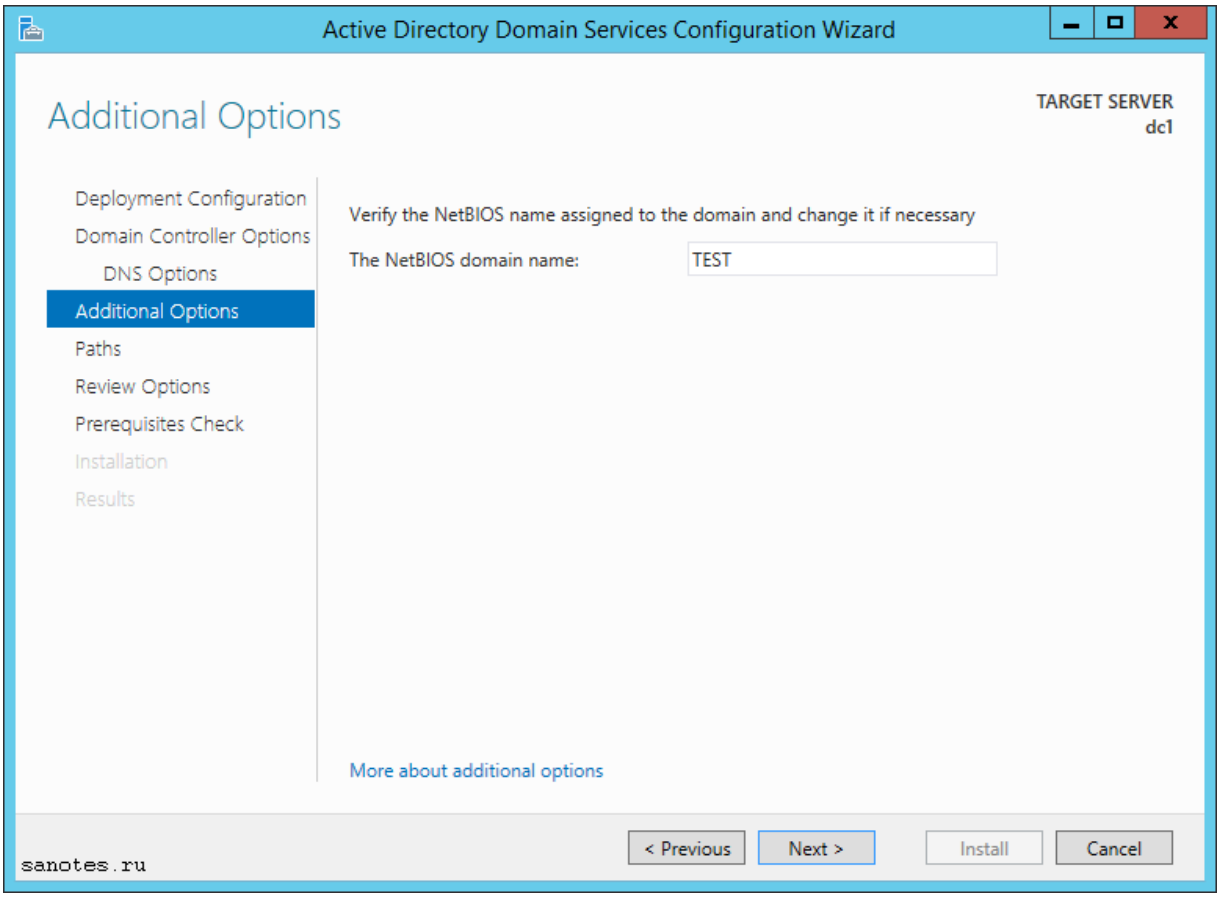
На следующей вкладке можно задать функциональный уровень домена и леса (по умолчанию 2016 R2), снять или отметить для установки DNS Server, и задать пароль для режима восстановления службы каталогов (DSRM). Укажем только пароль для DSRM и нажмем Далее.



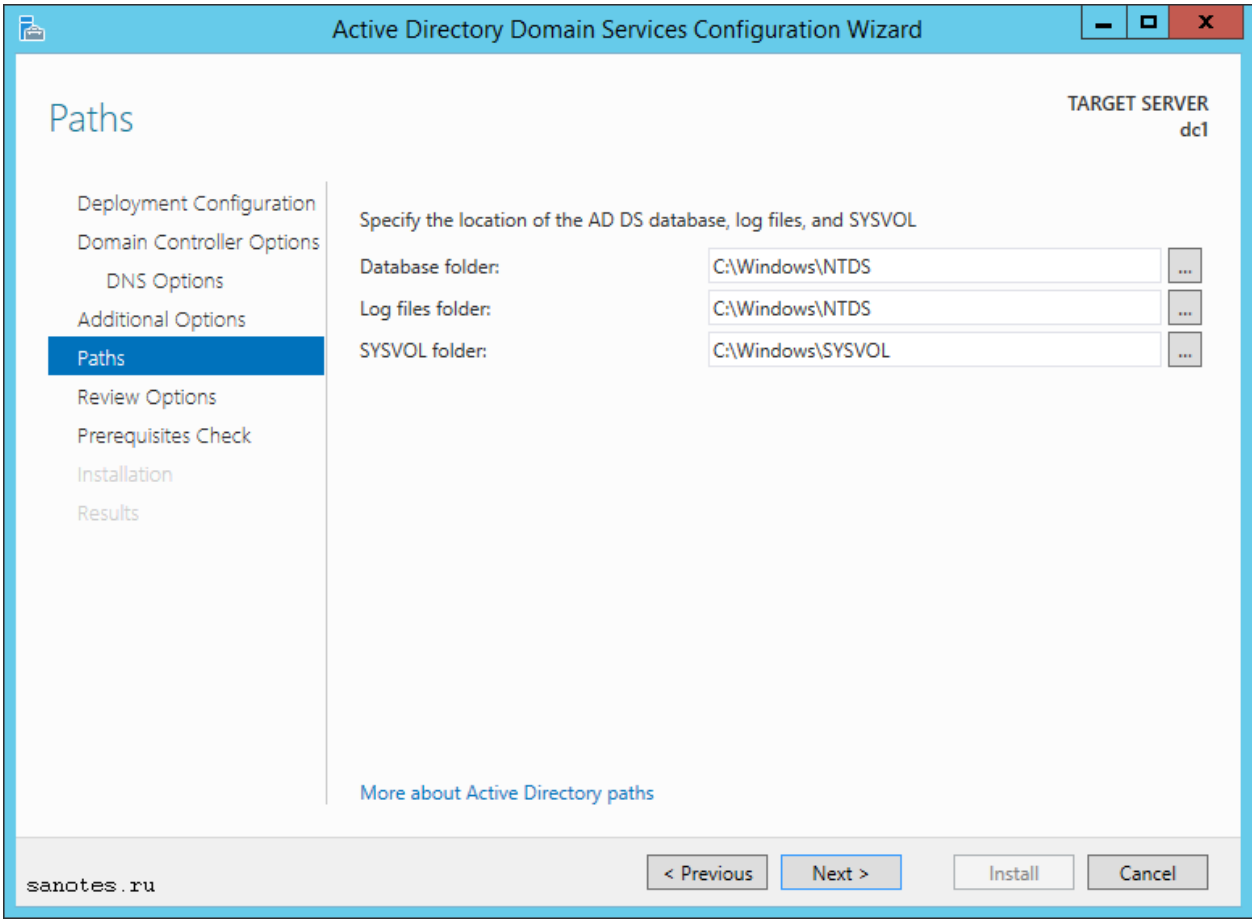
На следующем шаге **DNS Options** мастер ругнется, на то, что делегирование для этого DNS-сервера создано не было, потому что не найдена дочерняя зона или запущенный DNS-сервер. Что не удивительно, т.к. роль DNS Server у нас создается в процессе. Нажимаем Next.



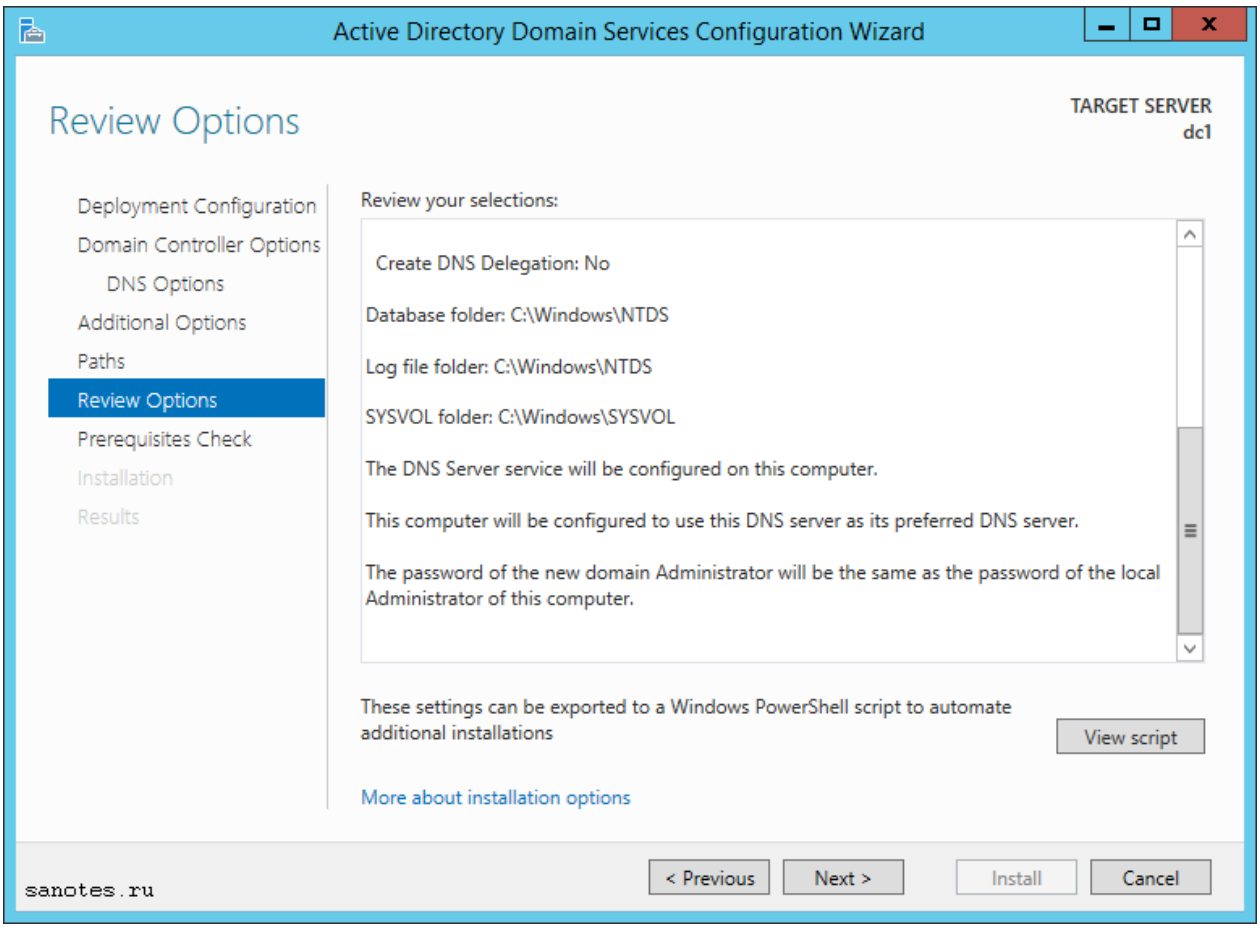
Далее в Addional Optional соглашаемся с NetBIOS именем, которое предлагает нам система, жмем Next.



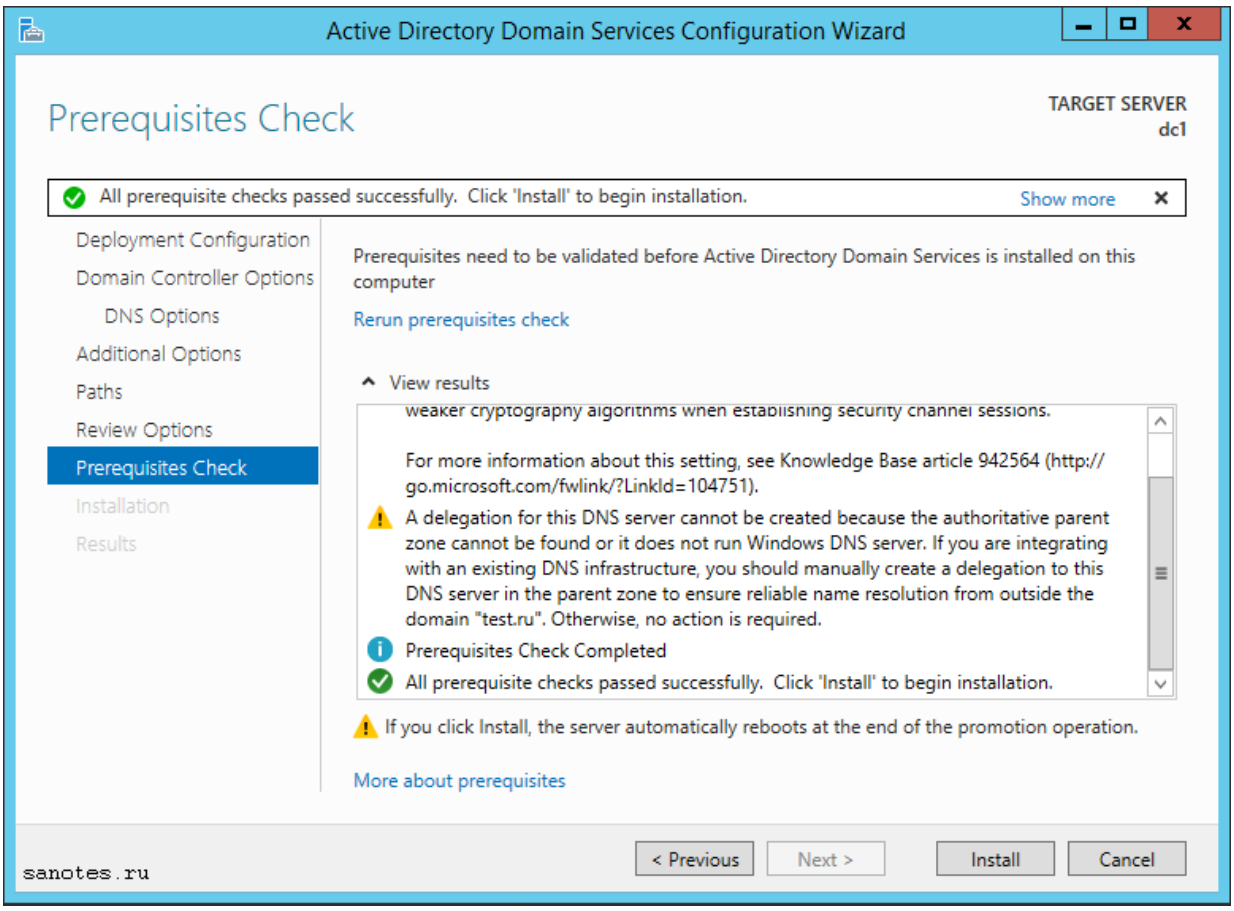
В разделе **Paths** можно изменить путь к каталогам баз данных, файлам журнала и к SYSVOL. Оставляем по умолчанию, нажимаем Next.



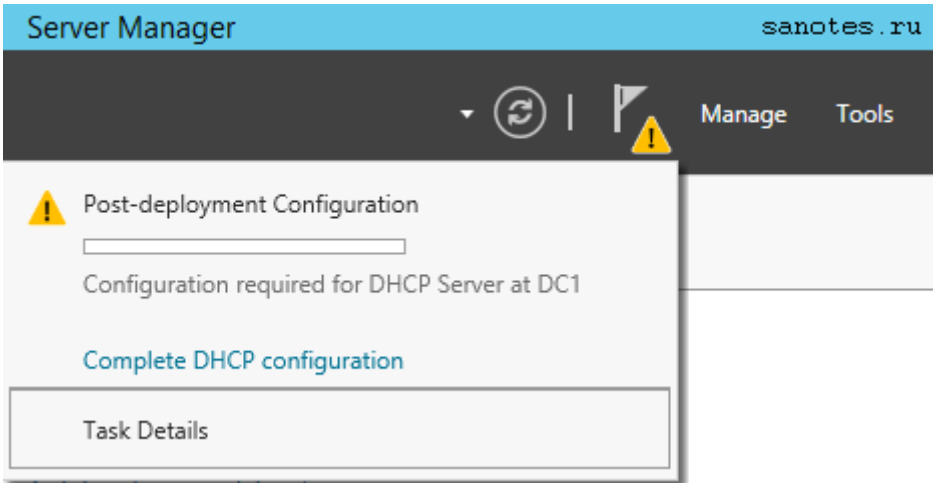
На следующем этапе **Review Options** отображается сводная информация по настройке. Кнопка **View Script**, позволяет посмотреть **Powershell** скрипт, при помощи которого, в будущем можно будет произвести настройку доменных служб **Active Directory**. Нажимаем Next.



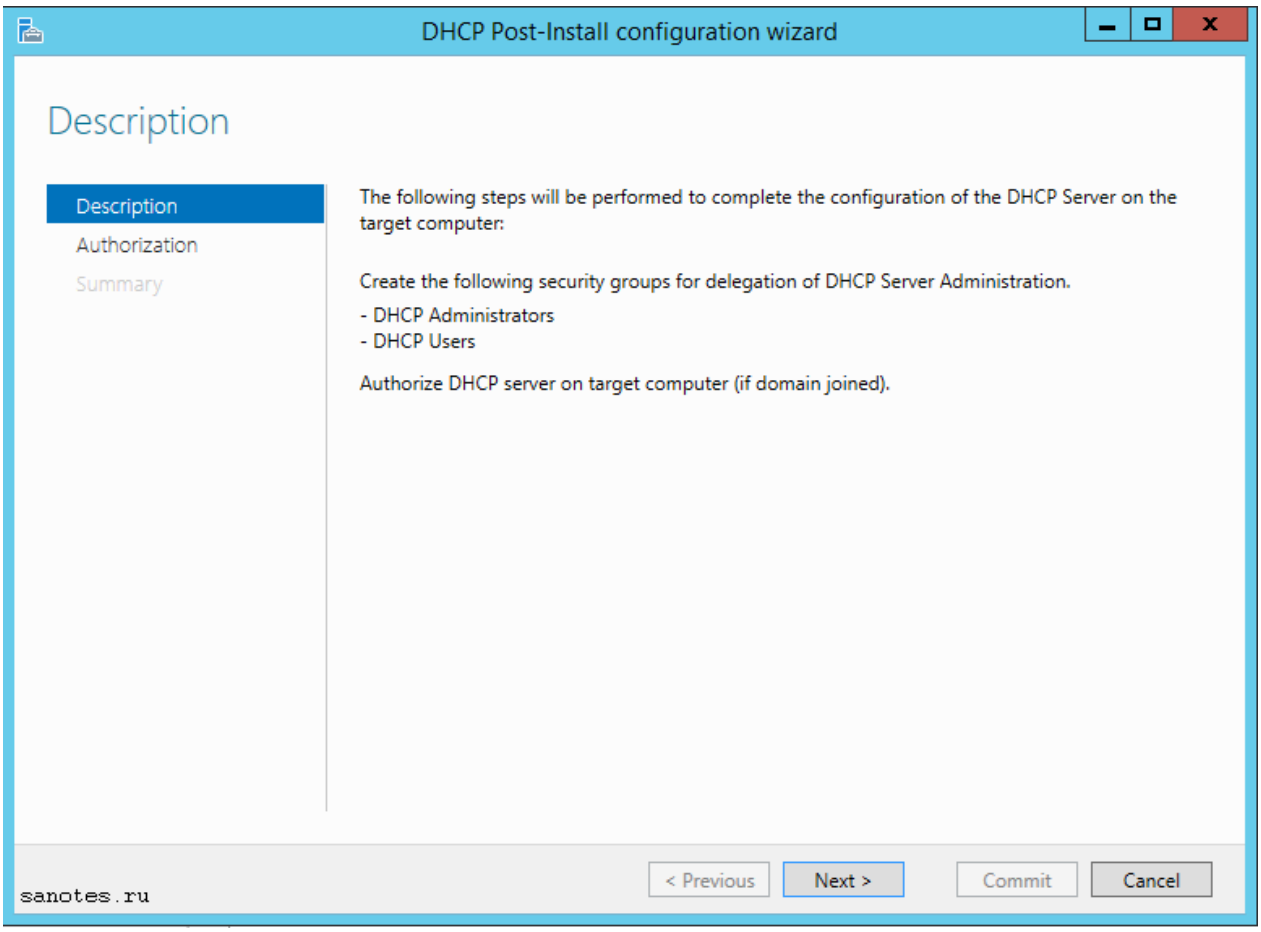
И наконец, на последнем этапе предварительных проверок, если видим надпись: *«All prerequisite checks are passed successfully. Click «install» to begin installation*.» (Все предварительные проверки пройдены успешно. Нажмите кнопку «установить», чтобы начать установку.), то нажимаем Install, дожидаемся окончания процесса установки.



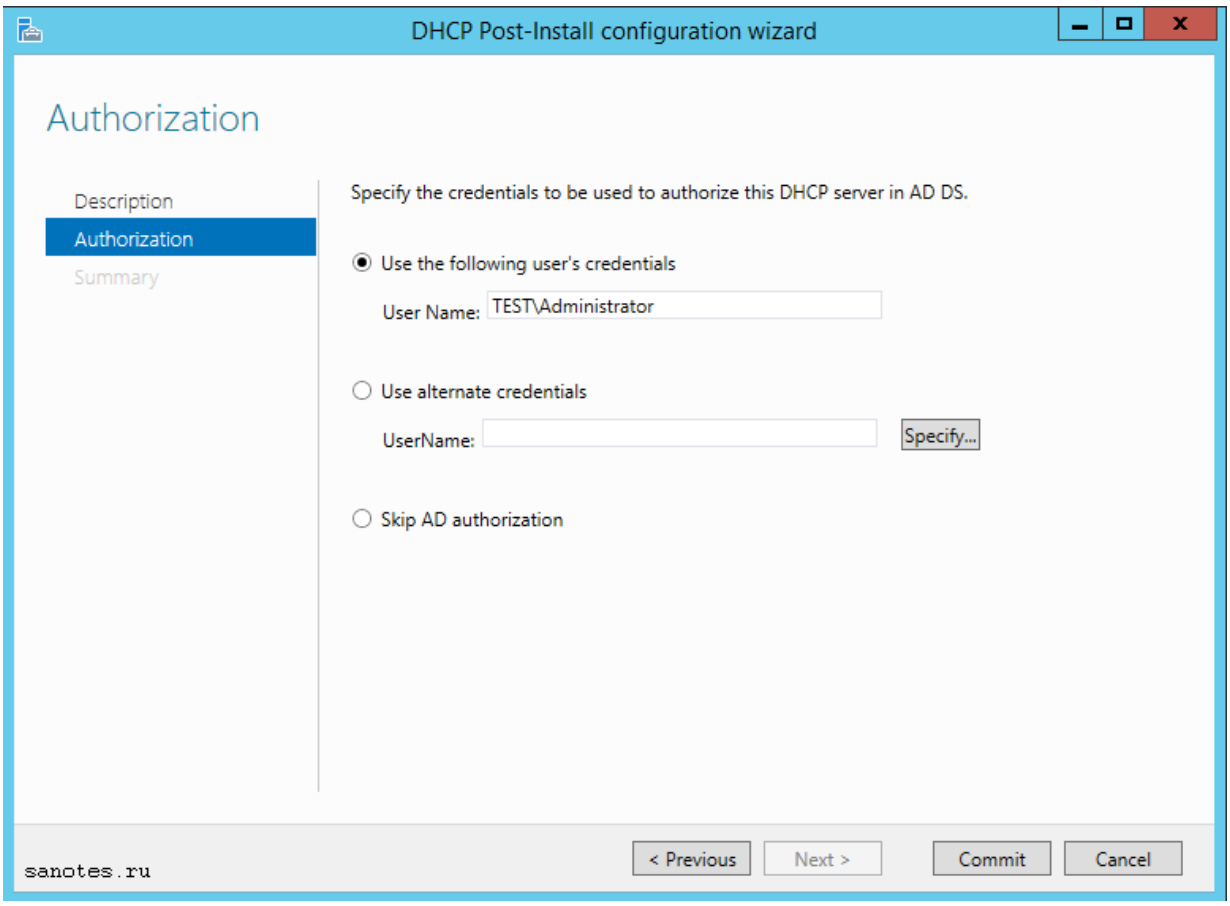
После перезагрузки, снова заходим в **Server Manager** -> **Dashboard** и запускаем пиктограмму треугольника с восклицательным знаком и выбираем там **Complete DHCP Configuration** (Завершение конфигурации DHCP).



Запустится мастер по конфигурированию DHCP, который нам сообщит, что будут созданы группы безопасности администратора и пользователя DHCP-сервера, и будет произведена авторизация в AD. Нажимаем Next.

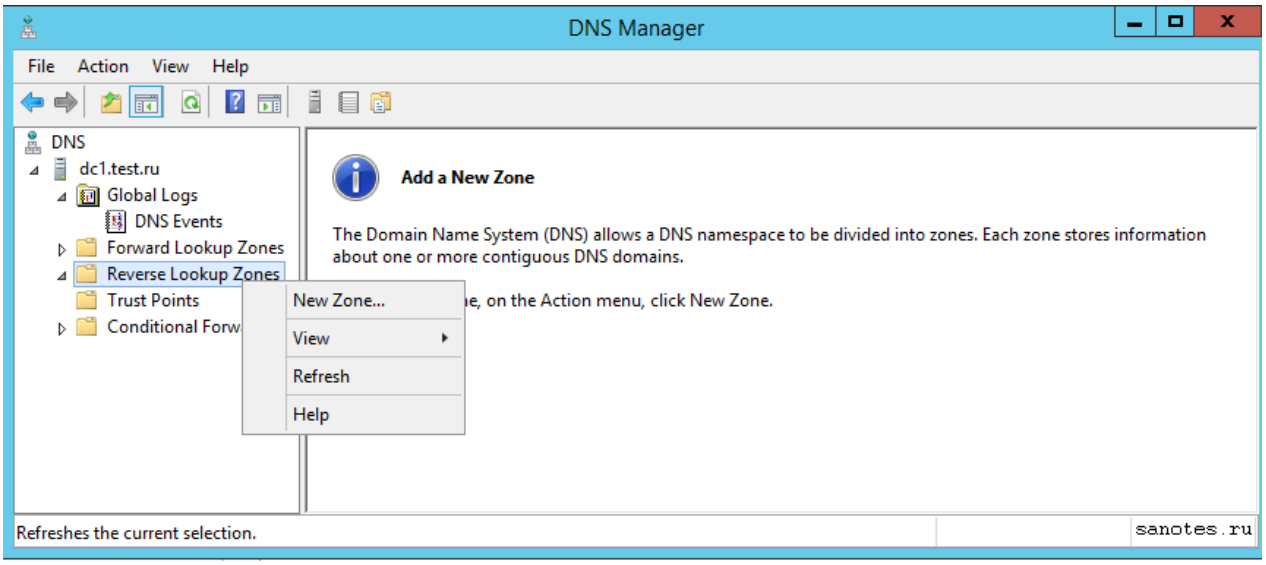


На следующем экране нажимаем Commit что бы завершить процесс авторизации в Active Directory.



Если видим, что *Create Security Group — Done* и *Authorizing DHCP Server — Done*, то процесс завершился успешно, нажимаем Close.

Теперь создадим обратную зону в DNS. Обратная зона, позволяет выполнить разрешение FQDN-имен хостов по их IP-адресам. В процессе добавления ролей AD и DNS по умолчанию не создаются, поскольку предполагается, что в сети может существовать другой DNS-сервер, контролирующий обратную зону. Поэтому создадим ее сами, для этого переходим в диспетчер DNS (DNS Manager), на вкладку Reverse Lookup Zones, кликаем правой кнопкой и выбираем New Zone.



Запустится мастер DNS-зоны. Соглашаемся с параметрами по умолчанию, а именно нам

предлагается создать основную зону которая будет хранится на этом сервере (Primary Zone) и будет интегрирована в Active Directory (Store the zone in Active Directory...). Нажимаем Next.

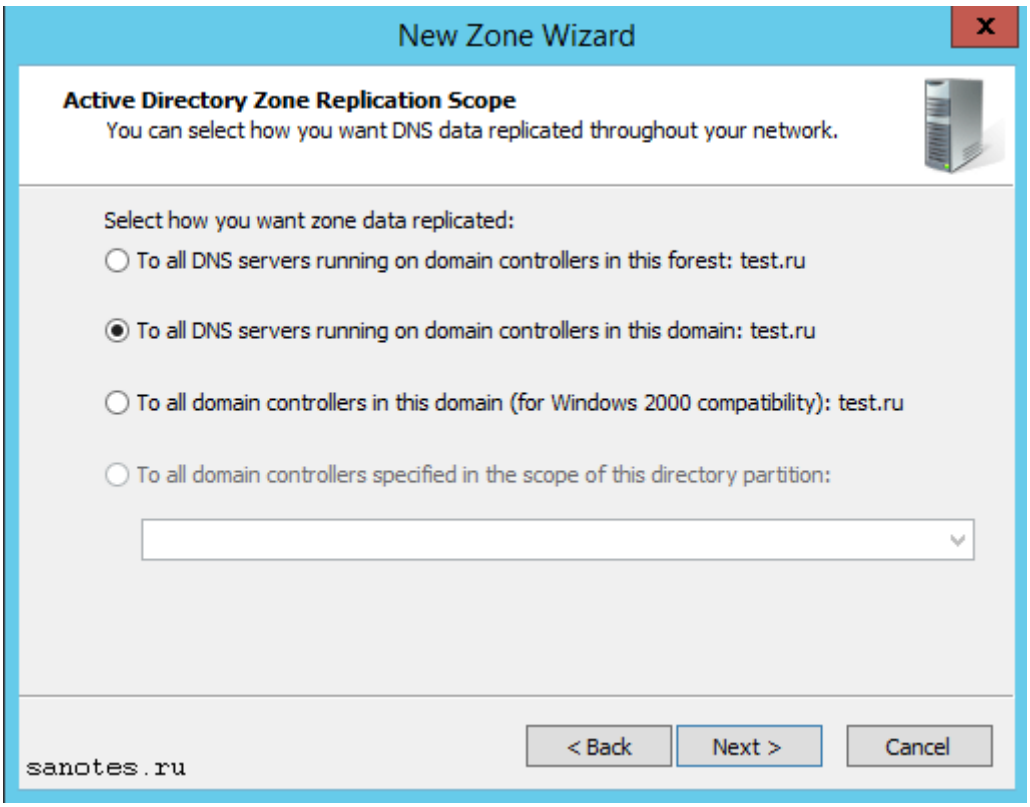
На следующем экране, предлагается выбрать как зона будет реплицироваться, обмениваться данными с другими зонами расположенными на контроллерах и DNS-серверах. Возможны следующие варианты:

Для всех DNS-серверов расположенных на контроллере домена в этом лесу (To all DNS servers running on domain controllers in this forest). Репликации во всем лесу Active Directory включая все деревья доменов.

Для всех DNS-серверов расположенных на контроллере домена в этом домене (To all DNS servers running on domain controllers in this domain). Репликация внутри текущего домена и его дочерних доменов.

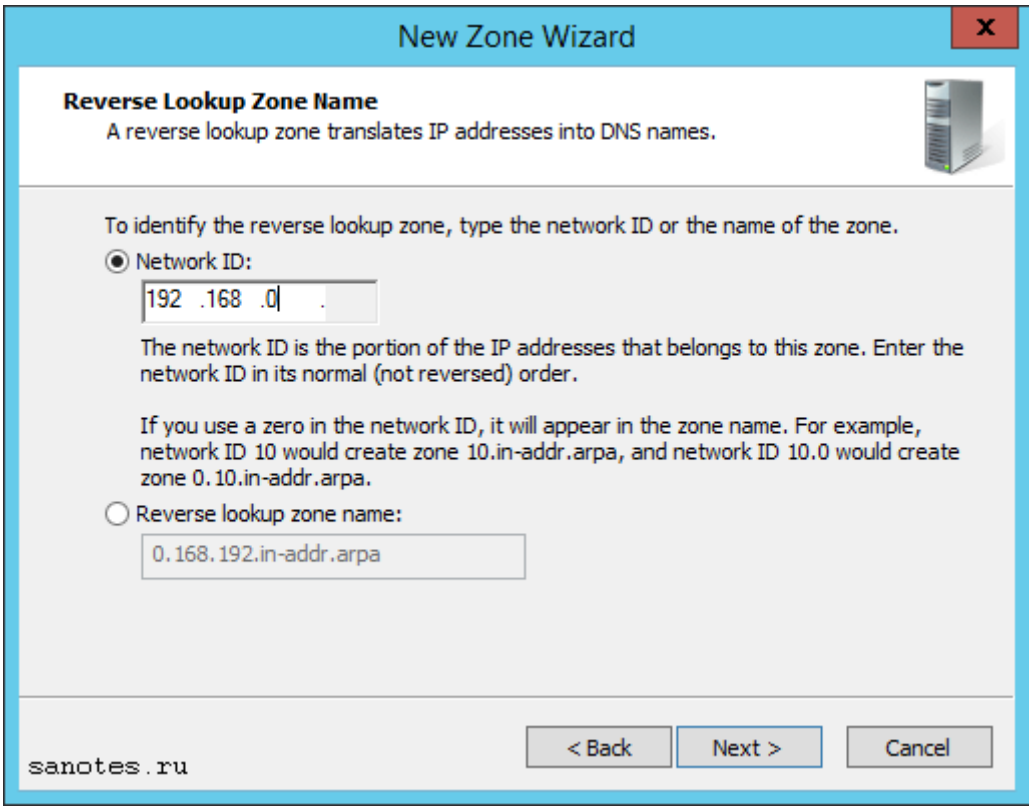
Для всех контроллеров домена в этом домене (To all domain controllers in this domain). Репликация на все контроллеры домена внутри текущего домена и его дочерних доменов.

На все контроллеры домена в указанном разделе каталога приложений (To all domain controllers specified in the scope of this directory partition). Репликация на все контроллеры домена, но DNS-зона располагается в специальном каталоге приложений. Поле будет доступно для выбора, после создания каталога.



Выбираем вариант по умолчанию, нажимаем Next. Затем выбираем протокол по умолчанию IPv4 и снова жмем Next.

На следующем экране зададим идентификатор сети (Network ID). В нашем случае 192.168.0. В поле Reverse Lookup Zone Name увидим как автоматически подставится адрес зоны обратного просмотра. Нажимаем Next.



На экране Dynamic Update (динамические обновления), выберем один из трех возможных вариантов динамического обновления.

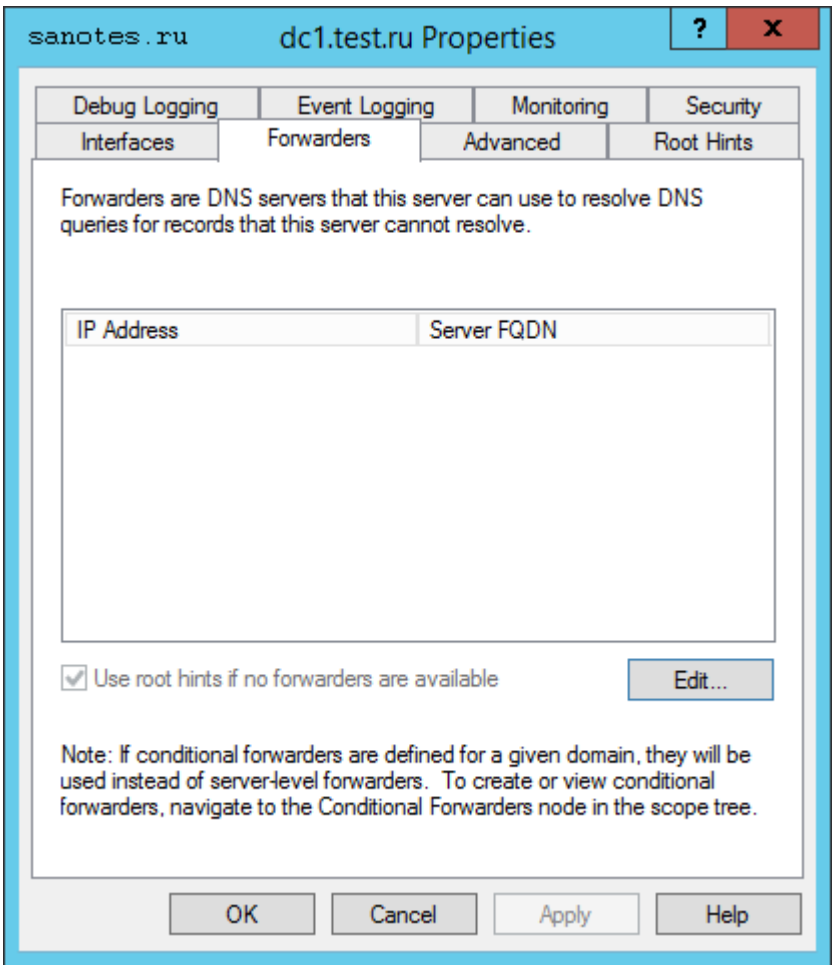
Разрешить только безопасные динамические обновления (Allow Only Secure Dynamic Updates). Это опция доступна, только если зона интегрирована в Active Directory.

Разрешить любые, безопасные и не безопасные динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates). Данный переключатель, позволяет любому клиенту обновлять его записи ресурса в DNS при наличии изменений.

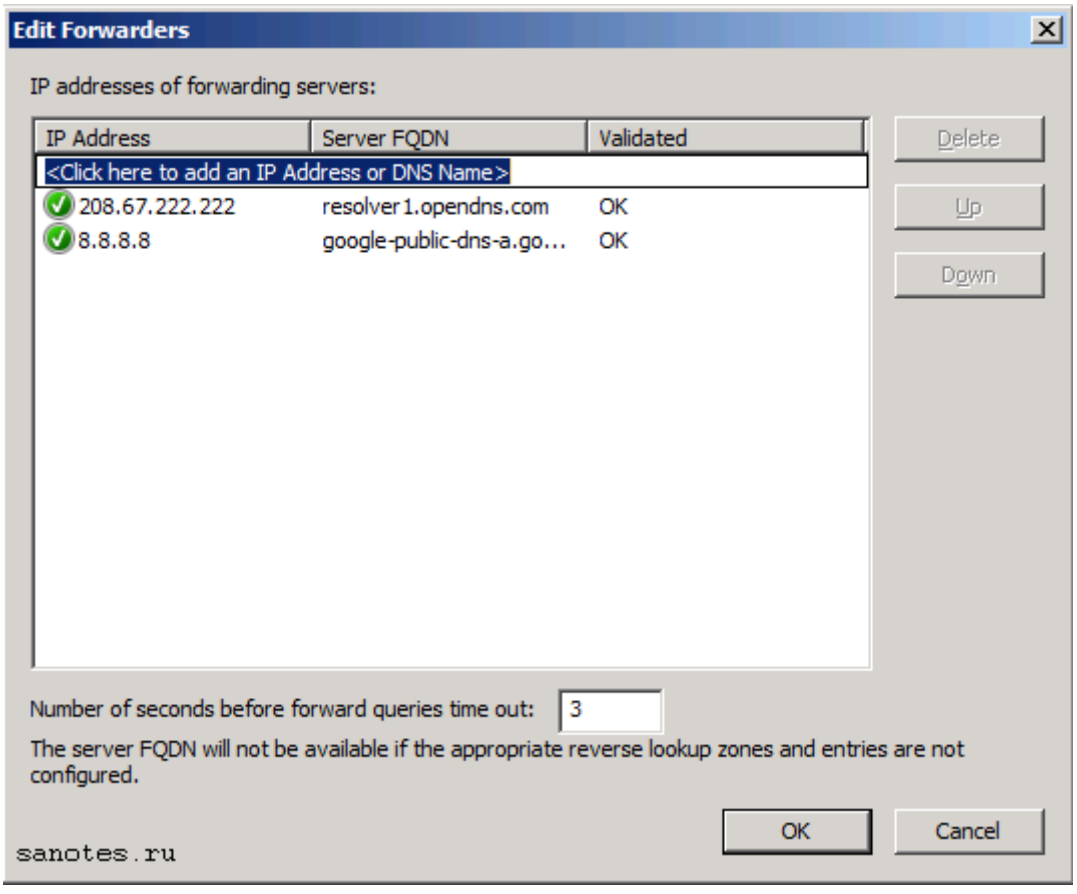
Запретить динамические обновления (Do Not Allow Dynamic Updates). Это опция отключает динамические обновления DNS. Ее следует использовать только при отсутствии интеграции зоны с Active Directory.

Выбираем первый вариант, нажимаем Next и завершаем настройку нажатием Finish.

Еще одна полезная опция, которая обычно настраивается в DNS — это серверы пересылки или Forwarders, основное предназначение которых кэшировать и перенаправлять DNS-запросы с локального DNS-сервера на внешний DNS-сервер в сети интернет, например тот что находится у провайдера. Например мы хотим, что бы локальные компьютеры в нашей доменной сети, в сетевых настройках у которых прописан DNS-сервер (192.168.0.3) смогли получить доступ в интернет, необходимо что бы наш локальный dns-сервер был настроен на разрешение dns-запросов вышестоящего сервера. Для настройки серверов пересылки (Forwarders) переходим в консоль менеджера DNS. Затем в свойствах сервера переходим на вкладку Forwarders и нажимаем там Edit.

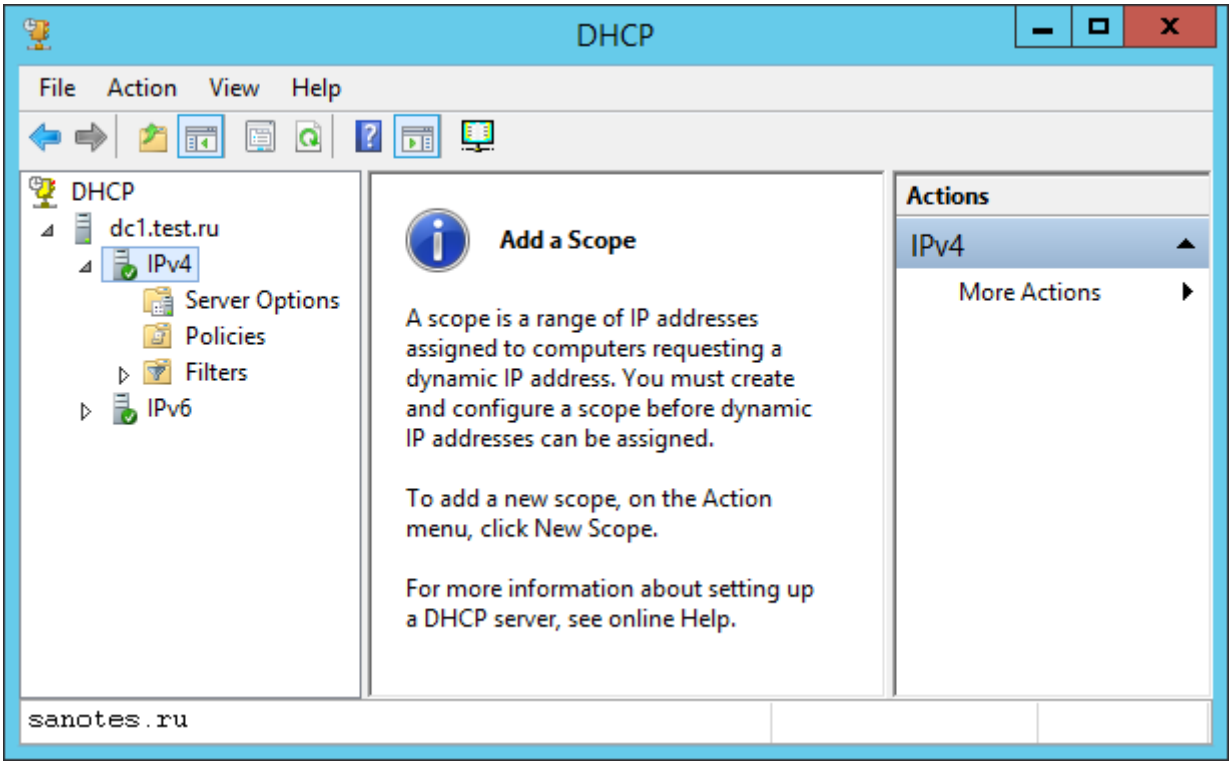


Укажем как минимум один IP-адрес. Желательно несколько. Нажимаем OK.

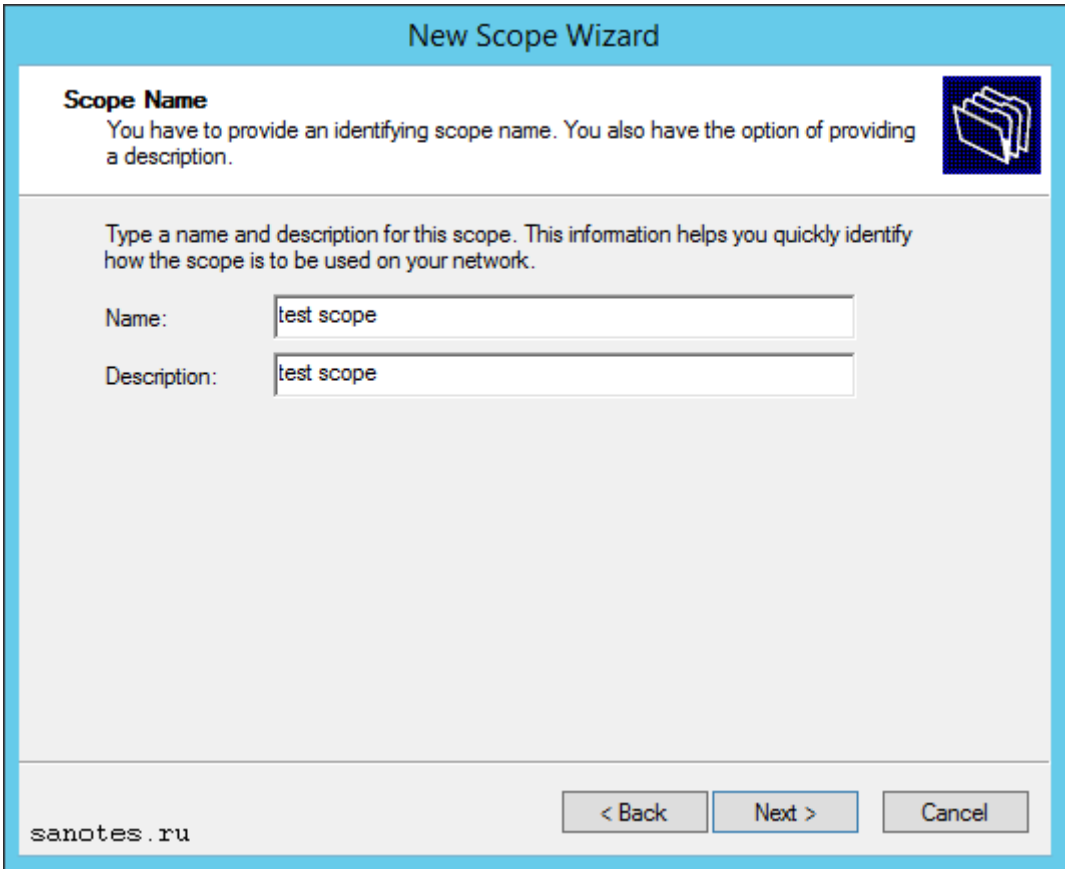


Настройка службы DHCP.

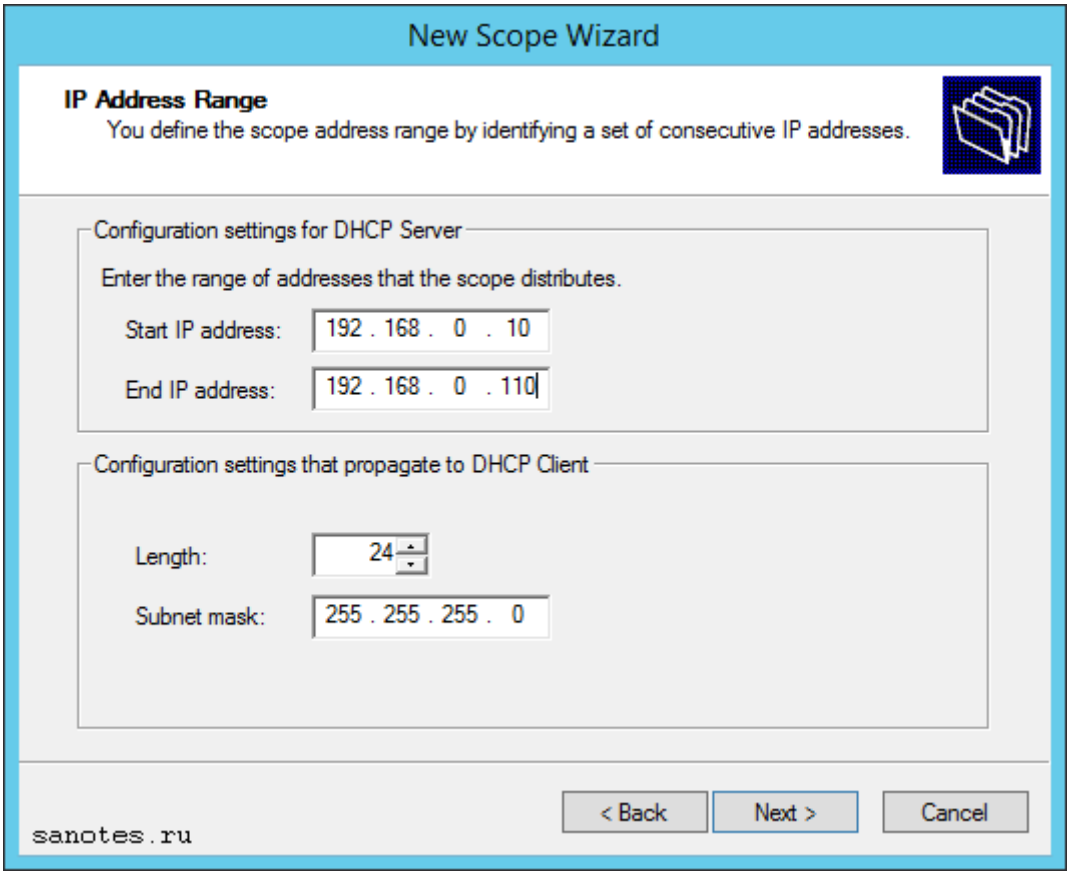
Запускаем оснастку DHCP.



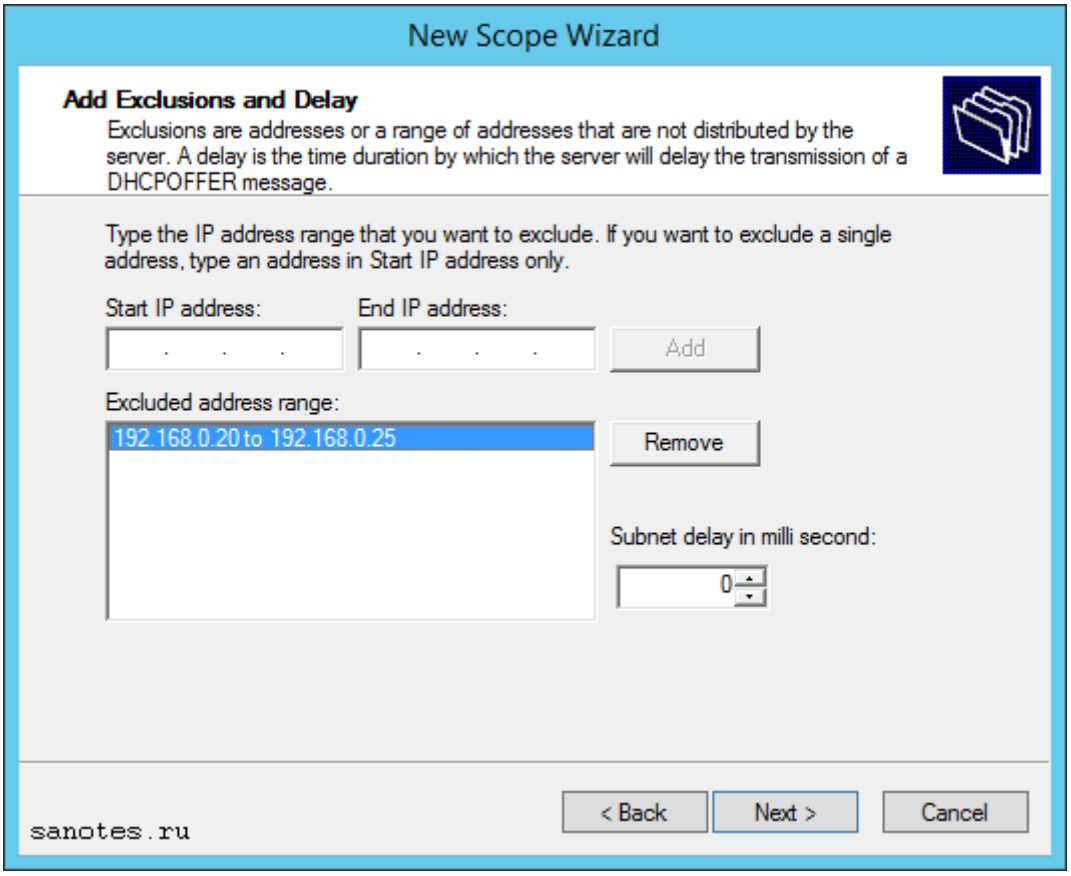
Сперва зададим полный рабочий диапазон адресов из которого будут браться адреса для выдачи клиентам. Выбираем Action\New Scope. Запустится мастер добавления области. Зададим имя области.



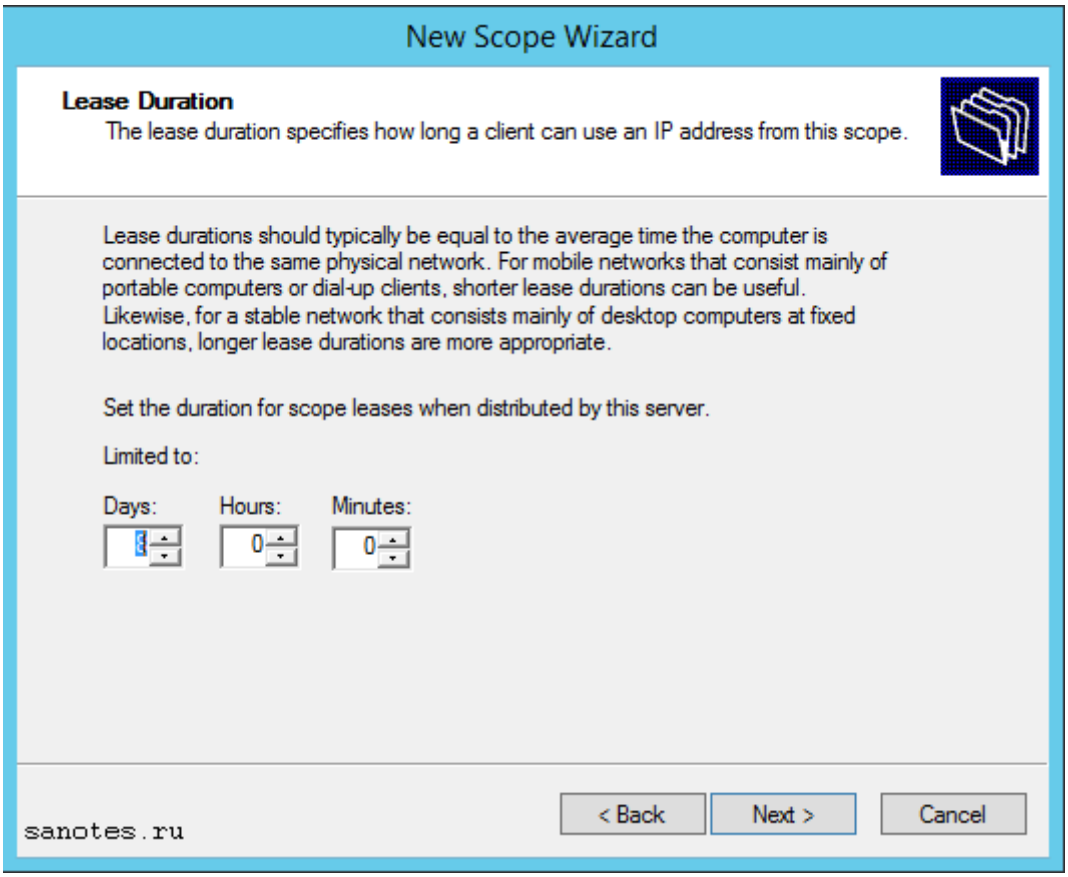
Далее укажем начальный и конечный адрес диапазона сети.



Далее добавим адреса которые мы хотим исключить из выдачи клиентам. Жмем Далее.

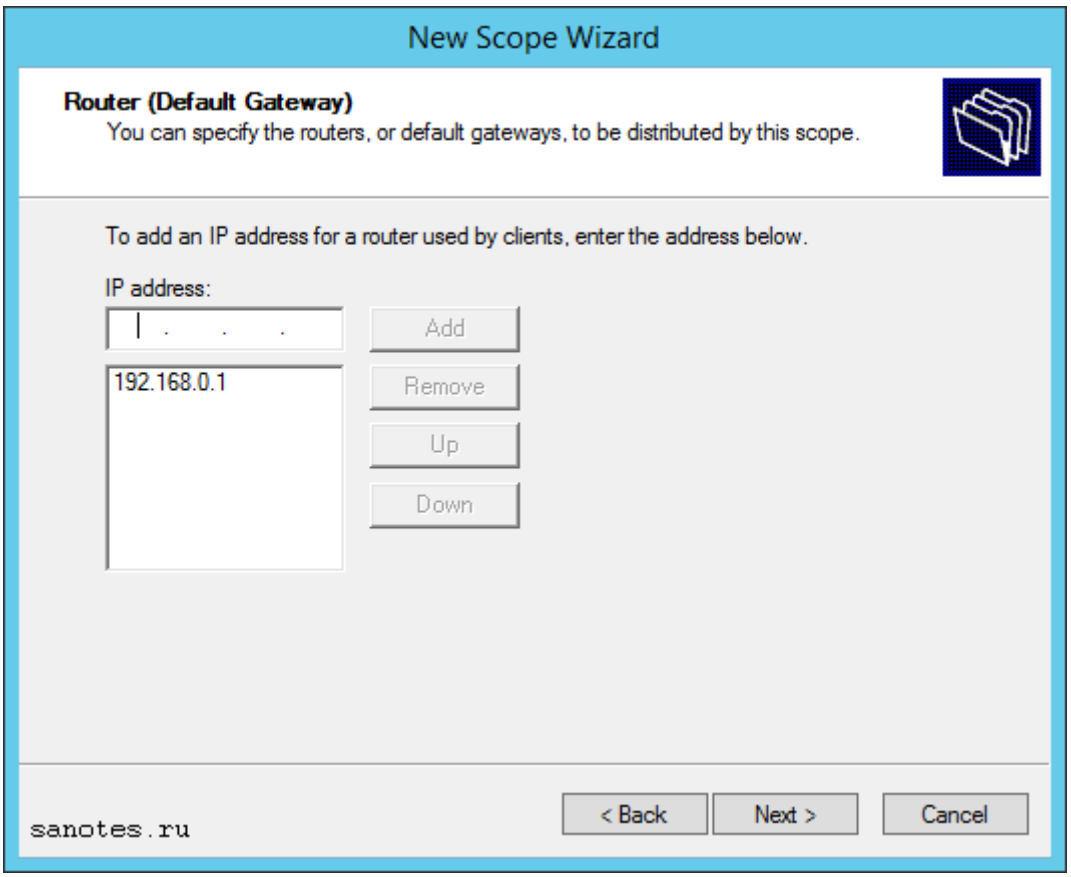


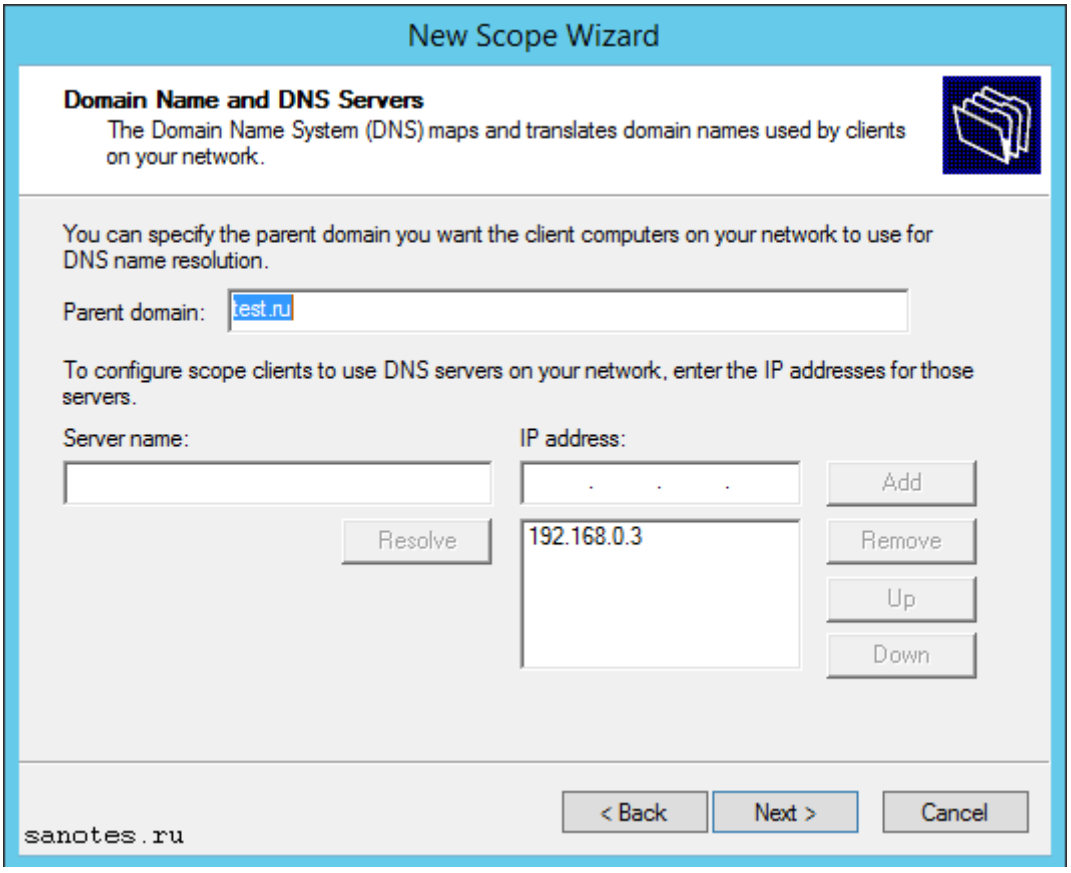
На экране Lease Duration укажем отличное от по умолчанию время аренды, если требуется. Жмем Далее.

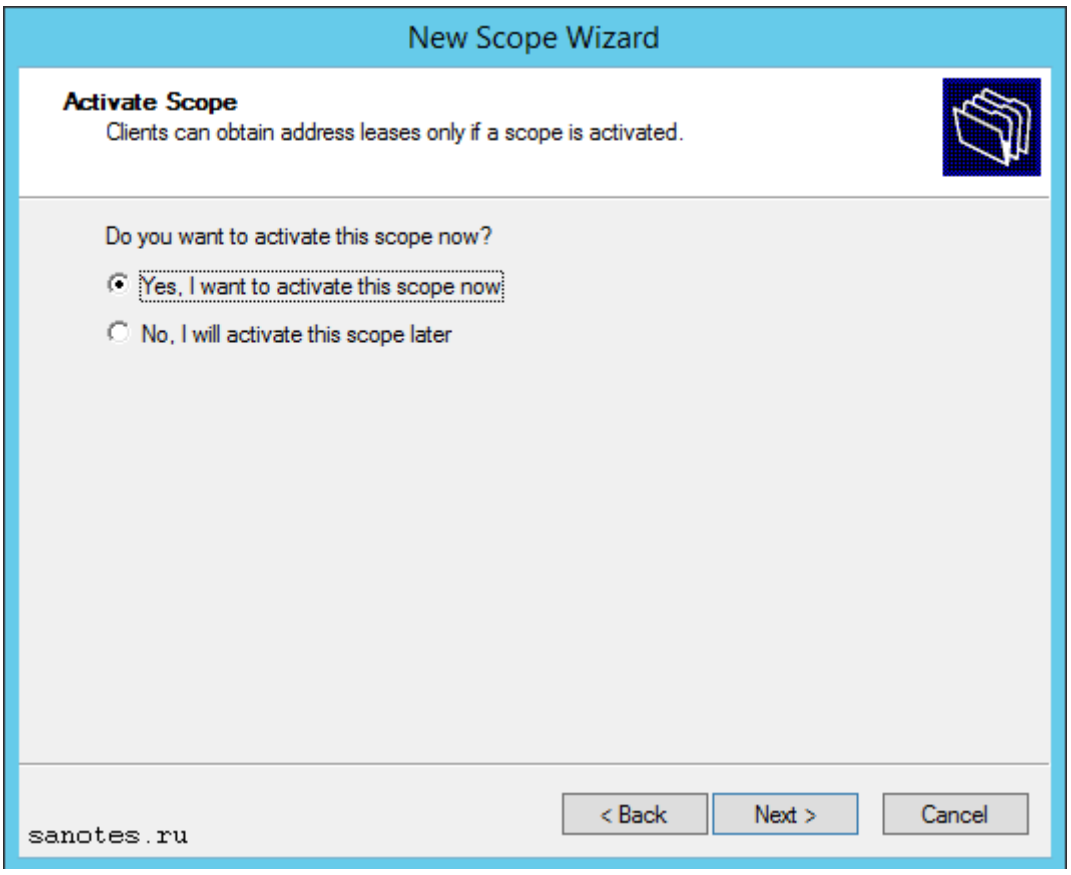


Затем согласимся, что хотим настроить опции DHCP: Yes, I want to configure these option now.

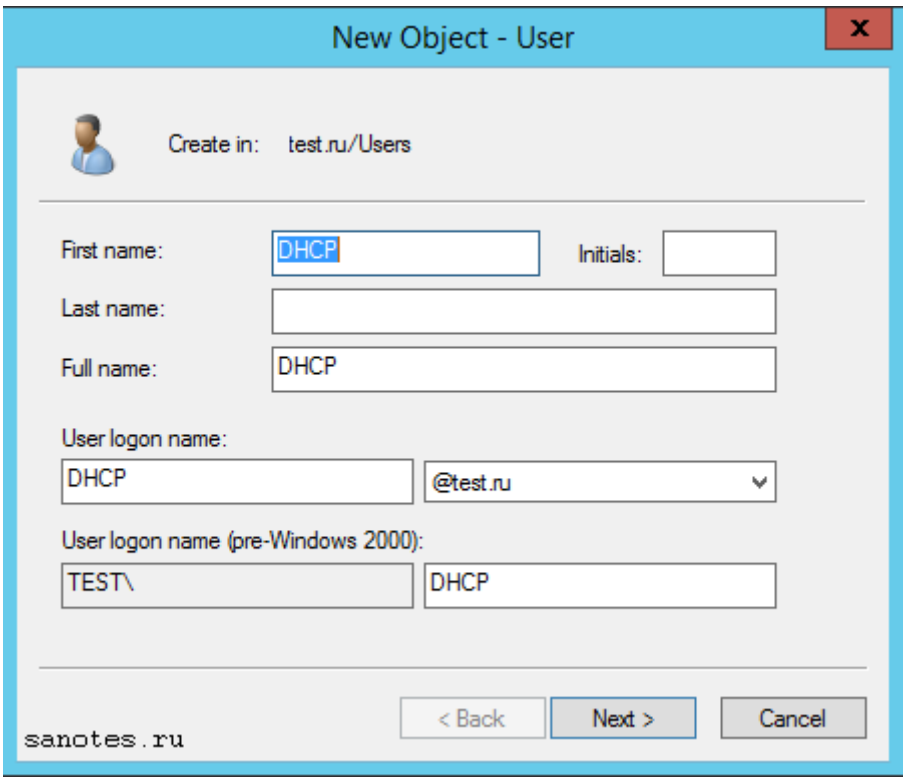
Последовательно укажем шлюз, доменное имя, адреса DNS, WINS пропускаем и в конце соглашаемся с активацией области нажатием: Yes, I want to activate this scope now. Finish.


New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
Add
192.168.0.1
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel

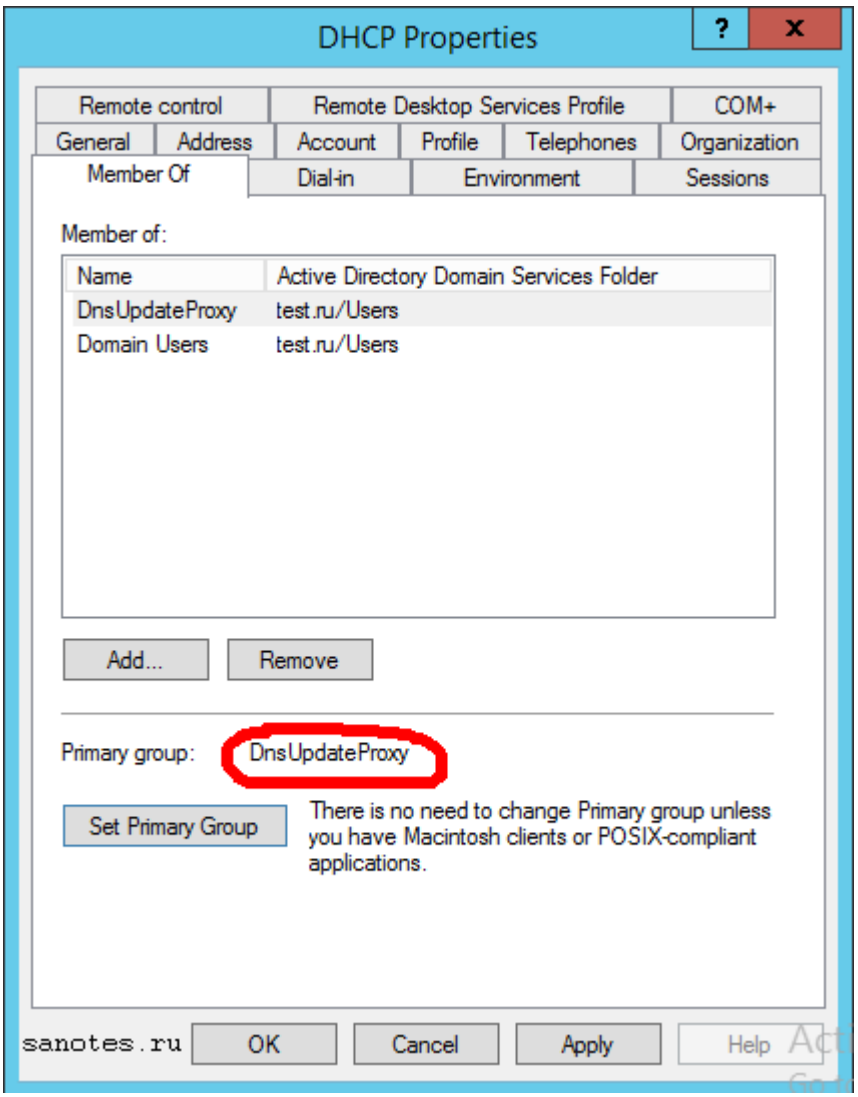

New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
test.ru
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.0.3
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel



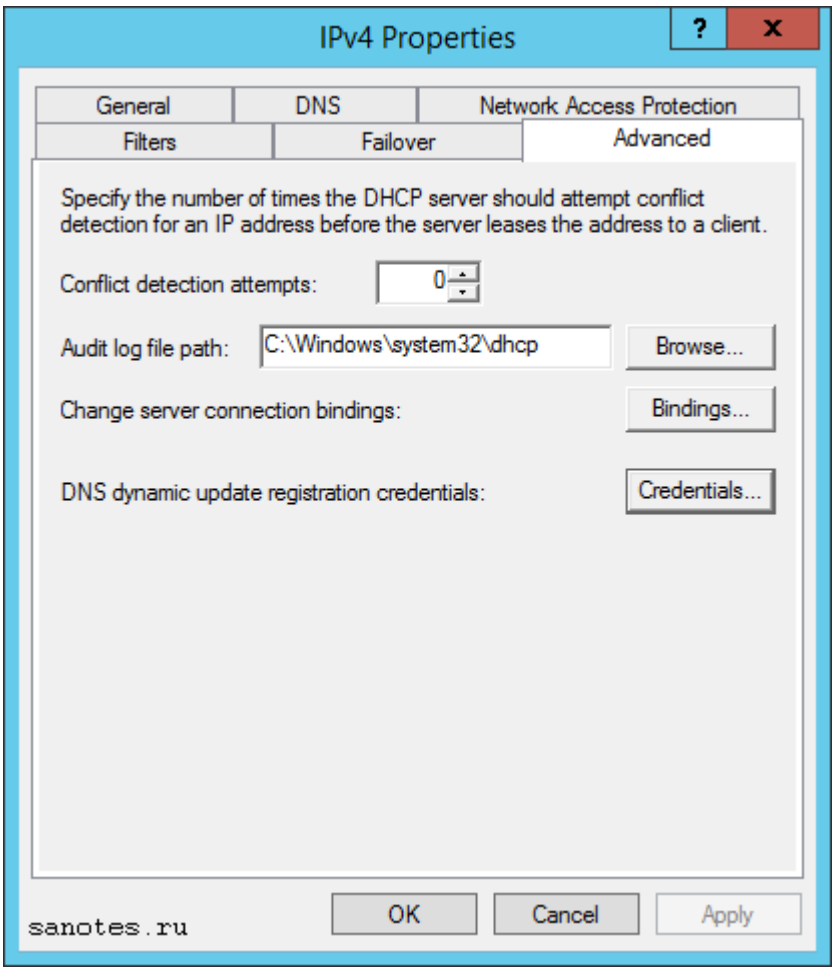
Для безопасной работы службы DHCP, требуется настроить специальную учетную запись для динамического обновления записей DNS. Это необходимо сделать, с одной стороны для того что бы предотвратить динамическую регистрацию клиентов в DNS при помощи административной учетной записи домена и возможного злоупотребления ею, с другой стороны в случае резервирования службы DHCP и сбоя основного сервера, можно будет перенести резервную копию зоны на второй сервер, а для этого потребуется учетная запись первого сервера. Для выполнения этих условий, в оснастке Active Directory Users and Computers создадим учетную запись с именем dhcp и назначим бессрочный пароль, выбрав параметр: Password Never Expires.



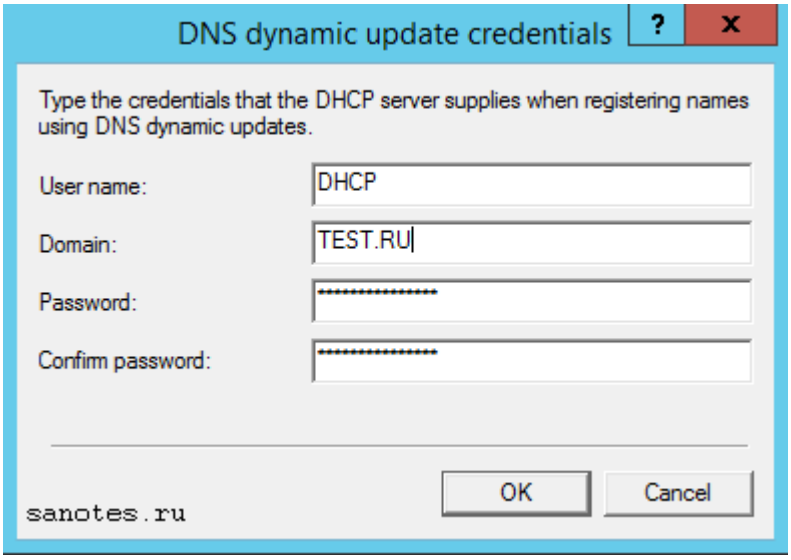
Назначим пользователю надежный пароль и добавим в группу DnsUpdateProxy. Затем удалим пользователя из группы Domain Users, предварительно назначив пользователю primary группу «DnsUpdateProxy». Данная учетная запись будет отвечать исключительно за динамическое обновление записей и не иметь доступа не каким другим ресурсам где достаточно базовых доменных прав.



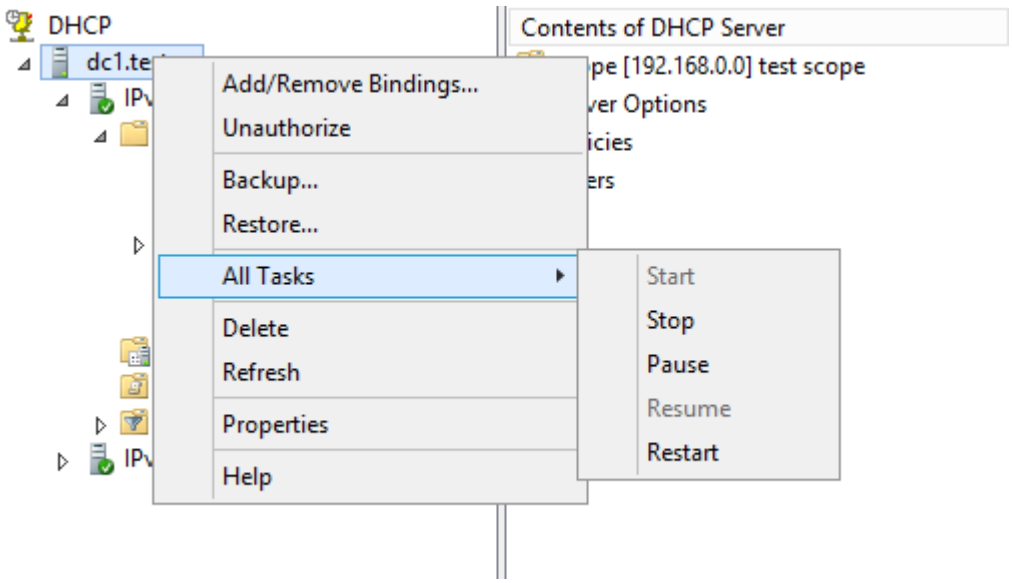
Нажимаем Apply и затем OK. Открываем снова консоль DHCP. Переходим в свойства протокола IPv4 на вкладку Advanced.



Нажимаем Credentials и указываем там нашего пользователя DHCP.



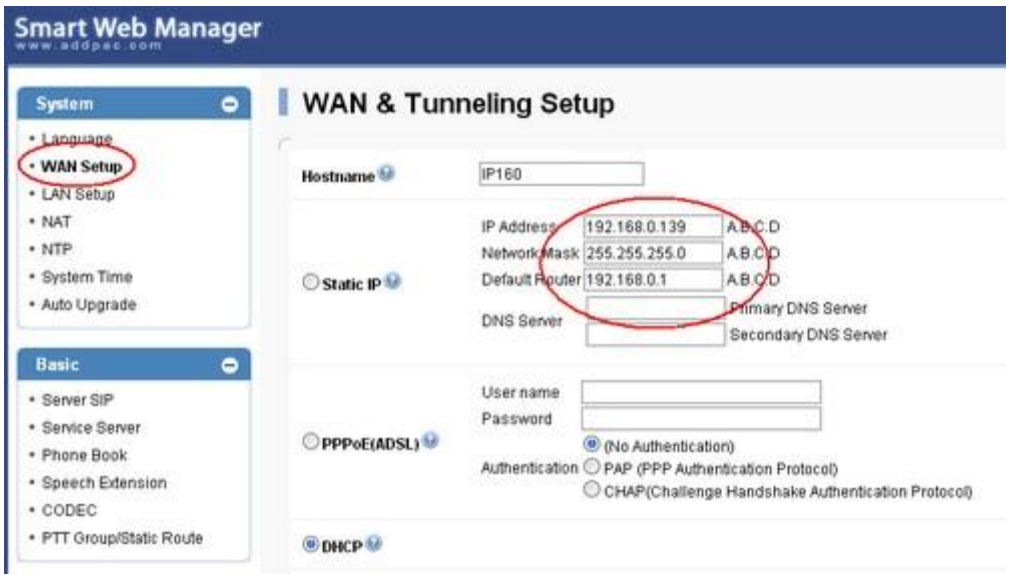
Нажимаем ОК, перезапускаем службу.



Позже мы еще вернемся к настройке DHCP, когда будем настраивать резервирование службы DHCP, но для этого нам надо поднять как минимум второй и последующий контроллеры домена.

2.21. Практическая работа № 21
Настройка аппаратных IP-телефонов

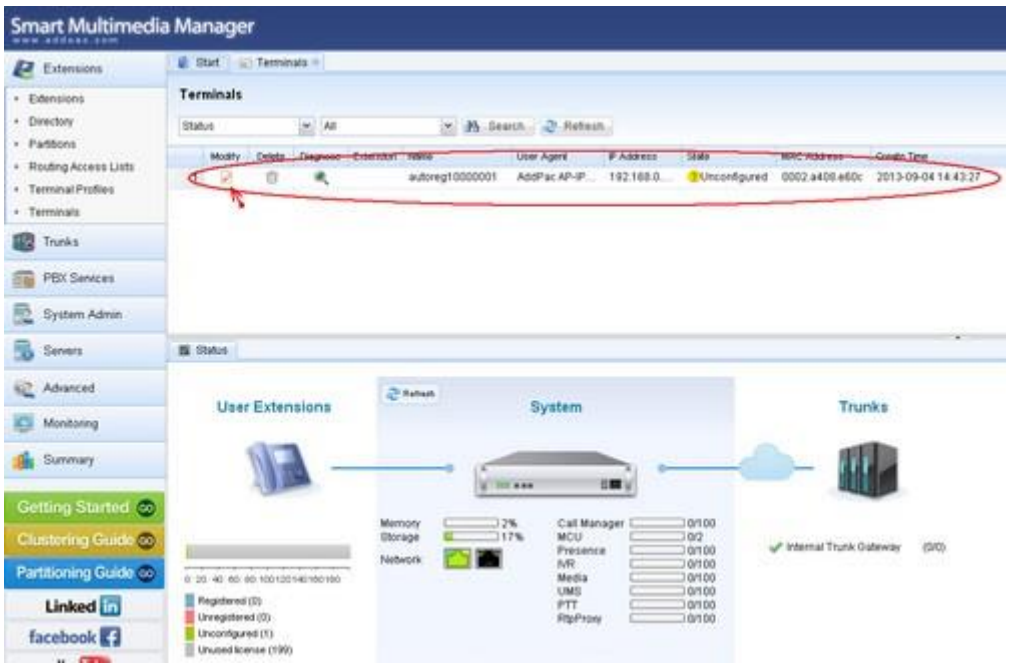
Настройка IP-телефона для работы с IP-АТС AddPac IPNext
Порядок настройки IP-телефона для работы с IP-АТС:
а) Подключите телефон через LAN разъем к сети, затем нажмите кнопку MENU и в интерфейсе телефона перейдите:
Menu => Network Setup => Internet Setup (далее выбираем тип: DHCP или статический IP)
Теперь необходимо указать адрес SSCP (адрес IPNext)
Menu => Network Setup => SSCP Setup => Use SSCP => Enable
Menu => Network Setup => SSCP Setup => CM Setup => Call Manager1 (вводим IP адрес АТС IPNext)
б) Те же самые настройки можно произвести через WEB-интерфейс телефона.



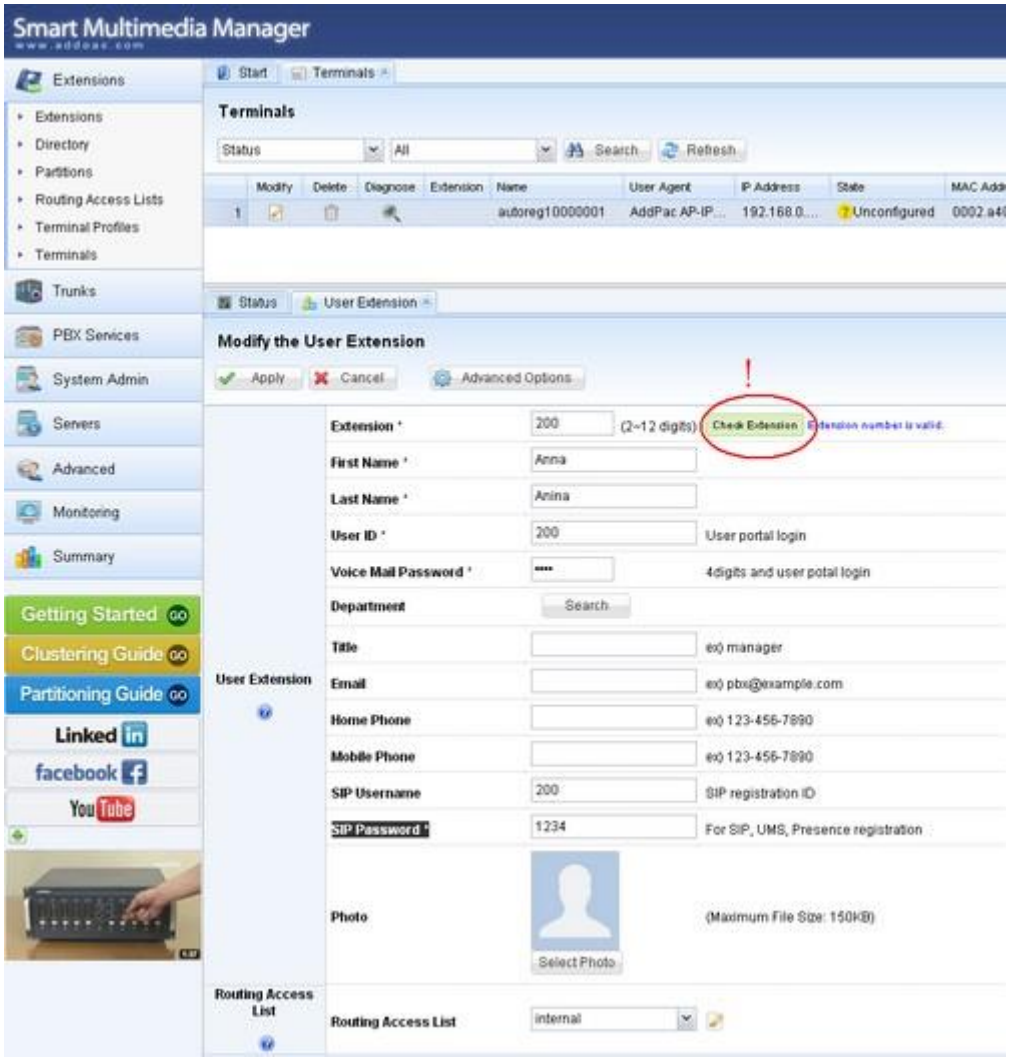
На этом настройка IP телефона закончена. Теперь телефон сообщается с IPNext по фирменному протоколу AddPac SSCP. Далее все настройки производим на IP-АТС через web-интерфейс.
Заходим на Smart Multimedia Manager IPNext

Выбираем меню Extensions, и подменю Terminals.

Здесь мы видим наш телефон, запросивший авторегистрацию (его модель, IP адрес, MAC адрес). Теперь нам нужно назначить ему номер. Нажимаем Modify.



Заполняем поля отмеченные звездочкой:
Extension * -внутренний номер телефона. Обязательно нажимаем Check Extension для проверки доступности номера!
First Name * - Имя
Last Name * - Фамилия
User ID * - для идентификации на персональном портале
Voice Mail Password * - пароль для голосовой почты
SIP Username, SIP Password * - логин/пароль для возможности регистрации по SIP с софт-телефона
И нажимаем Apply.



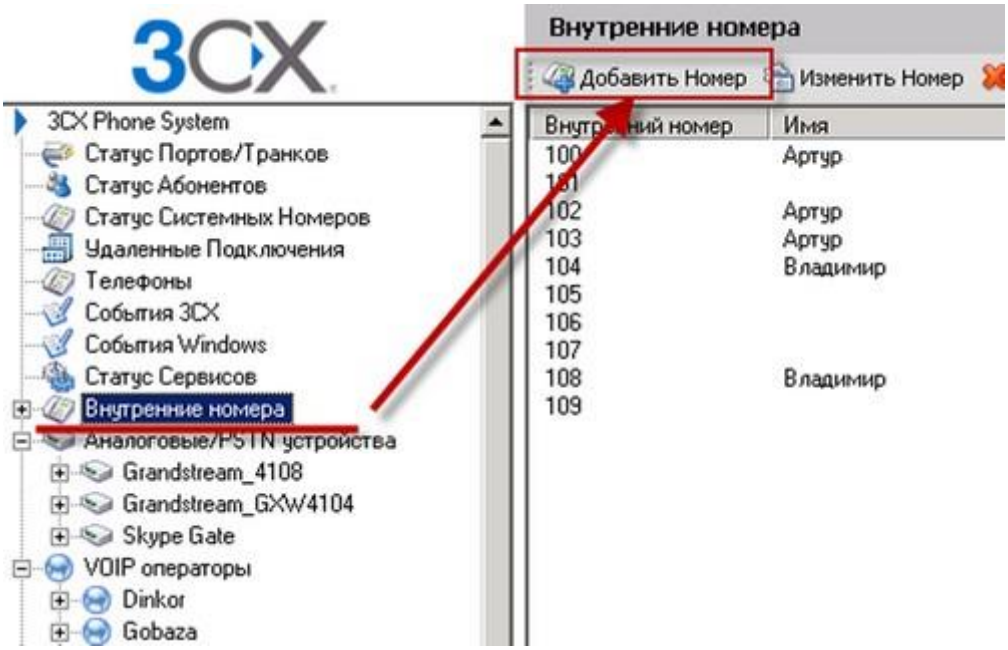
Теперь в меню Extensions мы можем наблюдать новый номер.

А в меню Terminals видим наш зарегистрированный IP телефон.

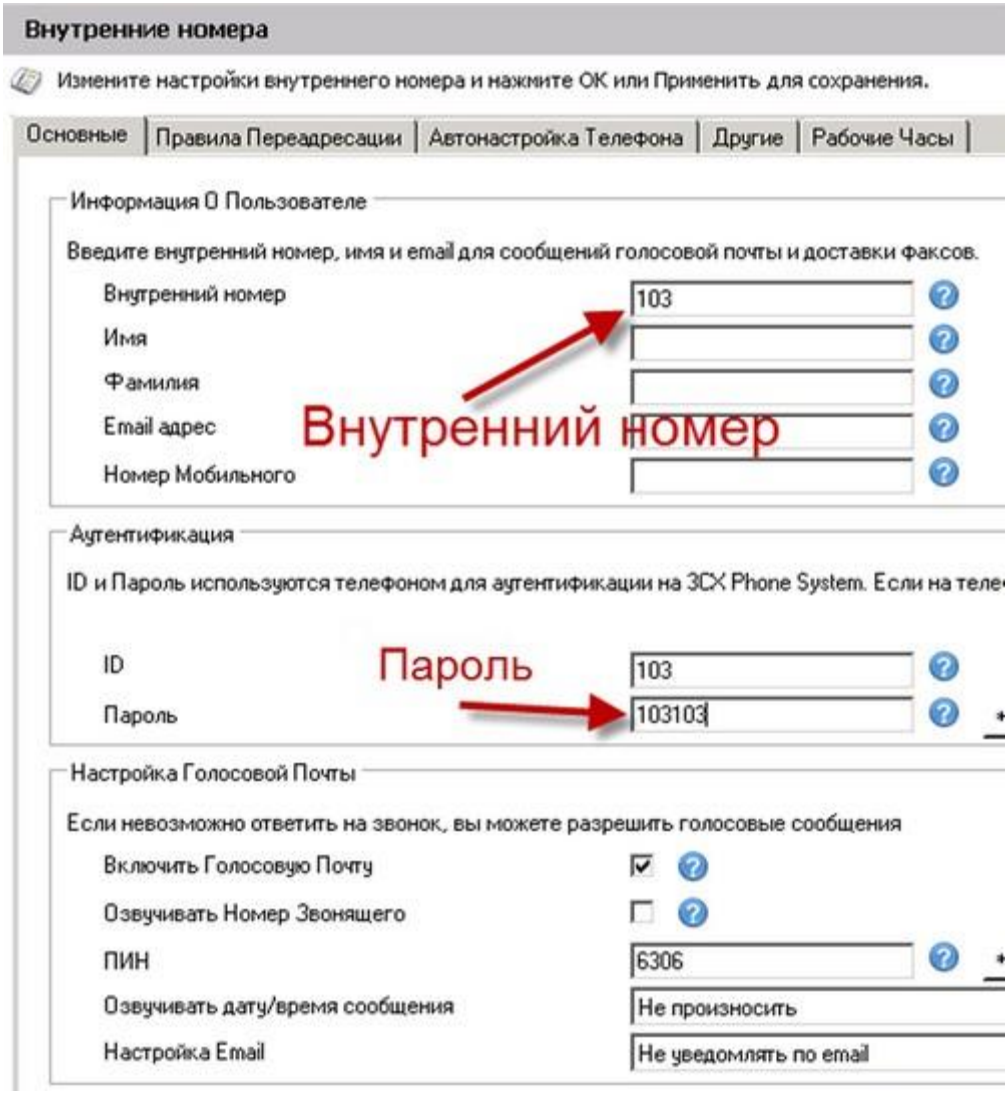
На самом аппарате должен высветится значок подключения ?и номер внутреннего абонента.
На этом настройка IP телефона для работы с IP-АТС AddPac IPNext успешно завершена.

Настройка IP-телефона для работы с 3CX Phone System

Настройка IP телефона (на примере Addpac AP-IP90) для работы с программной IP АТС 3CX начинается с регистрации внутреннего номера на сервере 3CX. Для этого перейдите во вкладку Внутренние номера и нажмите Добавить Номер.
Обращаем ваше внимание, что AddPac IP90 не понимает русский Caller Name, т.е. если на него приходит вызов с любого другого телефона, где имя-фамилия абонента на русском, разговор рвется через 30 секунд. С латиницей этого не происходит.



Затем задайте настройки внутреннего номера, в том числе и пароль.



Настройки в сервере 3CX Phone System на этом окончены.
Далее подключите IP телефон к АТС, для этого используйте программу удаленного доступа Telnet. Чтобы общение с аппаратом стало возможно нужно включить Telnet на своем компьютере (для Windows 7: Пуск – Панель управления – Программы и компоненты – Включение и отключение компонентов Windows) и узнать IP адрес вашего телефона.
Подключите телефон через LAN разъем к сети, затем нажмите кнопку MENU и в интерфейсе телефона перейдите Сетевые настройки – Настройки LAN. Здесь либо включите DHCP (автоматическое получение IP адреса в сети) либо задайте статический адрес. Для примера, мы задали - 192.168.0.112. Этот адрес будет фигурировать в дальнейших настройках телефона
Запускаем командную строку cmd и вводим:
telnet 192.168.0.112
Если компьютер нашел устройство по telnet, то IP–телефон запросит у вас login – root password – router. Выглядит в командной строке все так:
Welcome, APOS(tm) Kernel Version 8.51.001.
Copyright (c) 1999-2010 AddPac Technology Co., Ltd.
User Access Verification
Login: root
Password:
IP90> enable – нужно задать эту команду, что открыть доступ к телефону
IP90#

Далее введите команду, которая показывает все настройки вашего телефона show run – и сравните с тем, какие настройки должны быть для корректной работы АР IP90. Работающие настройки телефона приведены ниже (шаблон).
Для корректировки настроек используйте команду conf t или configure terminal:
IP90# configure terminal
IP90(config)#
Здесь вы можете изменить настройки IP телефона. Например, при подключении телефона к 3CX Phone System (для регистрации внутреннего номера) важна команда sip – ua. Вводите эту команду и перепишите все настройки sip – ua, как показано в шаблоне. Чтобы отменить неверно введенную команду используйте no.
Также особое внимание нужно уделить настройкам dial-peer. Именно эти настройки позволяют вашему телефону совершать входящие и исходящие звонки. Внимание, если dial-peer не настроены, соединение установить не удастся.
Шаблон настроек (с комментариями) Addpac IP90 (команда show run):
Welcome, APOS(tm) Kernel Version 8.51.001.
Copyright (c) 1999-2010 AddPac Technology Co., Ltd.
User Access Verification
Login: root
Password:
IP90> enable
IP90# show run (команда - показать все настройки)
Building configuration...
Current configuration:
!
version 8.51.001
!
hostname IP90
debug monitor
!
username root password router administrator
!
!
interface Loopback0
ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0 (информация о конфигурациях вашего порта LAN)
ip address 192.168.0.112 255.255.255.0
bridge-group 1
speed auto
no qos-control
!
interface FastEthernet0/1 (информация о конфигурациях вашего порта PC, как видно, он не подключен)
no ip address
bridge-group 1
speed auto
no qos-control
!
no ip routing
ip route 0.0.0.0 0.0.0.0 192.168.0.100
!
!

!
snmp name IP90_G2
!
ip tcp keep-alive count 5
ip tcp keep-alive idle 60
ip tcp keep-alive interval 5
!
!
http server
!
!
!
!
! IP PHONE OSD configuration.
!
Osd (пользовательские настройки)
language russian
network signaling sip
network sscp disable
phone save-mode always
phone lcd-type graphic
phone ring-type 1
phone volume ring 2
phone volume input 5
phone volume output 10
phone volume micbooster disable
phone auto-hook-on disable
phone display-name AP-IP90
phone dnd-mode silence
phone pbx-mode general
phone hook-mode digitwithdirect
phone auto-answer disable
phone conference-status disable
phone password 2337
phone password-status disable
phone admin-lock factory status disable
phone admin-lock internet status disable
phone admin-lock voip status disable
phone admin-lock service status disable
phone admin-lock auto-upgrade status disable
phone admin-lock sscp status disable
phone privacy-password 0000
phone privacy-status disable
phone privacy-lock menu status disable
phone privacy-lock incoming status disable
phone privacy-lock outgoing status disable
phone noanswer-sound off
phone noanswer-sound notify interval 60
phone emergency-number 1 112
phone emergency-number 2 119
phone emergency-number 3 911
phone emergency-number 4 999

phone contact-profile id 0 version 0
phone recording disable
!
! SSCP configuration.!
!
!
! SSCP Static CM List
sscp
!
! SSCP Dynamic CM List
sscp
!
!
sscp
call-manager broadcast port 8855
logger disable
logger level info
!
!
!
!
! VoIP configuration.
!
!
! Voice service voip configuration.
!
voice service voip
fax protocol t38 redundancy 0
fax rate disable
timeout tmohdt 300
call-barring unconfigured-ip-address
voip-inbound-call-barring enable
!
!
! Voice port configuration.
!
! SPEECH
voice-port 0/0
!
!
! N/A
voice-port 0/1
!
!
!
!
! Pots peer configuration.
!
dial-peer voice 0 pots (настройка исходящих звонков)
destination-pattern 103 (назначение 103 – внутренний номеров абонента в 3CX)
port 0/0 (важный параметр)
call-waiting

recording all
!
!
!
! Voip peer configuration.
!
dial-peer voice 1001 voip (настройка входящих звонков)
destination-pattern T (важный параметр)
session target sip-server (важный параметр)
voice-class codec 0
no vad
dtmf-relay rtp-2833
huntstop
recording all
!
!
!
dial-peer ipaddr-prefix n
dial-peer call-hold h
dial-peer call-transfer h
!
!
!
! Gateway configuration.
!
gateway
!
!
!
! Recording configuration.
!
recording
direction all
!
!
! Codec classes configuration.
!
voice class codec 0
codec preference 1 g711ulaw
codec preference 2 g711alaw
codec preference 3 g729
codec preference 4 g7231r63
codec preference 5 g726r32
!
!
!
! SIP UA configuration.
!
sip-ua (настройка регистрации телефона в 3CX Phone System)
no fault-tolerance
user-register
sip-username 103 (здесь, 103 – внутренний номер абонента в 3CX)

sip-password 103103 (здесь, 103103 – пароль внутреннего номера в 3CX)
sip-server 192.168.0.4 (здесь, 192.168.0.4 – адрес сервера 3CX)
rport enable
call-transfer-mode attended
media-channel early
register e164 (важный параметр)
3way-conference local
recording-info-notify
!
!
! SMS UA configuration.
!
sms-ua
check-to-header enable
!
!
! Tones
!
!
!
!
line console
!
line vty
!
!
sms
quota 30
!
!
! PS Client configuration.
!
psclient
service disable
retry_timer 10000
alive_timer 15000
!
!
End

2.22. Практическая работа № 22
Настройка программных IP-телефонов, факсов

Этапы:
Подготовка ОС Ubuntu 14.04 LTS к установке Asterisk:
обновление системы;
установка компилятора и его пакетов.
Скачивание пакетов с официального сайта:
Asterisk 13;

LibPRI;
DAHDI.
Распаковка пакетов в usr/src.
Компиляция:
LibPRI;
DAHDI;
Asterisk.
Вход в CLI, проверка работоспособности внутренних команд.
Запуск как службы. Настройка автозагрузки.
Перезагрузка сервера и проверка корректности автозапуска.
Заходим в темнинал Ubuntu сочетанием клавиш Ctrl+Alt+T и получим права суперпользователя вводом команды. (все дальнейшие действия будут проводиться с использованием прав root)

```
sudo -s
```

Обновим системные пакеты, а так же установим дополнительные build-essential, libxml2-dev и ncurses-dev – пакеты, без которых Asterisk не сможет корректно запуститься.

```
apt-get update
apt-get install build-essential libxl2-dev ncurses-dev
```

Перезагрузим систему.

```
reboot
```

Создадим папку, куда будем скачивать дистрибутивы Asterisk, DAHDI и LibPRI и сразу же перейдем в созданный каталог.

```
mkdir -p /usr/src/asterisk
cd /usr/src/asterisk
```

Скачиваем все необходимые пакеты с официального сайта Asterisk (http://www.asterisk.org/), а это: исходные файлы Asterisk 13.8.2 (на момент написания инструкции является последней актуальной версией)(Рисунок 2.1.1), DAHDI (пакет, осуществляющий обработку цифровых и аналоговых интерфейсов) (Рисунок 2.1.2), и LibPRI (библиотека, которая предназначена для работы с потоковыми TDM-интерфейсами ISDN: PRI (Primary Rate Interface) и BRI (Basic Rate Interface)) (Рисунок 2.1.3):

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/
asterisk-13-current.tar.gz
```

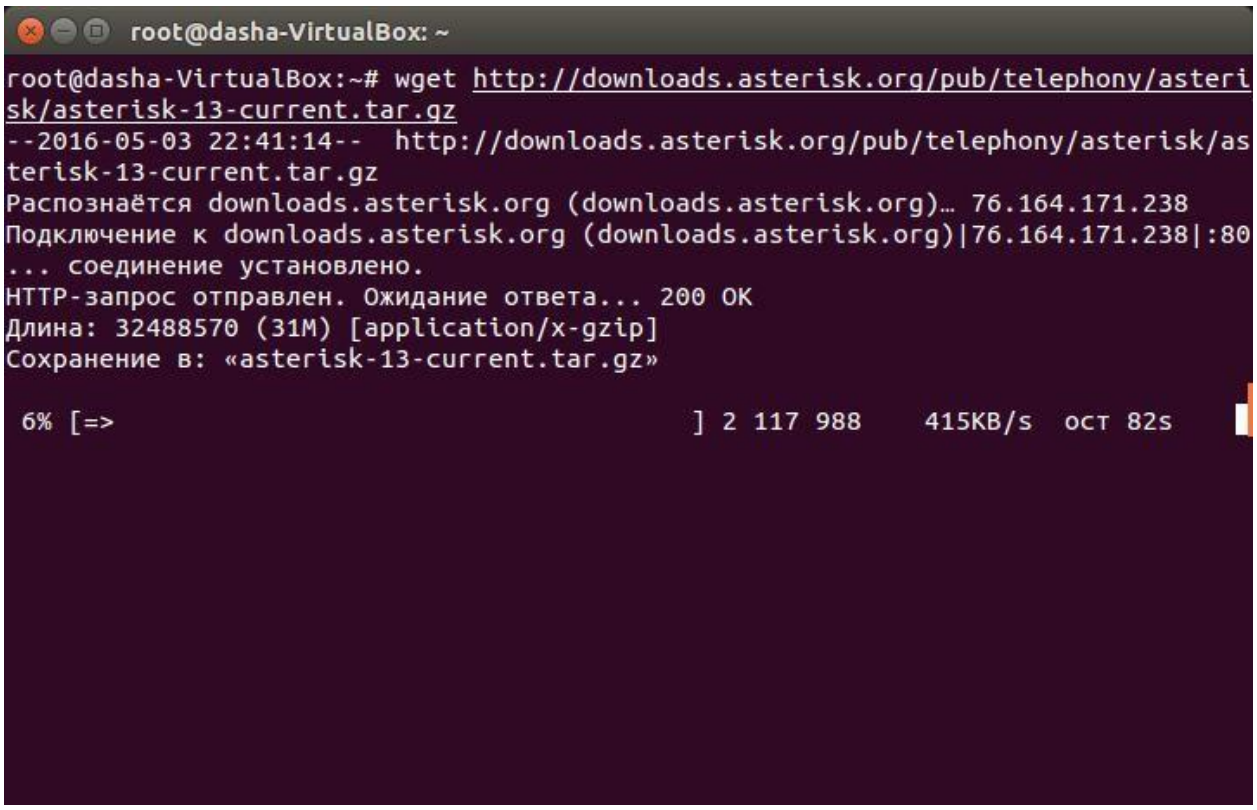


Рисунок 2.1.1 – Окно загрузки Asterisk с официального сайта.

wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz

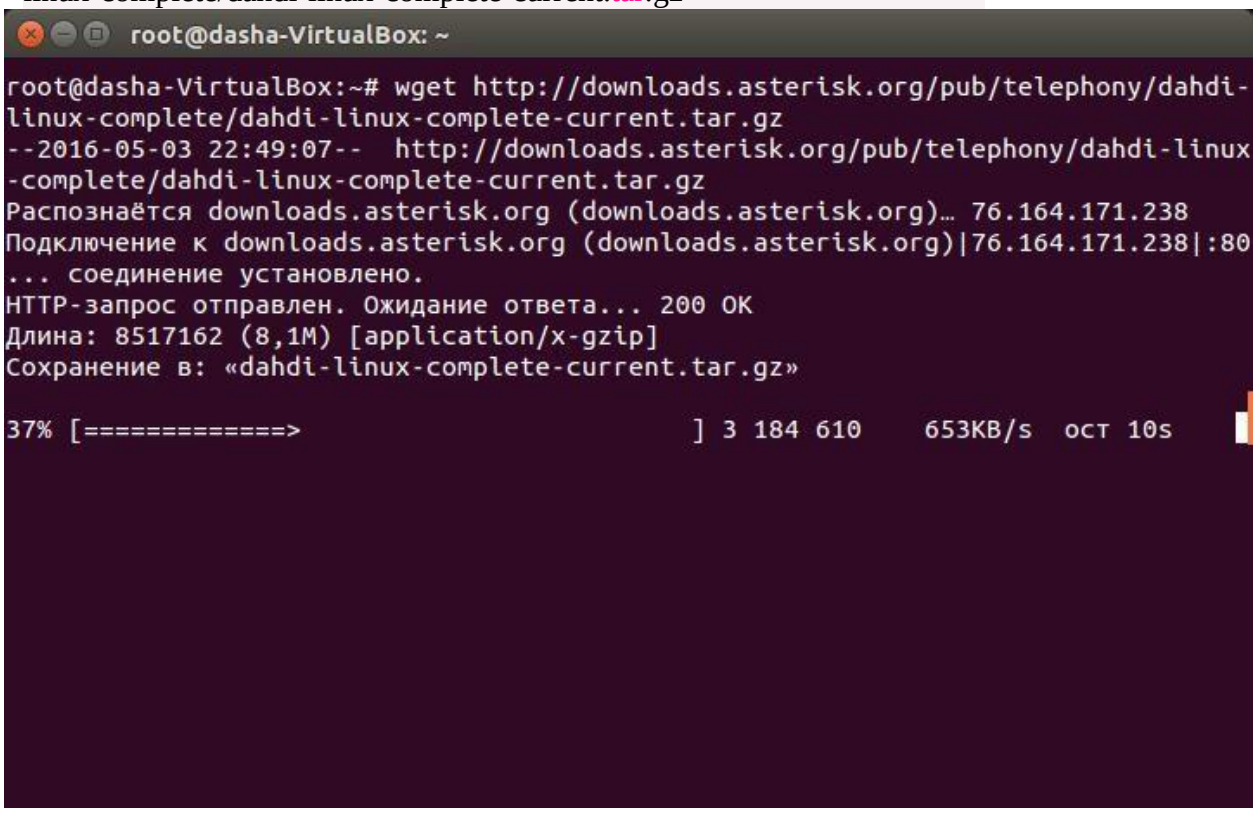


Рисунок 2.1.2 – Окно загрузки DAHDI с официального сайта.

```
wget
http://downloads.asterisk.org/pub/telephony/libpri/libpri-
current.tar.gz
```

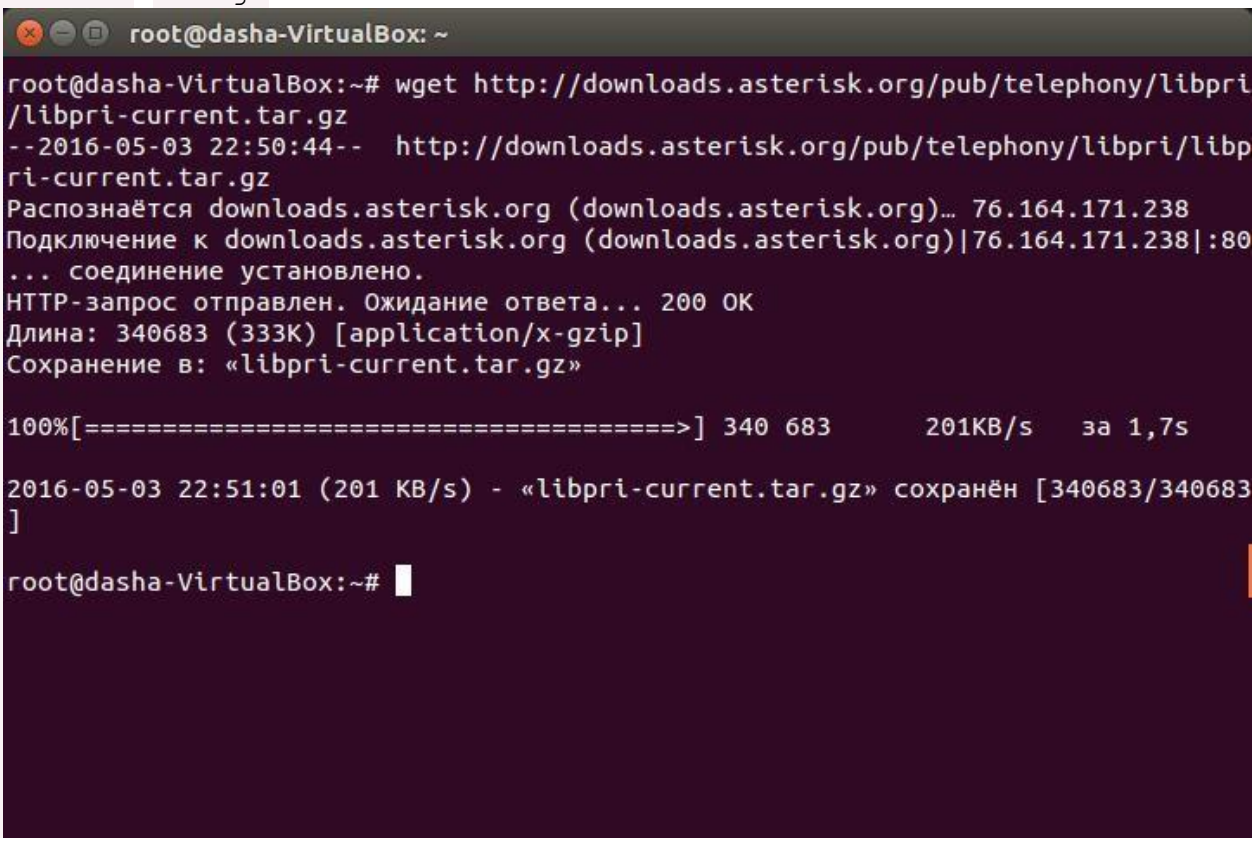


Рисунок 2.1.3 – Окно загрузки LibPRI с официального сайта

Распаковываем скачанные исходные файлы с помощью консольного архиватора tar и команды -xvf в папку, которую создали ранее, с помощью команды -C.

```
tar -xvf dahdi-linux-complete-current.tar.gz -C
/usr/src/asterisk tar -xvf libpri-current.tar.gz -C /usr/src/asterisk tar -xvf asterisk-13-
current.tar.gz -C /usr/src/asterisk
```

В первую очередь произведем компиляцию DAHDI, а затем зададим автоматический запуск службы DAHDI при старте системы.

```
cd /usr/src/asterisk/dahdi-linux-complete-* make all make install make config sysv-rc-conf
dahdi on
```

8) Далее компилируем библиотеку LibPRI.

```
cd /usr/src/asterisk/libpri-*
  make
  make install
```

9) Приступим к установке Asterisk 13.

```
  cd /usr/src/asterisk/asterisk-*
  ./configure
```

При проверке конфигураций Asterisk может выдавать сообщения об ошибках разного рода. Ниже приведены некоторые из них и их решения.

– Текст ошибки:

configure: error: *** JSON support not found (this typically means the libjansson development package is missing)

В этом случае необходим пакет jansson, причем нужна development редакция: jansson-devel. Чтобы исправить данную ошибку, следует сделать следующее:

```
cd /usr/src/
wget http://www.digip.org/jansson/releases/jansson-
```

2.7.tar.gz
tar -xvf jansson-2.7.tar.gz cd /usr/src/jansson* ./configure --prefix=/usr/
make clean make make install ldconfig
– Текст ошибки:
configure: error: *** uuid support not found (this typically means the uuid development package is missing
Отсутствует библиотека uuid, причем нужна development редакция: libuuid-devel. Чтобы исправить данную ошибку, следует сделать следующее:
apt-get install uuid-dev – Текст ошибки:
configure: error: *** termcap support not found (on modern systems, this typically means the ncurses development package is missing)
Отсутствует библиотека ncurses, точнее не сама библиотека (она может быть), а ее компоненты для разработчиков, для сборки программ. Чтобы исправить данную ошибку, следует сделать следующее:
apt-get -y install ncurses-dev – Текст ошибки:
configure: WARNING: *** Asterisk now uses SQLite3 for the internal Asterisk database.
Отсутствует библиотека SQLite, точнее не сама библиотека (она может быть), а ее компоненты для разработчиков и сборки программ. Чтобы исправить данную ошибку, следует сделать следующее:
apt-get -y install sqlite-dev
Далее запускаем проверку конфигураций еще раз.
cd /usr/src/asterisk/asterisk-*
./configure
Когда увидим заставу, как на Рисунке 2.1.4, значит, что с настройками все в порядке и можно начать компиляцию Asterisk.

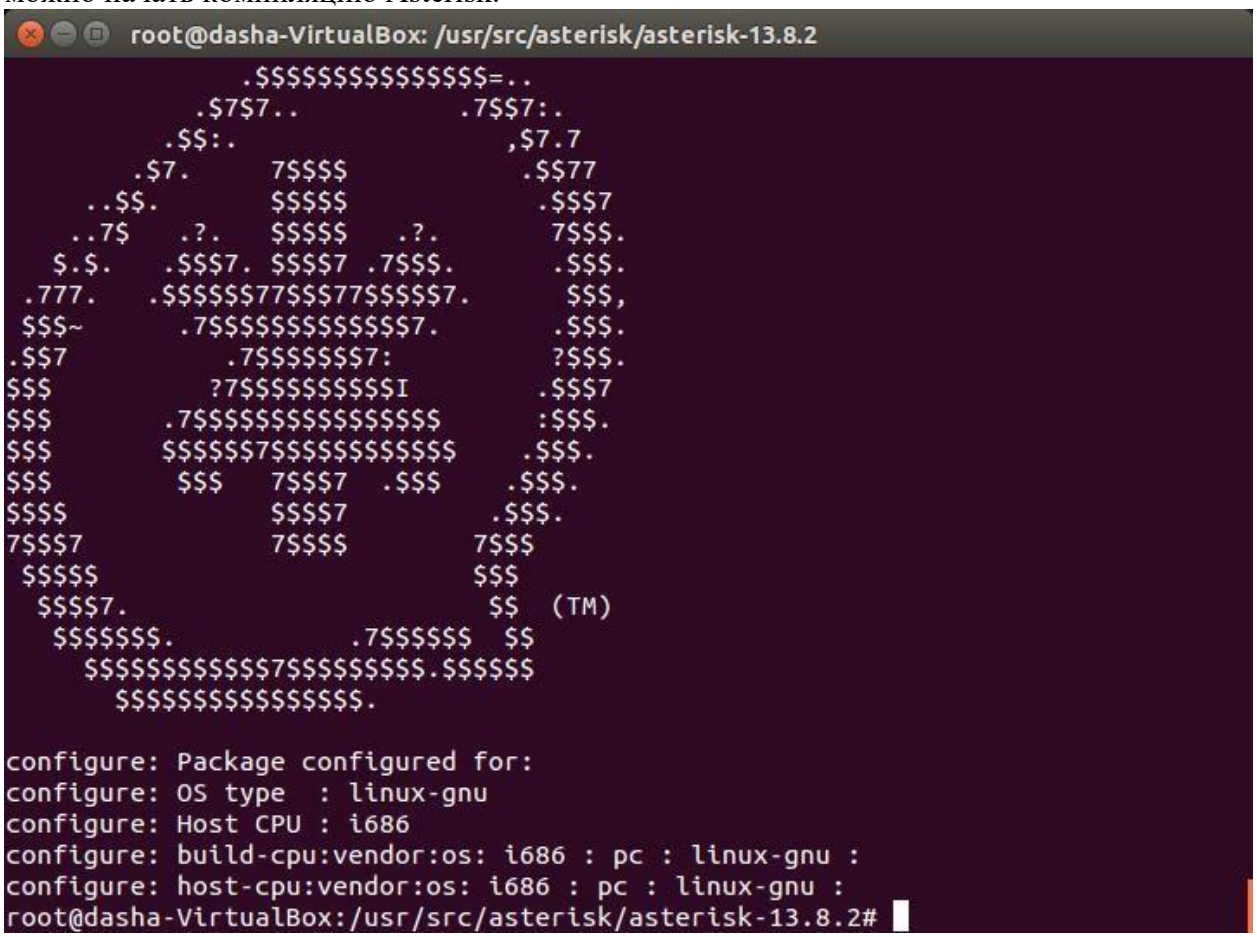


Рисунок 2.1.4 – Окно с заставкой, информирующей о готовности Asterisk к компиляции

Теперь вызовем систему выбора модулей Asterisk, для дополнительных надстроек перед основной установкой (Рисунок 2.1.5).

make menuselect

Рисунок 2.1.5 – Окно выбора компилируемых модулей через make menuselect По большей части, все необходимые модули уже включены. Предоставлен полный выбор для добавления или удаления модулей. При его выборе у него будет короткое описание, за что он отвечает.

В разделе Add-ons можно выбрать модуль format_mp3, который понадобится для того, чтобы всякая звуковая запись производилась в формате mp3, а не в gsm. Также, выбираем раздел Core Sound Packages и выбираем все необходимые форматы звуковых пакетов
(Рисунок 2.1.6).

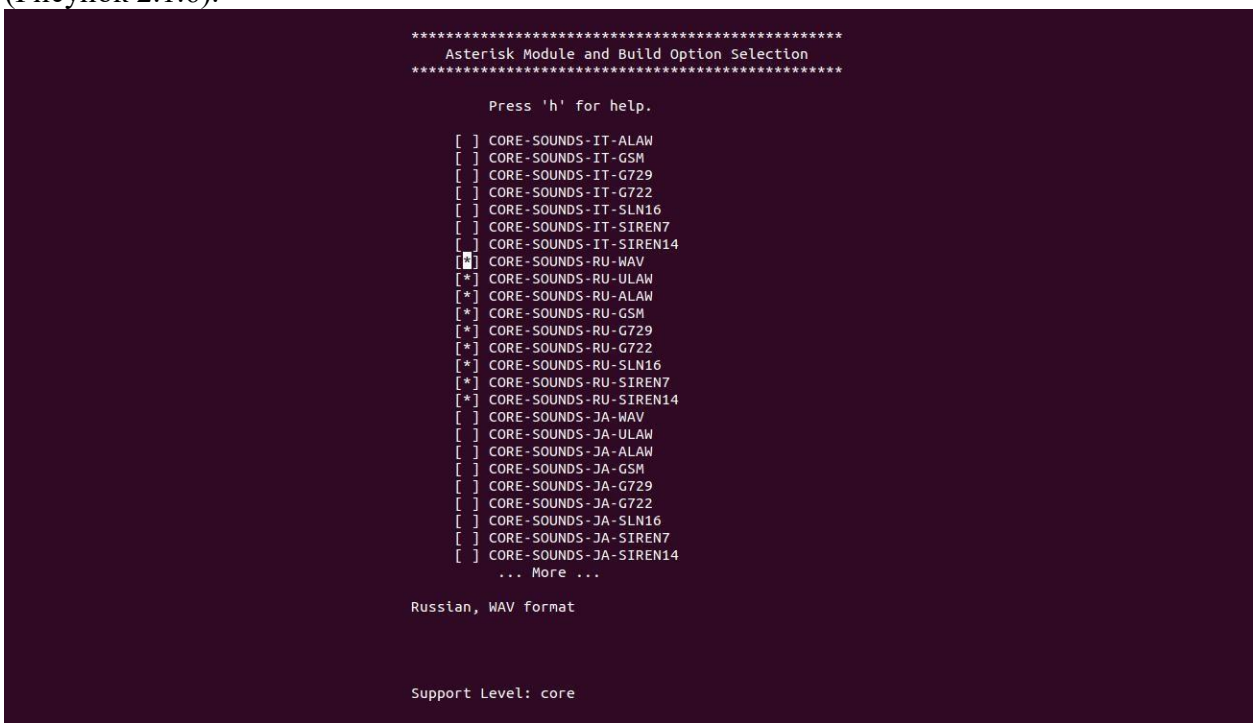


Рисунок 2.1.6 – Окно выбора всех русскоязычных форматов во вкладке Core Sound Packages

В разделе Music On Hold File Packages включаем все модуди, а в Extras Sound Packages включаем первые четыре модуля, содержащие EN.
После сделанных надстроек нажимаем клавишу «x» (в английской раскладке) для сохранения и выхода в окно консоли для конечной установки Asterisk. Далее вводим команду:

```
make
```

В ходе выполнения функции make произошла ошибка, показанная на Рисунке 2.1.7.

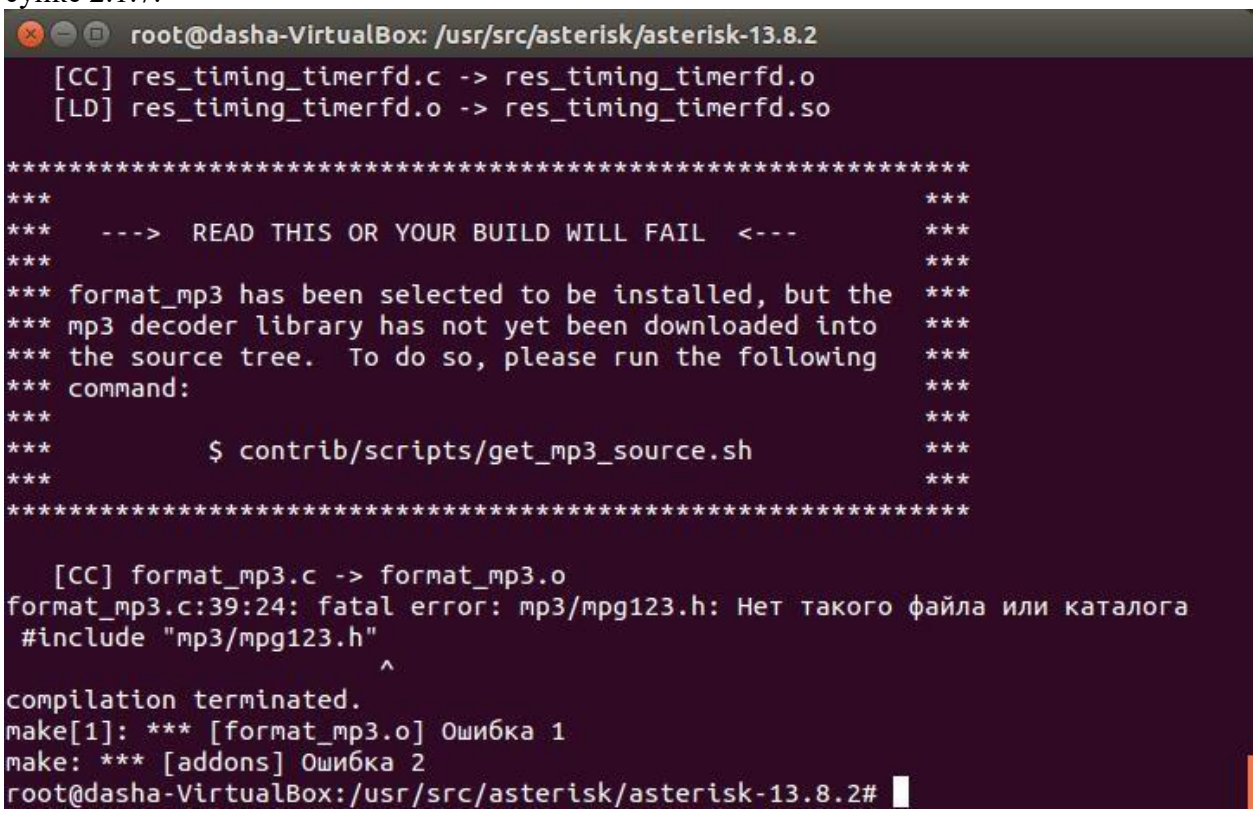


Рисунок 2.1.7 – Окно с сообщением об ошибке Для ее устранения вводим требуемую команду:

```
contrib/scripts/get_mp3_source.sh
```

Затем снова запускаем команду:

```
make
```

После успешного выполнения команды make, увидим совет сделать следующий шаг (Рисунок 2.1.8).

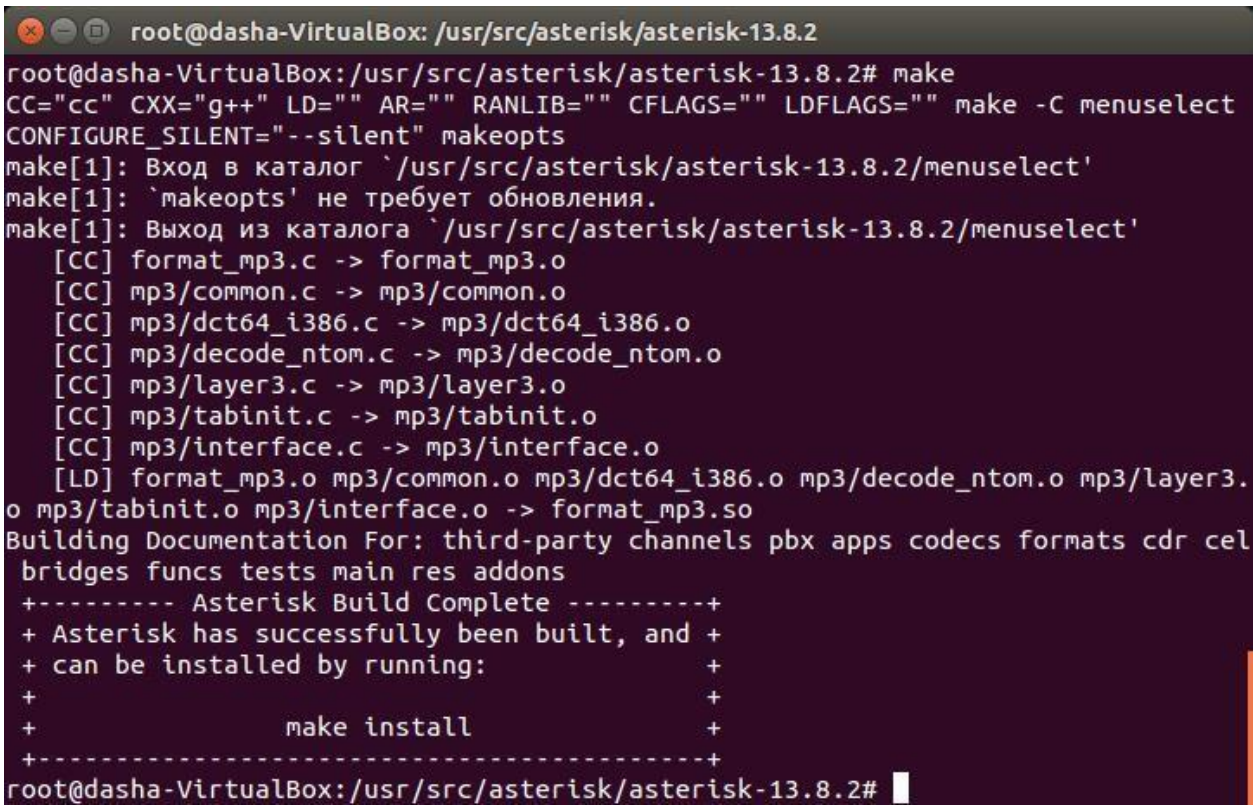


Рисунок 2.1.8 – Окно с сообщением об успешной сборке Asterisk

Далее вводим команды, обозначающие установку Asterisk в систему, создание образцов, создание автозапуска и добавление Asterisk в автозагрузку.

make install make samples make config sysv-rc-conf asterisk on

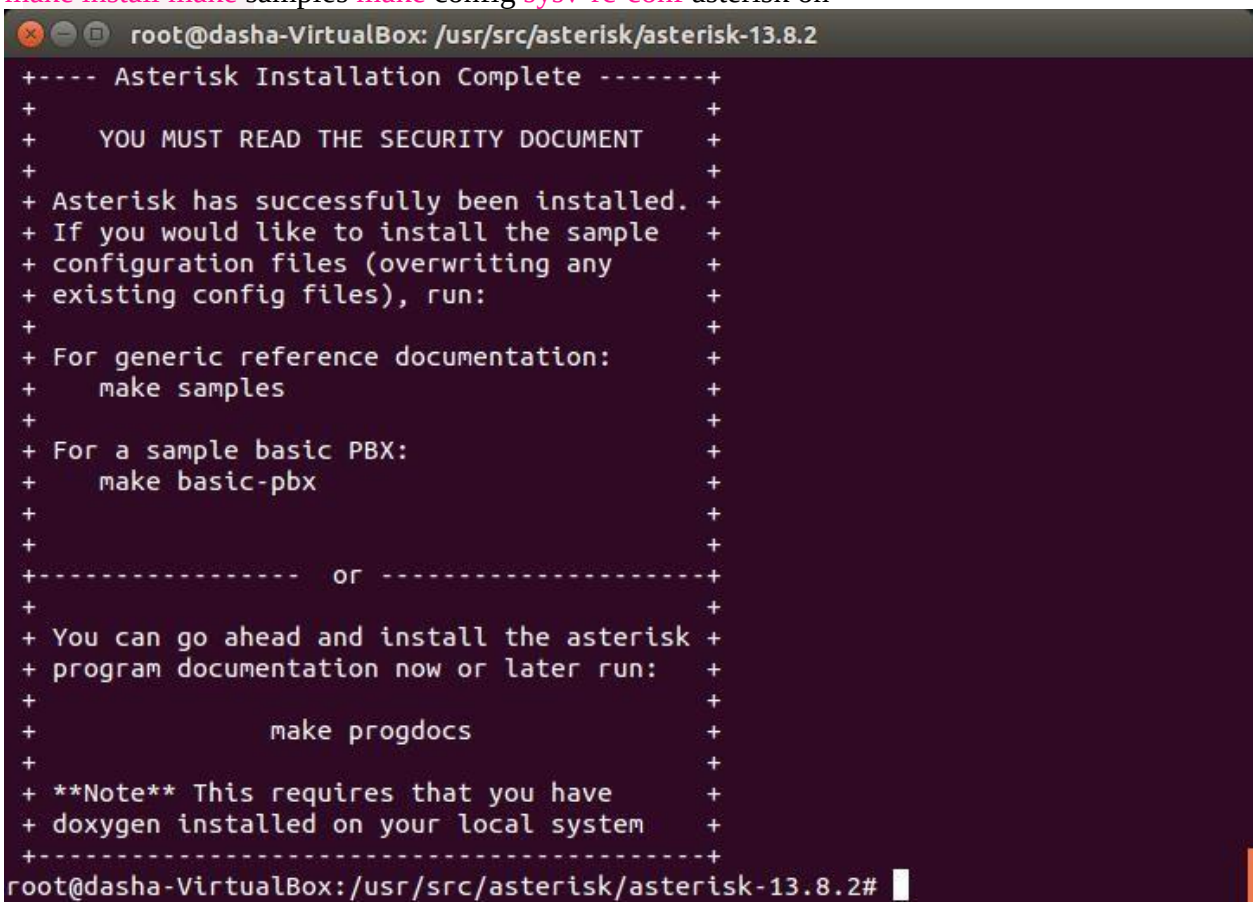


Рисунок 2.1.9 – Окно, подтверждающее успешную установку Asterisk в систему 10)

Перезагружаем сервер:

reboot

11) Проверяем работоспособность Asterisk, вводя команду (Рисунок 2.1.10):

rasterisk

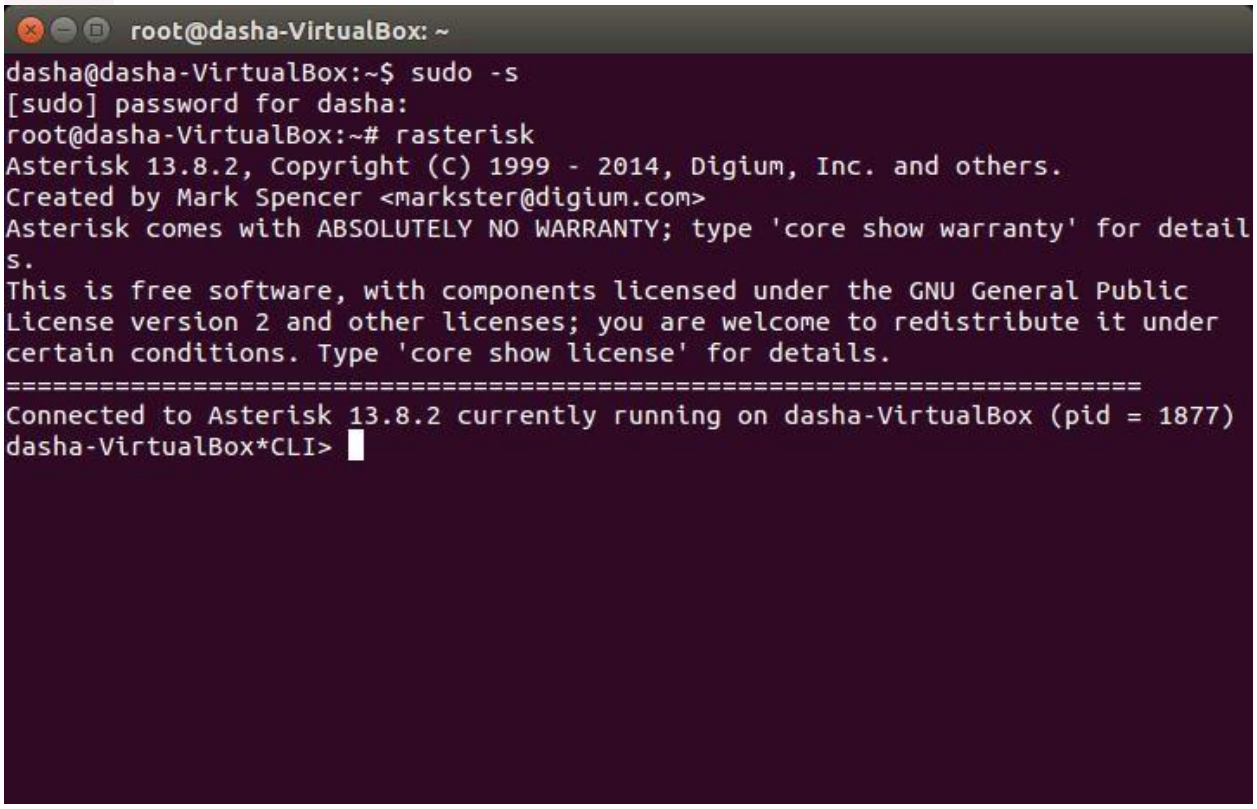


Рисунок 2.1.10 – Окно успешного соединения с Asterisk

12) Проверяем командой sysv-rc-conf --list о том, что Iptables – отключен, а Asterisk и DAHDI – включены.

Контрольное тестирование к лабораторной работе №1.

Кто является основным разработчиком Asterisk?

Стив Джобс;

Марк Спенсер;

Разработано народом; Линус Торвальдс.

Какие протоколы из перечисленных поддерживает Asterisk?

H.323; Skype;

SIP;

IAX.

Что такое DAHDI?

Программа телефонии;

Модуль эхоподавления;

Драйверы для внешних интерфейсов Asterisk; Библиотека.

По какой лицензии распространяется Asterisk?

Comercial;

GSPF;

WTFPL;

GNU GPL.

Что нужно сделать перед установкой Asterisk из исходных кодов?

Обновить систему;

Установить антивирус;

Установить компиляторы и зависимости;

Отключить автоматическое обновление системы.

Какая команда служит для распаковки tar.gz архивов?

tar xvf <имя архива>;
unarchive <имя архива>;
bar xvf <имя архива>; rar xvf <имя архива>.
Какая утилита служит для компиляции исходного кода?
install;
./configure;
make; cd.
В какой директории хранятся конфигурационные файлы Asterisk?
/var/asterisk;
/root/asterisk;
/etc/asterisk; /src/asterisk.
Какой из кодеков, можно использовать для записи голосовых сообщений в стандартной сборке Asterisk (без установки дополнительных модулей)?
G.729;
GSM;
G.711; mp3.
Что делает команда wget?
Установку пакетов из интернета;
Компиляцию;
Перезапускает астериск;
Изменяет конфигурацию файла.

Организация способов взаимодействия и подключения абонентов к сети

2.23. Практическая работа № 23
Развертывание сети с использованием VLAN для IP-телефонии

Внутристанционное соединение;
Установка редактора файлов в Linux;
Изменение конфигурационных файлов:
indications.conf;
sip.conf;
extensions.conf.
Проверка работоспособности сети.

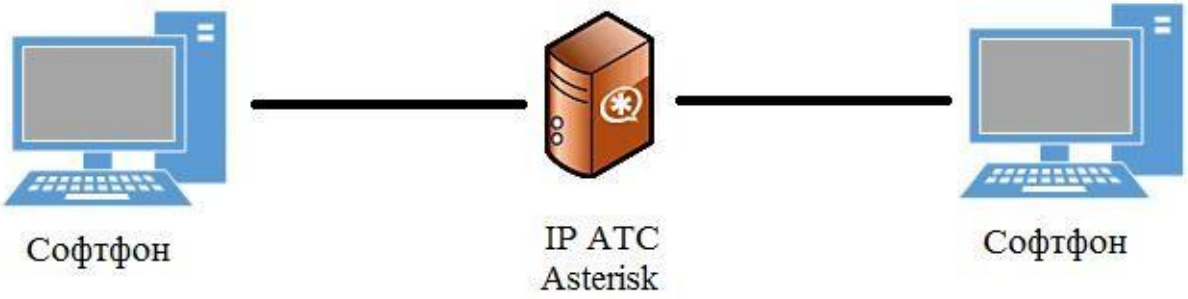


Рисунок 3.2.1 – Схематичное построение сети к лабораторной работе №2

1) Работа будет производится в виртуальной машине Oracle VM VirtualBox на двух операционных системах: Linux Ubuntu 14.04 LTS и Windows XP. Создадим для них внутреннюю локальную сеть со статическими IP адресами. Для этого

XP: Пуск → Панель управления → Сетевые подключения → Щелкнем ПКМ на Подключение по локальной сети и выбираем пункт Свойства → Выбираем Протокол интернета (TCP/IP) и нажимаем на его свойства → Задаем параметры, как на рисунке 3.2.2.

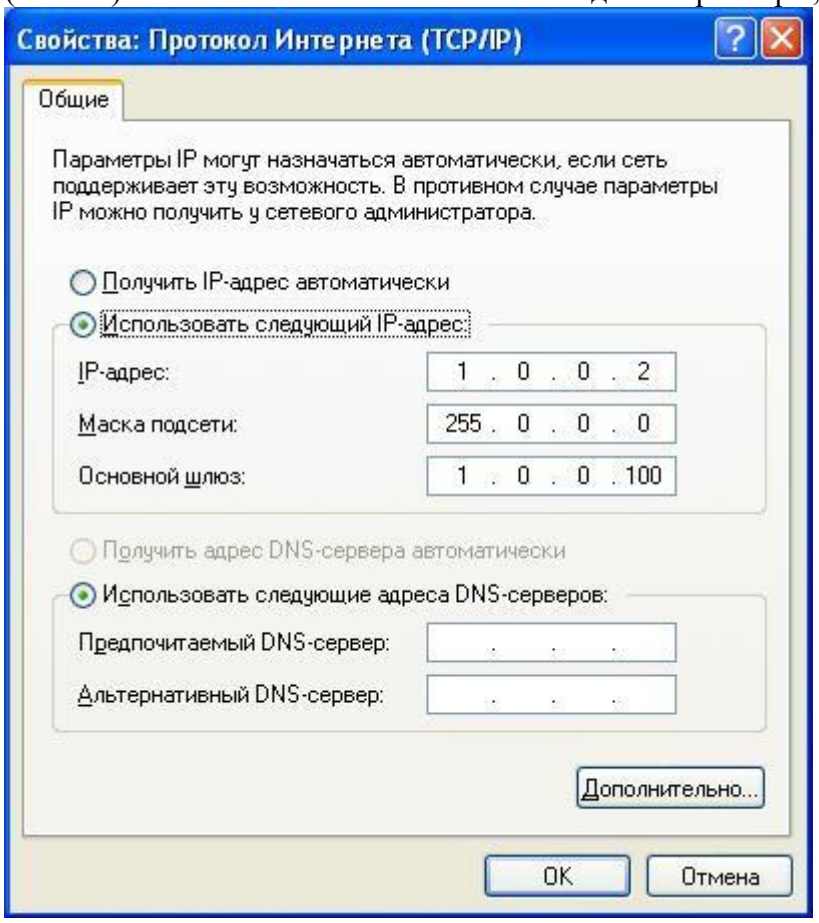


Рисунок 3.2.2 – Окно свойств: протокол интернета (TCP/IP) в ОС Windows

Linux: Параметры системы → Сеть → Параметры используемой сети → Параметры IPv4 → Задаем параметры, как на рисунке 3.2.3.

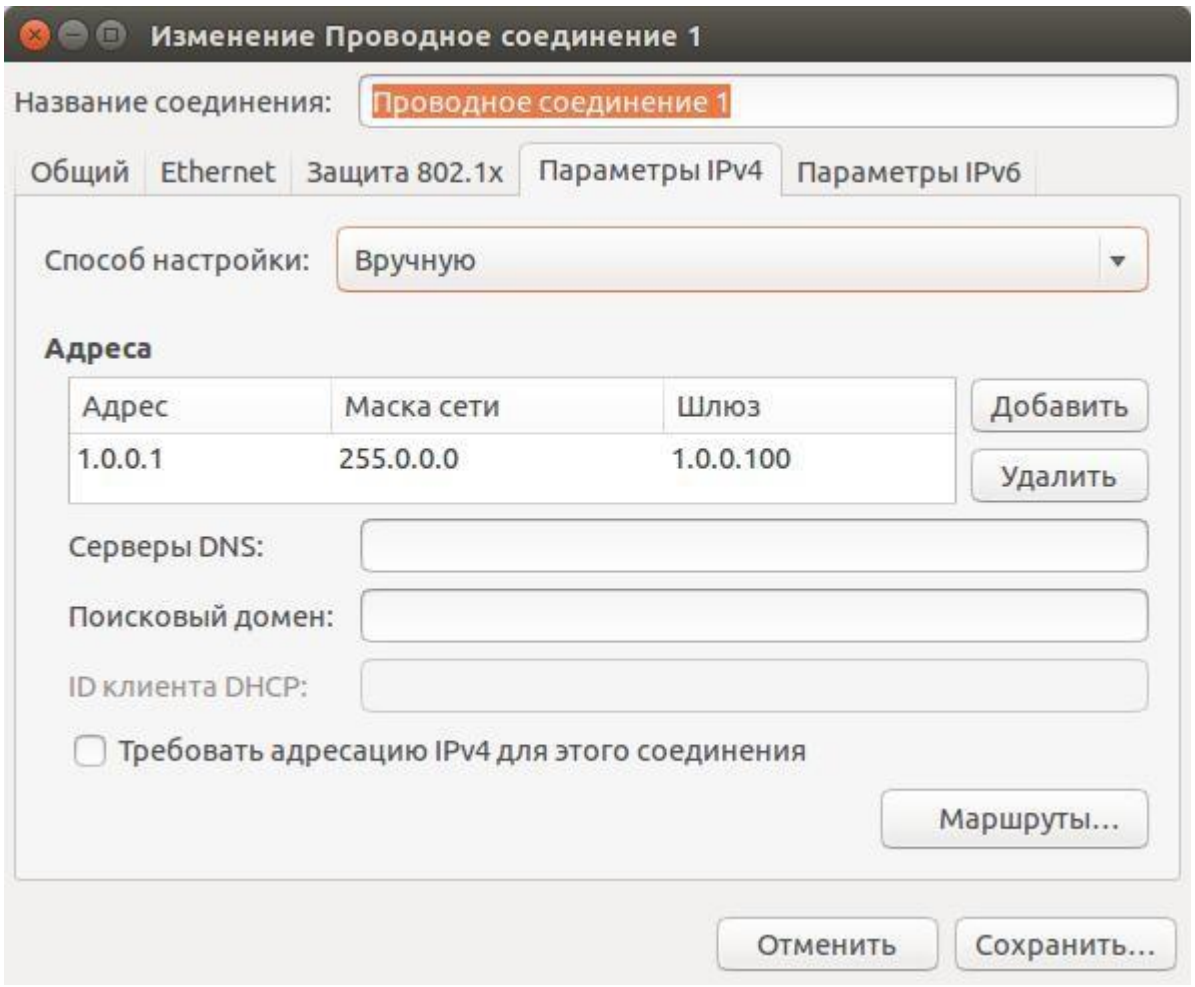


Рисунок 3.2.3 – Окно изменений проводного соединения в ОС Linux

После этого начнем изменение конфигурационных файлов, начиная с indications.conf, отвечающий за звуки, которые абонент слышит в телефонной трубке.

Для того, чтобы редактировать те или иные файлы в ОС Linux, необходимо иметь права суперпользователя. Т.к. получить эти права можно лишь используя терминал, то и редактировать файлы нужно тоже в терминале, а для этого нам понадобится редактор Vim. Первым делом, скачиваем этот редактор, выполняя в терминале команду:

```
apt-get install vim
```

После успешной установки Vim, следует открыть файл, который мы хотим отредактировать. Для этого перейдем в директорию, где находится интересующий нас файл и откроем его командой vim.

```
cd /etc/asterisk/
vim indications.conf
```

Для каждой страны звуки, которые абонент слышит в телефонной трубке - свои, поэтому, когда мы откроем файл indications.conf, то увидим, что по умолчанию стоит страна США, но раздел, посвященный России в файле так же имеется, где проведены необходимые настройки, поэтому следует просто поменять первоначальную настройку, записав в строке вместо country=us, countru=ru, после этого сохраним и выйдем (Рисунок 3.2.4).

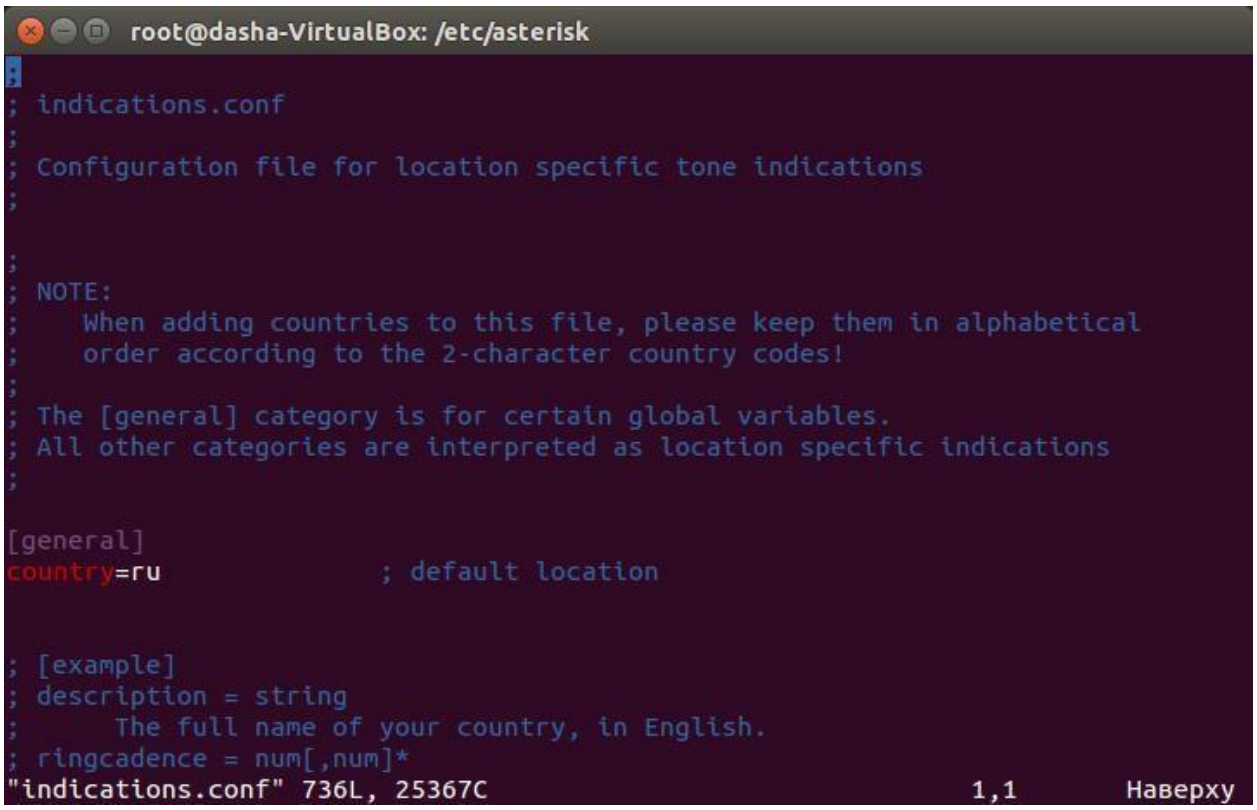


Рисунок 3.2.4 – Окно файла indications.conf

Следующим конфигурационным файлом, который мы будем изменять – файл sip.conf, который определяет работу SIP устройств.

В данном файле существуют готовые шаблоны, которые можно использовать при формировании настроек SIP устройств. Признаком шаблона является восклицательный знак (!). Шаблоны имеют структуру уложенности, т.е. создав шаблон [basic-options](!), мы можем создать на его основании еще один шаблон, к примеру [nattedphone](!,basic-options), в который будут включены дополнительные настройки и настройки из шаблона [basic-options](!).(Рисунок 3.2.5)

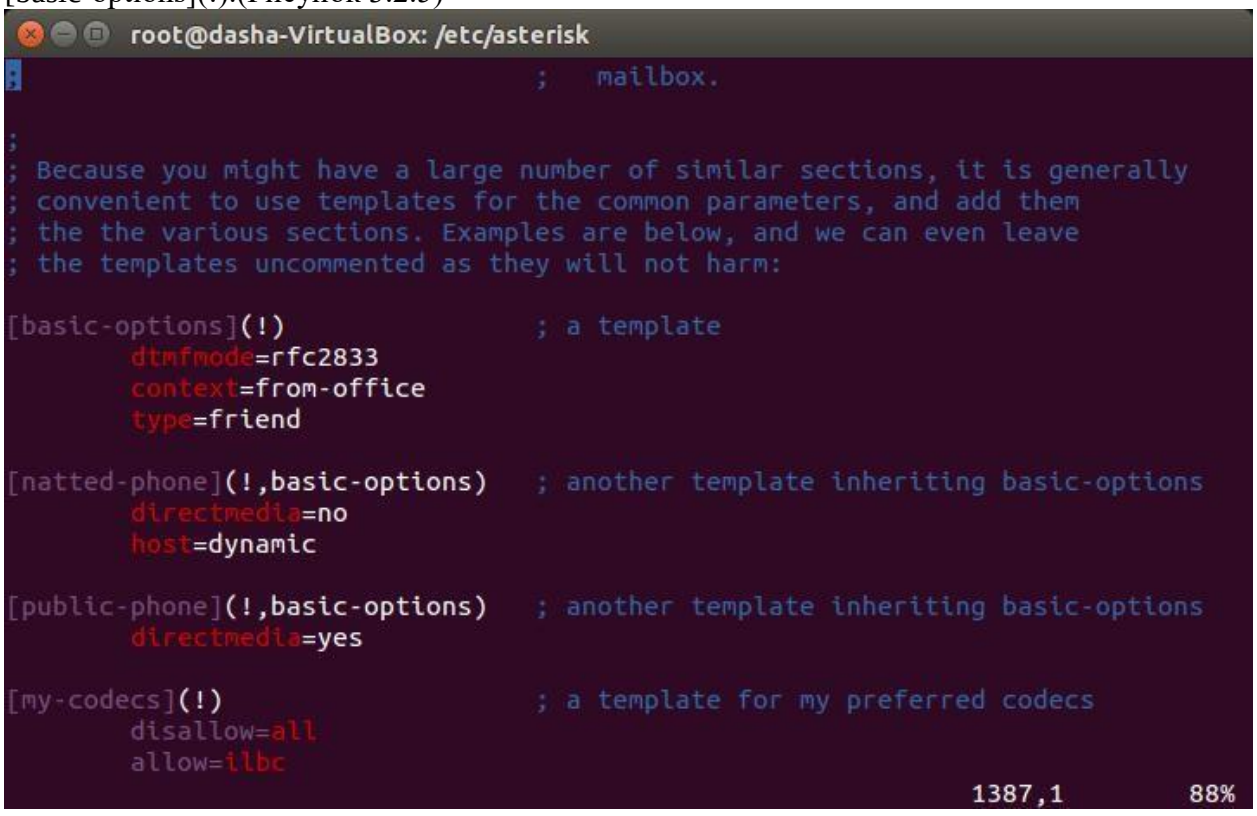


Рисунок 3.2.5 – Окно файла sip.conf с готовыми шаблонами

В шаблонах [basic-options] и [natted-phone] использовались такие команды, как dtmfmode, context, type, directmedia и host. Рассмотрим все по порядку:

dtmfmode – команда, отвечающая за звуковые сигналы, передаваемые по телефонному каналу. Здесь используем стандарт rfc2833, отвечающий за тональный набор в SIP протоколе. Также можно вписать inband или info, но info не рекомендуется, т.к. стандарт еще в процессе разработки, а inband передает тоны в форме синусоидальной кривой, т.е. без сжатия, а это значит, что при нажатии на кнопок на телефоне можно ничего не услышать.

context – команда, в которой можно прописать любое имя, которое далее будет использоваться в контексте как ссылка, к примеру, в файле extensions.conf.

type – параметр, который может принимать одно из трех значений: peer, user, friend. Peer – SIP пир, который Asterisk может использовать для совершения исходящих вызовов; user – SIP пир, для входящих вызовов Asterisk; friend – запись, которая одновременно и user и peer, этот тип наиболее подходит для телефонов и других устройств.

directmedia – параметр, определяющий направление трафика. Возможные варианты: yes (направляет трафик по оптимальному пути), no (запрещает перенаправления трафика, в этом случае все RTP потоки проходят через Asterisk).

host – имя домена или хоста SIP сервера. Если параметр задан как dynamic, тогда не будет совпадений, до того как SIP клиент зарегистрируется на сервере.

Заходим в файл

```
cd /etc/asterisk/
vim sip.conf
```

Редактируем его, создавая двух sip-клиентов, воспользовавшись шаблоном [natted-phone], задав только пароль (Рисунок 3.2.6).

```
[101](natted-phone)
secret=ваш_любой_пароль
[102](natted-phine)
secret=ваш_любой_пароль
```

После этого нужно сохраниться и выйти.

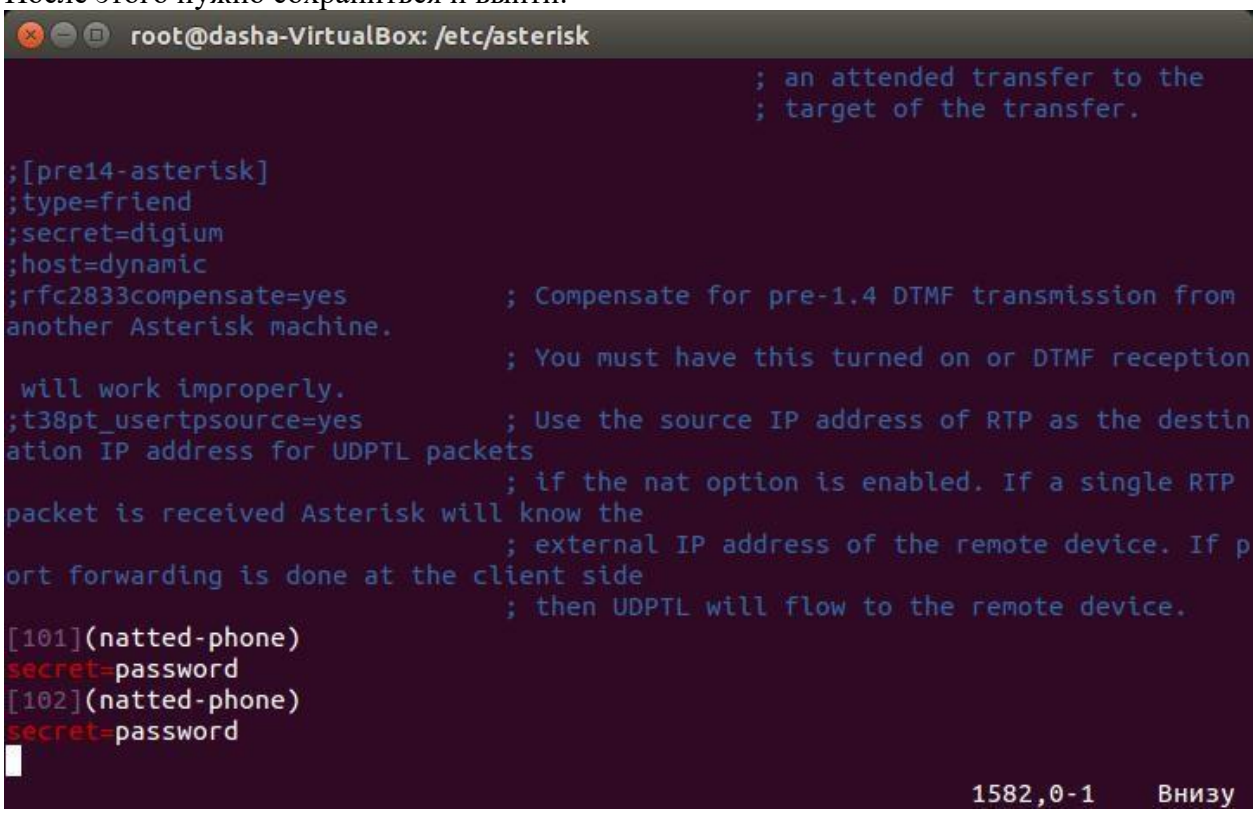


Рисунок 3.2.6 – Окно файла sip.conf с измененными параметрами

Следующим шагом нужно отредактировать файл extensions.conf. Он регулирует правила совершения звонков, т.е. в нем содержится то, как будут происходить звонки через нашу АТС. В нем есть несколько разделов [general] и [global], а так же названия диалпланов. Диалплан направляет каждый звонок от его источника, с помощью приложений (Dial, Voicemail, Background, ConfBridge и тд), в пункт назначения.

```
cd /etc/asterisk/
vim extensions.conf
```

После перехода в файл extensions.conf его нужно отредактировать (Рисунок 3.2.7).

```
[from-office]
exten => 101,1,Dial(SIP/101)
exten => 102,1,Dial(SIP/102)
```

Команда плана набора Asterisk "Dial", пытается установить соединение, одного устройства с другим, произведя вызов SIP пира.

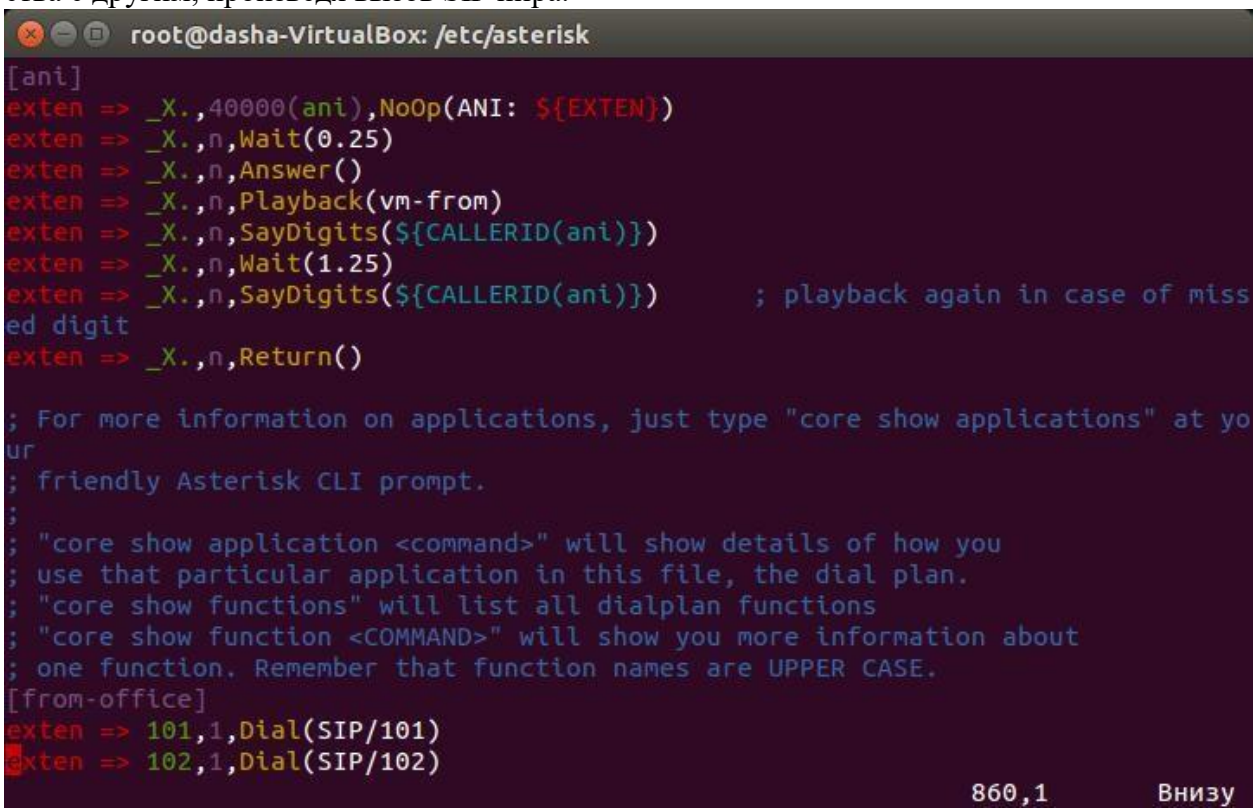


Рисунок 3.2.7 – Окно редактирования файла extensions.conf

После выполненныхопераций заходим в Asterisk с максимальным уровнем детализации и запускаем перезагрузку всех конфигураций:

```
asterisk -rvvv
reload
```

4) Проверка работоспособности сети.

Для проверки связи нам потребуется бесплатный SIP SoftPhone, к примеру, PhonerLite (скачивается с официального сайта http://www.phonerlite.de/), работающий на ОС Windows. Устанавливаем его в систему, запускаем и произведем настройку, а это - впишем IP адрес Asterisk в раздел Прокси/сервер авторизации (Рисунок 3.2.8).

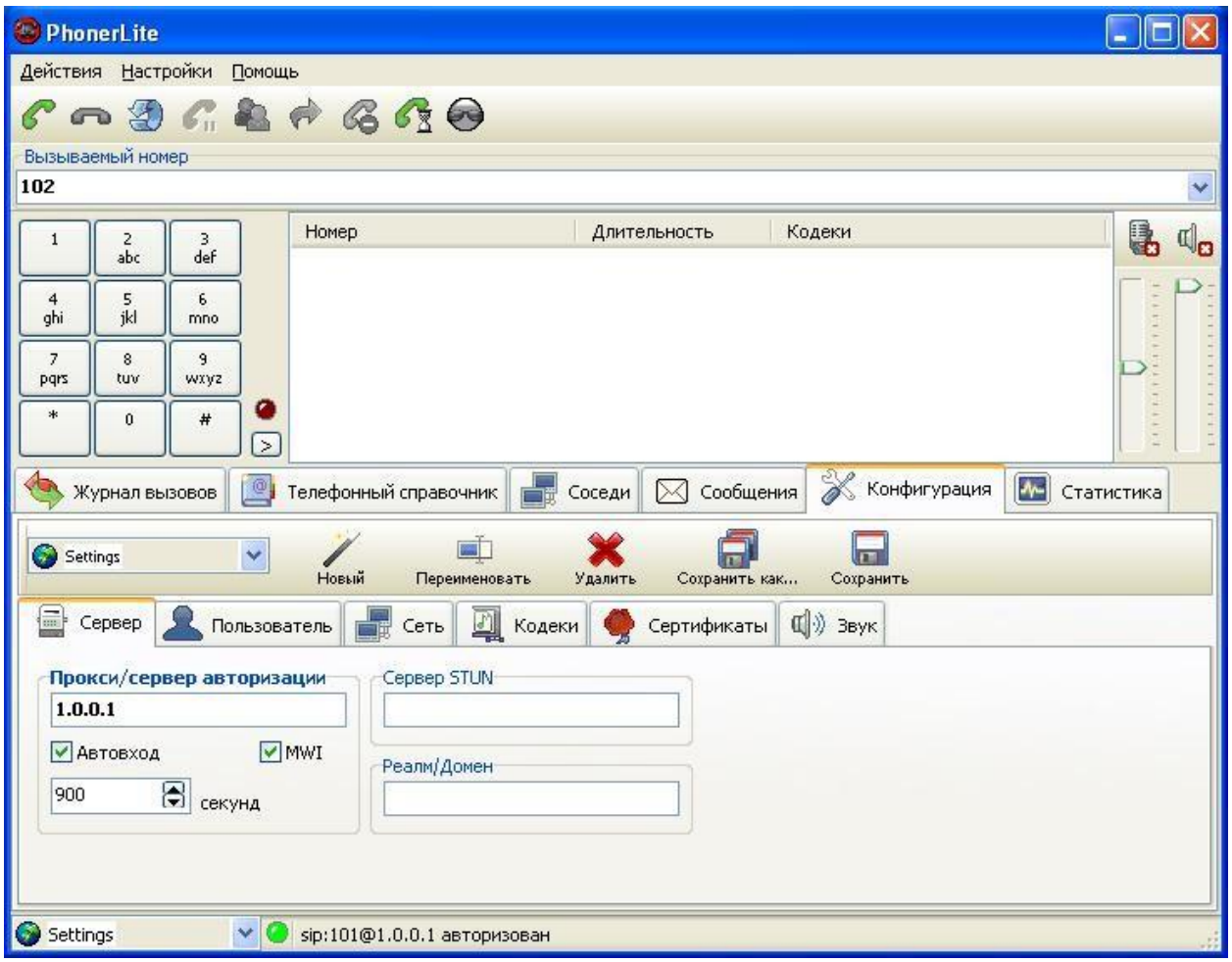


Рисунок 3.2.8 – Окно программы PhonerLite

Во вкладке Пользователь впишем Имя пользователя (логин) [101], Пароль [password]. Далее не обязательно: Отображаемое имя (ник) [PhonerLite] и Имя для авторизации [101].

После этого, зайдем в Asterisk и проверим наличие зарегистрированных пользователей (пиров) командой:

sip show peers

Как видно из Рисунка 3.2.9 оба абонента зарегистрированы и сейчас в сети (online)

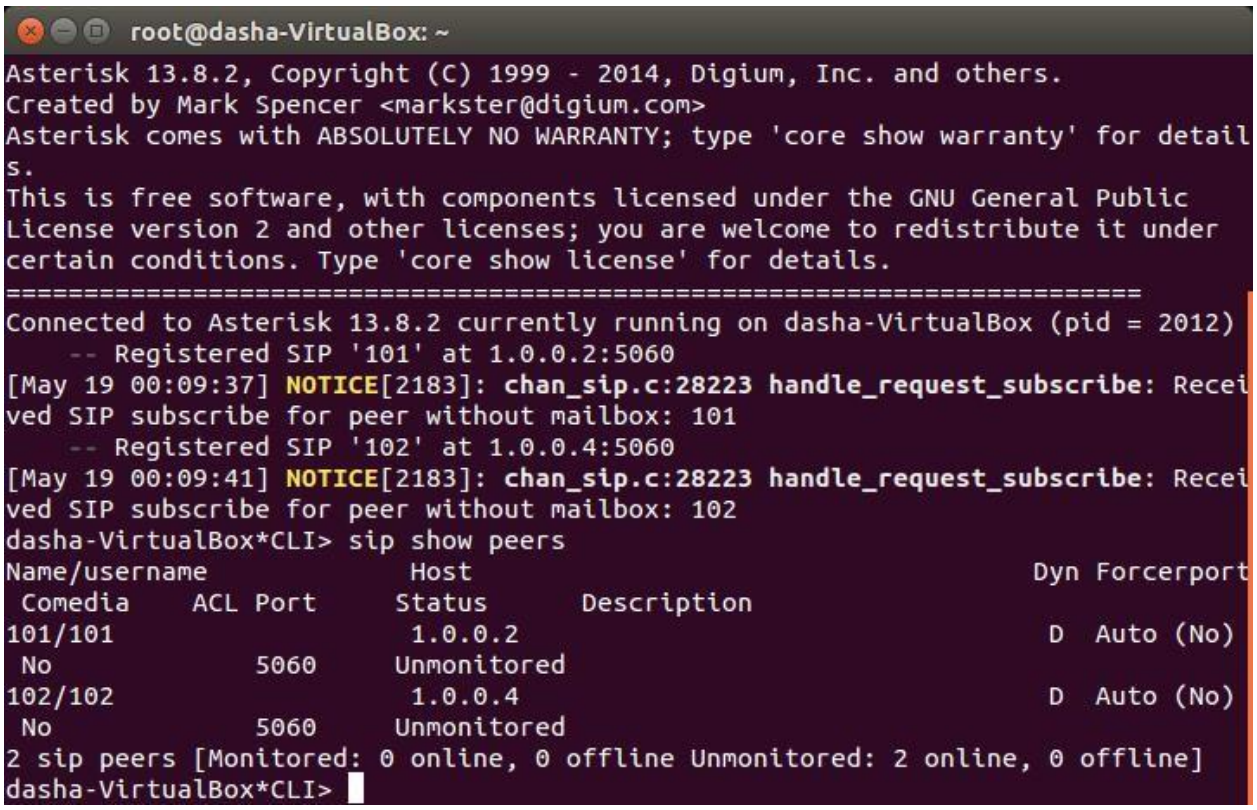


Рисунок 3.2.9 – Окно Asterisk с зарегистрированными пользователями

Далее произведем вызов от одного абонента к другому. Как видно из Рисунка 3.2.10 вызов был произведен успешно.

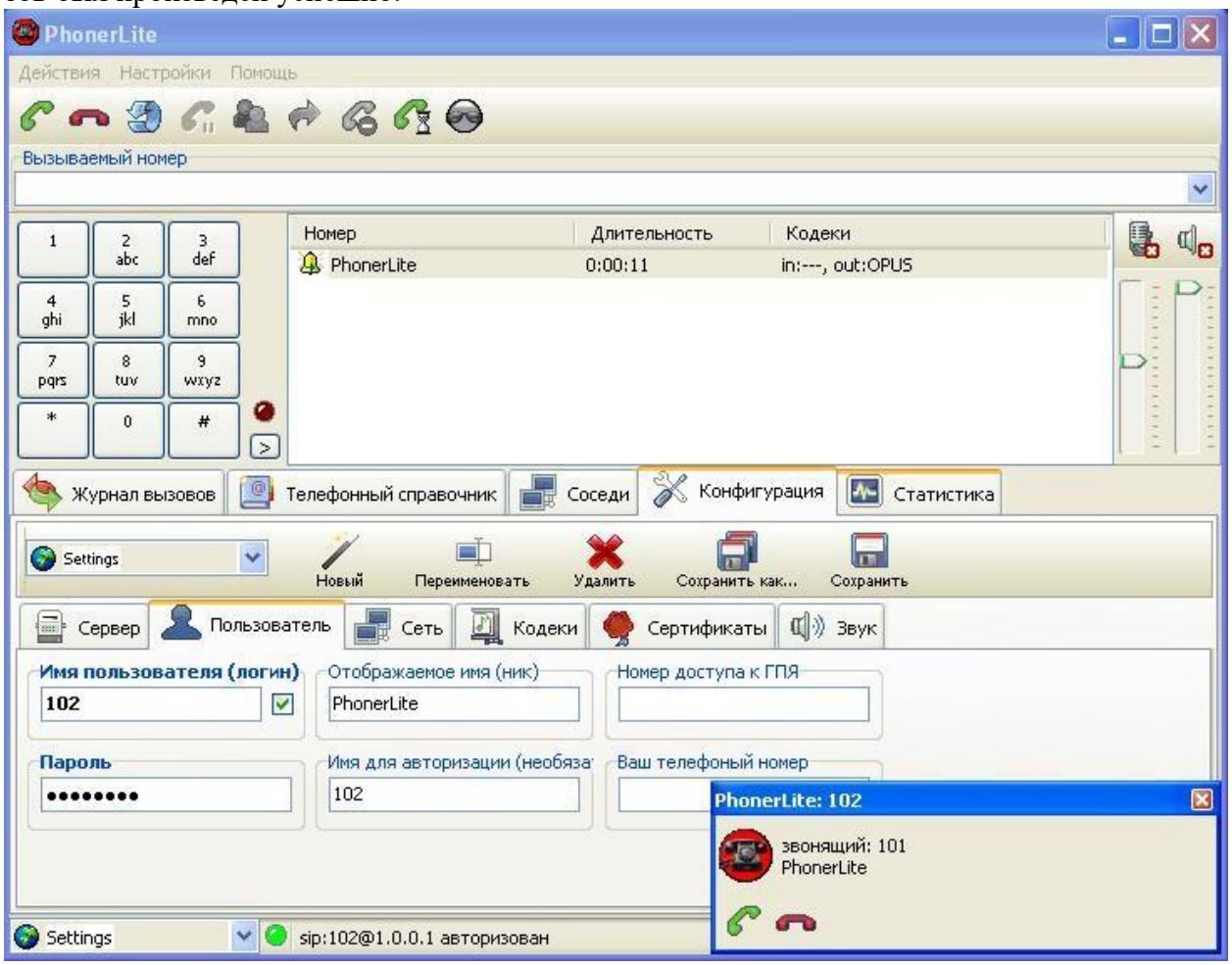


Рисунок 3.2.10 – Окно PhonerLite с входящим вызовом

Контрольное тестирование к лабораторной работе №2.
В каком файле нужно редактировать диалплан?
/etc/asterisk/dialplan.conf;
/etc/dialplan.conf; /etc/asterisk/extensions.conf; /etc/extensions.conf.
Что делает команда sip reload?
Перегружает модуль sip канала и применяет изменения из файла sip.conf;
Переподключает активных sip клиентов;
Презапускает астериск; Нет такой команды.
Что показывает команда sip show peers?
Существующие каналы;
Существующие SIP клиенты и их статус;
Существующие SIP сообщения; Существующие диалпланы.
Какие из перечисленных настроек для параметра host верны?
dynamic;
pbx.domain.ru;
192.168.0.101; 192.168.0.256.
Для чего предназначен протокол SDP?
Для описания передачи потоковых данных;
Для передачи трафика в реальном времени;
Для описания способа установления и завершения сеанса; Для шифрования данных.
Протокол SIP отвечает за:
Передачу звуковой сигнализации;
Обнаружение абонентов в сети;
Установление соединения между абонентами; Передачу голоса по соединению.
По какому порту работает SIP?
6050:UDP;
5060:UDP;
5060:TCP;
36600-39999:UDP.
Диалплан - это
Набор правил, описывающий алгоритмы обработки звонков;
Привязка - "абонент" - "аппарат"; Схема обработки входящих вызовов; Не существующее слово.
Применение настроек диалплана происходит командой
dialplan restart;
dialplan reload;
service dialplan restart; dialplan renew.
С чего начинается описание конфигурационного файла extensions.conf (синтаксис):
exten => ;
extension => ;
exten ;
exten = .

2.24. Практическая работа № 24
Настройка шлюза

Этапы:
Внутристанционное соединение;
Изменение конфигурационных файлов для АТС1 (sip.conf, extensions.conf);

Изменение конфигурационных файлов для АТС2 (sip.conf, extensions.conf);
Проверка работоспособности сети.

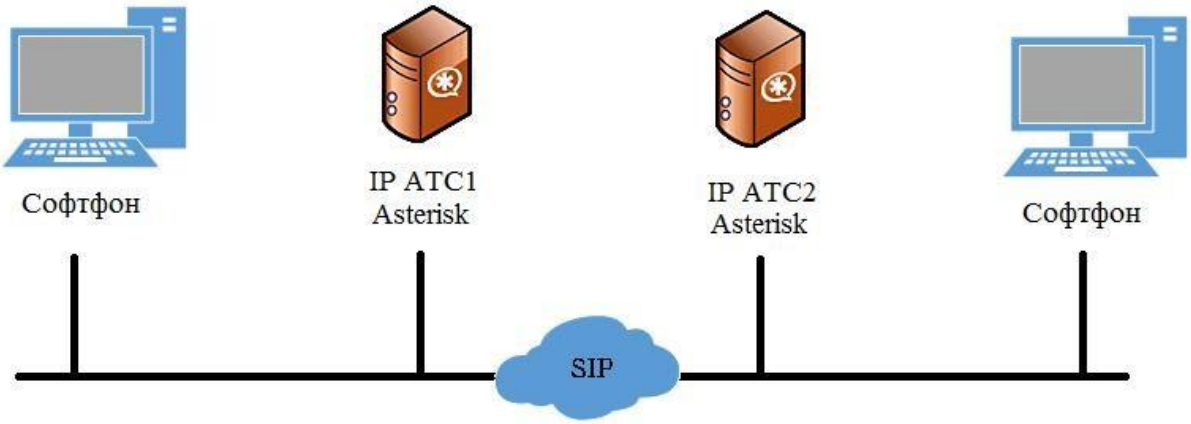


Рисунок 3.3.1 – Схематичное построение сети к лабораторной работе №3

Данная лабораторная работа будет производиться в виртуальной машине Oracle VM VirtualBox на двух операционных системах: Linux Ubuntu 14.04 LTS и Windows XP. Для их корректной работы следует создать внутреннюю сеть, как в лабораторной работе №2 пункт 1.

После этого приступим к изменению конфигурационных файлов начиная с АТС 1 и в нем файла sip.conf. Перейдем в директорию нахождения файла и командой vim откроем его для редактирования.

cd /etc/asterisk/ vim sip.conf

Редактировать файл следует так же, как показано на рисунке 3.3.2.

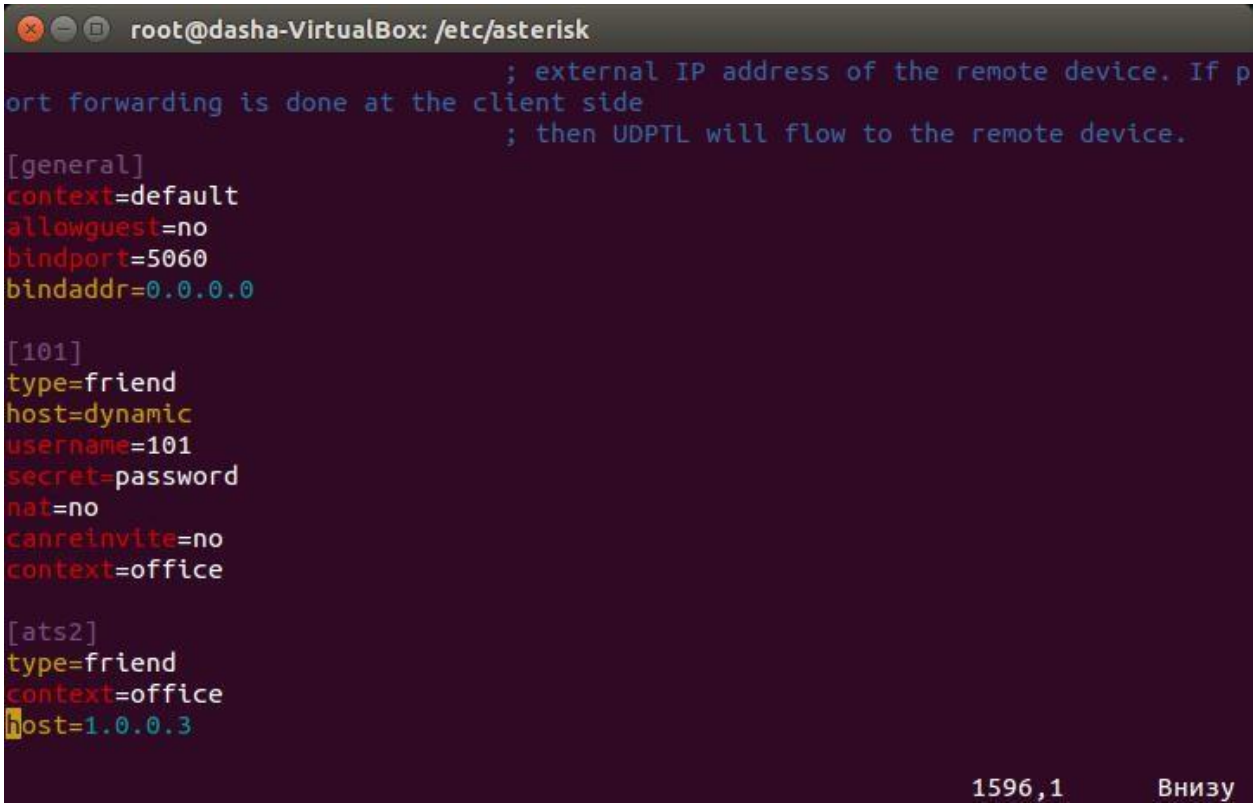


Рисунок 3.3.2 – Окно файла sip.conf с измененными параметрами для АТС1

[general] context=default allowguest=no bindport=5060 bindaddr=0.0.0.0
[101] type=friend host=dynamic username=101 secret=password nat=no canreinvite=no context=office [ats2] type=friend context=office host=1.0.0.3

Здесь использовались такие новые команды, как allowguest, bindport, bindaddr, nat и canreinvite. Рассмотрим их более подробно:
allowguest – команда, отвечающая за гостевые вызовы. Возможны только два варианта yes и no.
bindport – команда, отвечающая за используемый порт в Asterisk. Клиенты SIP традиционно используют порт 5060 TCP и UDP для соединения серверов и других элементов SIP.
bindaddr – команда, устанавливающая адрес для прослушивания. Значение по умолчанию для прослушивания всех адресов (0.0.0.0).
nat – команда для определения клиентов в качестве глобальной настройки. По умолчанию можно использовать варианты yes, no. Значение yes , заставляет сервер Asterisk игнорировать информацию об адресах, содержащуюся в полях SIP. Значение no подразумевает отсутствие поддержки rfc3581 (стандарт о симметричном установлении маршрута)
canreinvite – это параметр для клиентов, которые описаны в файле конфигурации sip.conf, используется для информирования сервера Asterisk. Значение no блокирует отправку сообщений о поступающем медиатрафике, когда соединение уже установлено.
После успешного редактирования файла sip.conf следует сохранить файл и выйти из него, а затем начать редактировать следующий конфигурационный файл extensions.conf.
cd /etc/asterisk/ vim extensions.conf
Редактирование должно быть произведено также, как на рисунке 3.3.3.

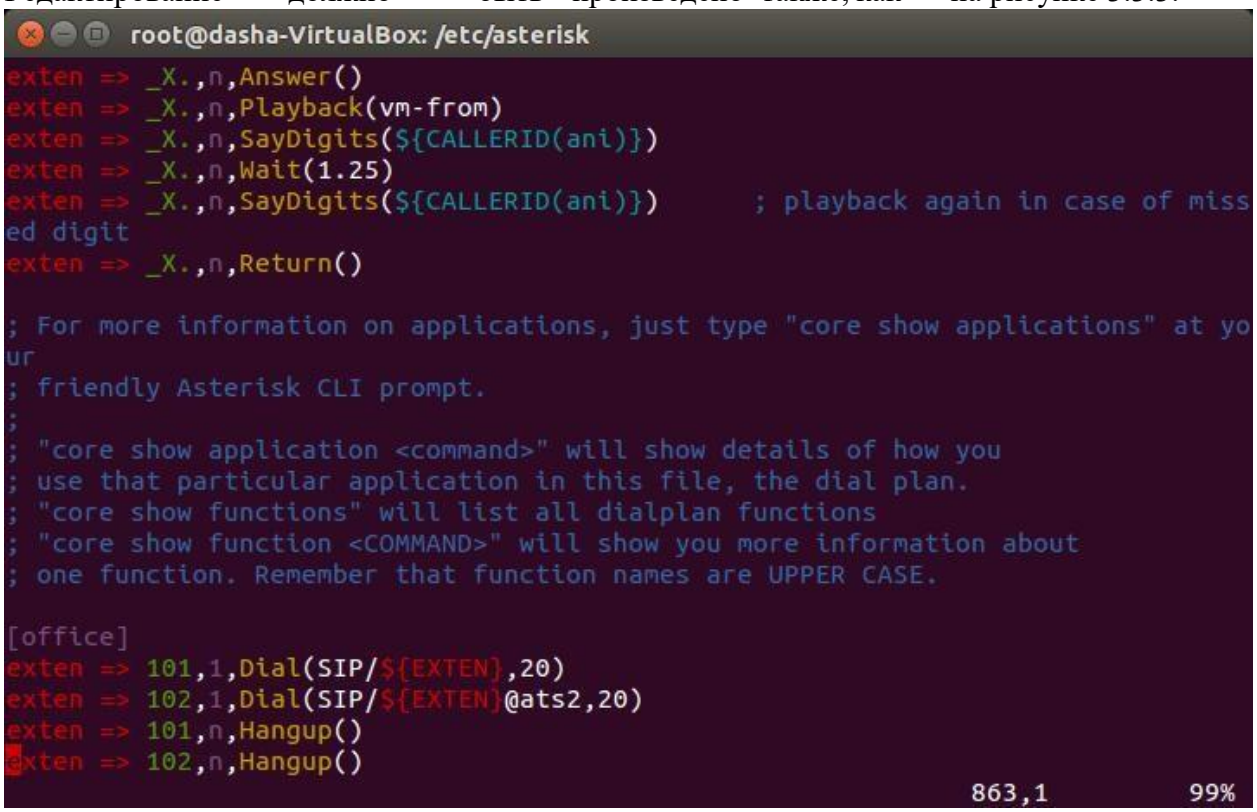


Рисунок 3.3.3 – Окно редактирования файла extensions.conf для АТС 1

[office]
exten => 101,1,Dial(SIP/${EXTEN},20) exten => 102,1,Dial(SIP/${EXTEN}@ats2,20) exten => 101,n,Hangup() exten => 102,n,Hangup()
Команда Dial(SIP/${EXTEN},20) означает, что вызов будет производиться по SIP каналу и прекратится через 20 секунд.
Команда Dial(SIP/${EXTEN}@ats2,20) означает, что вызов будет производиться по SIP каналу через ats2 транк
(это виртуальный канал между IP АТС клиента и IP АТС

оператора, работающий по IP технологии) и завершится через 20 секунд.
Команда Hangup() означает, что вызовы на любые запрашиваемые каналы прекращаются, кроме 101 и 102.
Завершив редактирование файла extensions.conf нужно его сохранить и выйти из директории asterisk, а затем войти в cli Asterisk для перезапуска всех измененных ранее конфигураций.
cd rasterisk reload
3) Произведем все те же изменения файлов, как для АТС1, только для АТС2, и с небольшой разницей в синтаксисе.
Изменение файла sip.conf (Рисунок 3.3.4)
cd /etc/asterisk/ vim sip.conf

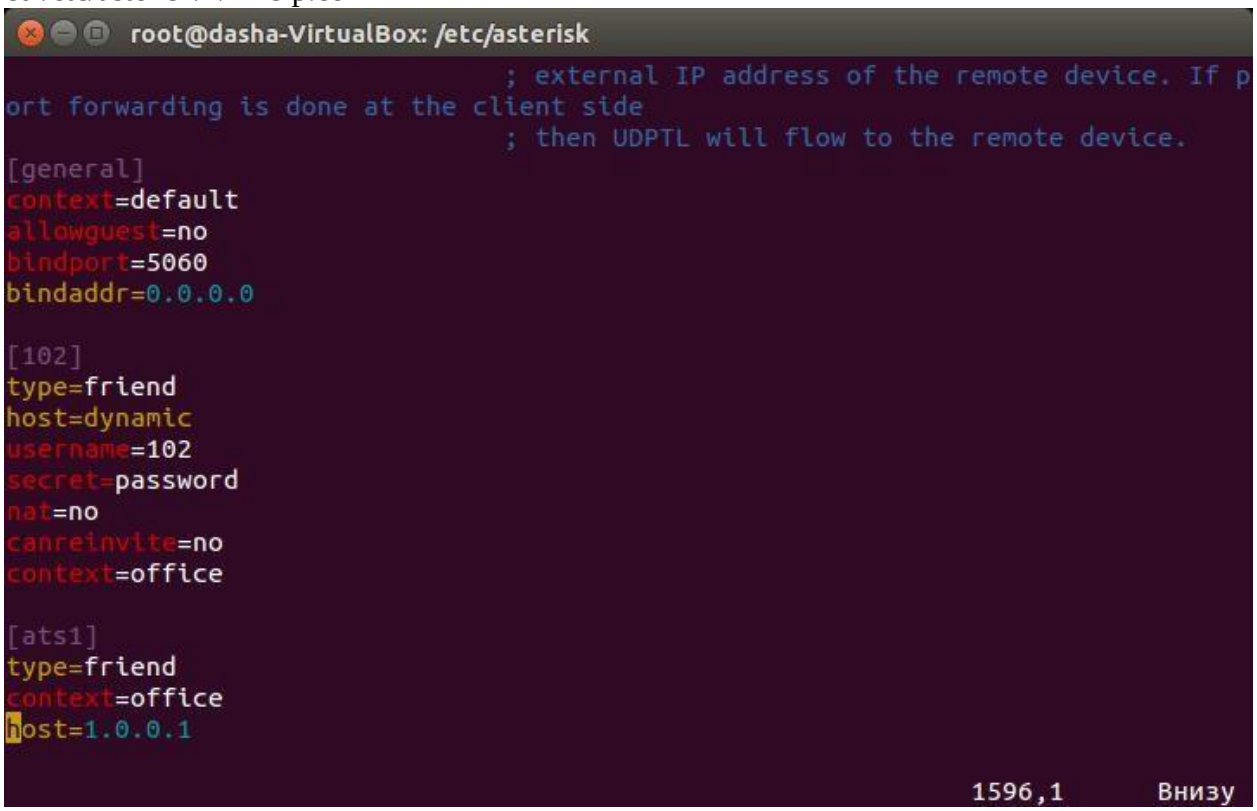


Рисунок 3.3.4 – Окно файла sip.conf с измененными параметрами для АТС2

[general] context=default allowguest=no bindport=5060 bindaddr=0.0.0.0 [102] type=friend host=dynamic username=102 secret=password nat=no canreinvite=no context=office [ats1] type=friend context=office host=1.0.0.1
Изменение файла extensions.conf. (Рисунок 3.3.5)

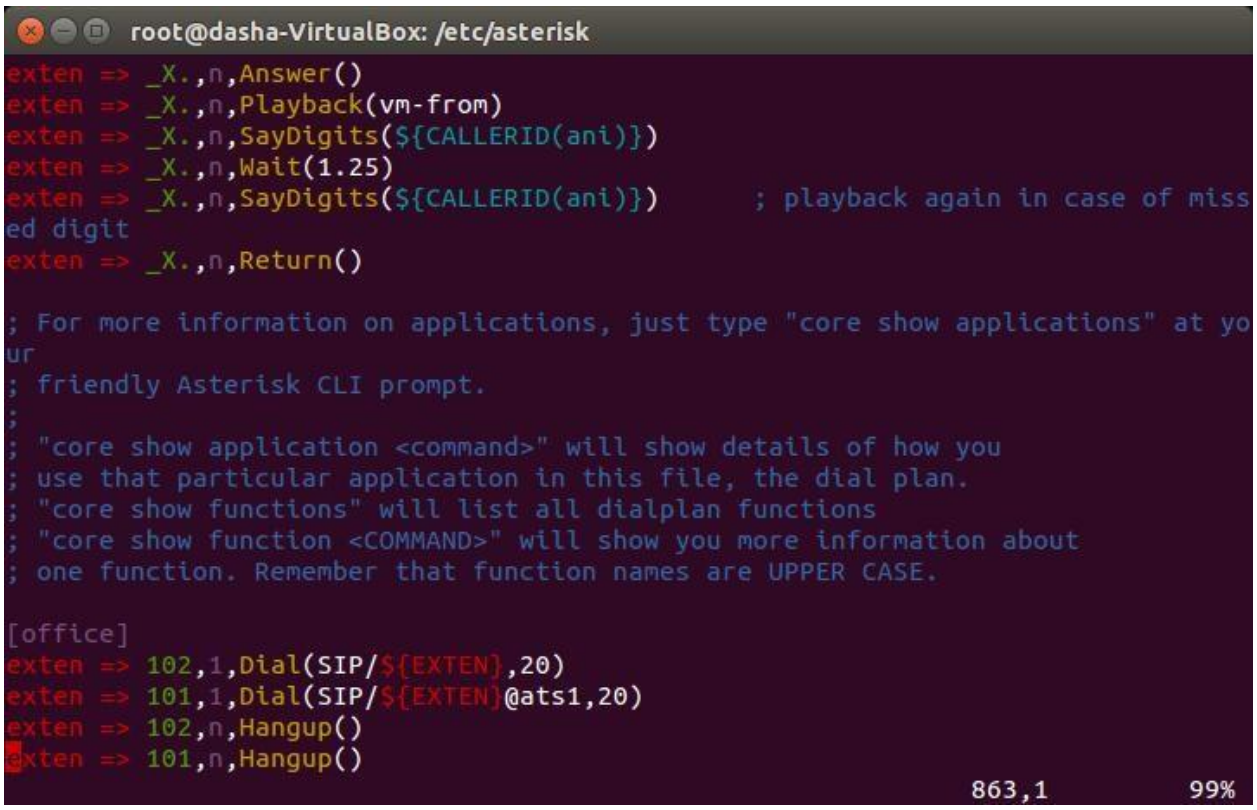


Рисунок 3.3.5 – Окно редактирования файла extensions.conf для АТС 2

[office]

exten => 102,1,Dial(SIP/${EXTEN},20) exten => 101,1,Dial(SIP/${EXTEN}@ats1,20) exten => 102,n,Hangup() exten => 101,n,Hangup()

Перезапуск всех измененных ранее конфигураций.

cd rasterisk reload

4) Произведем проверку звонком от одного абонента другому с помощью программы PhonerLite. Запускаем и настраиваем: впишем IP адрес Asterisk в раздел Прокси/сервер авторизации (Рисунок 3.3.6).

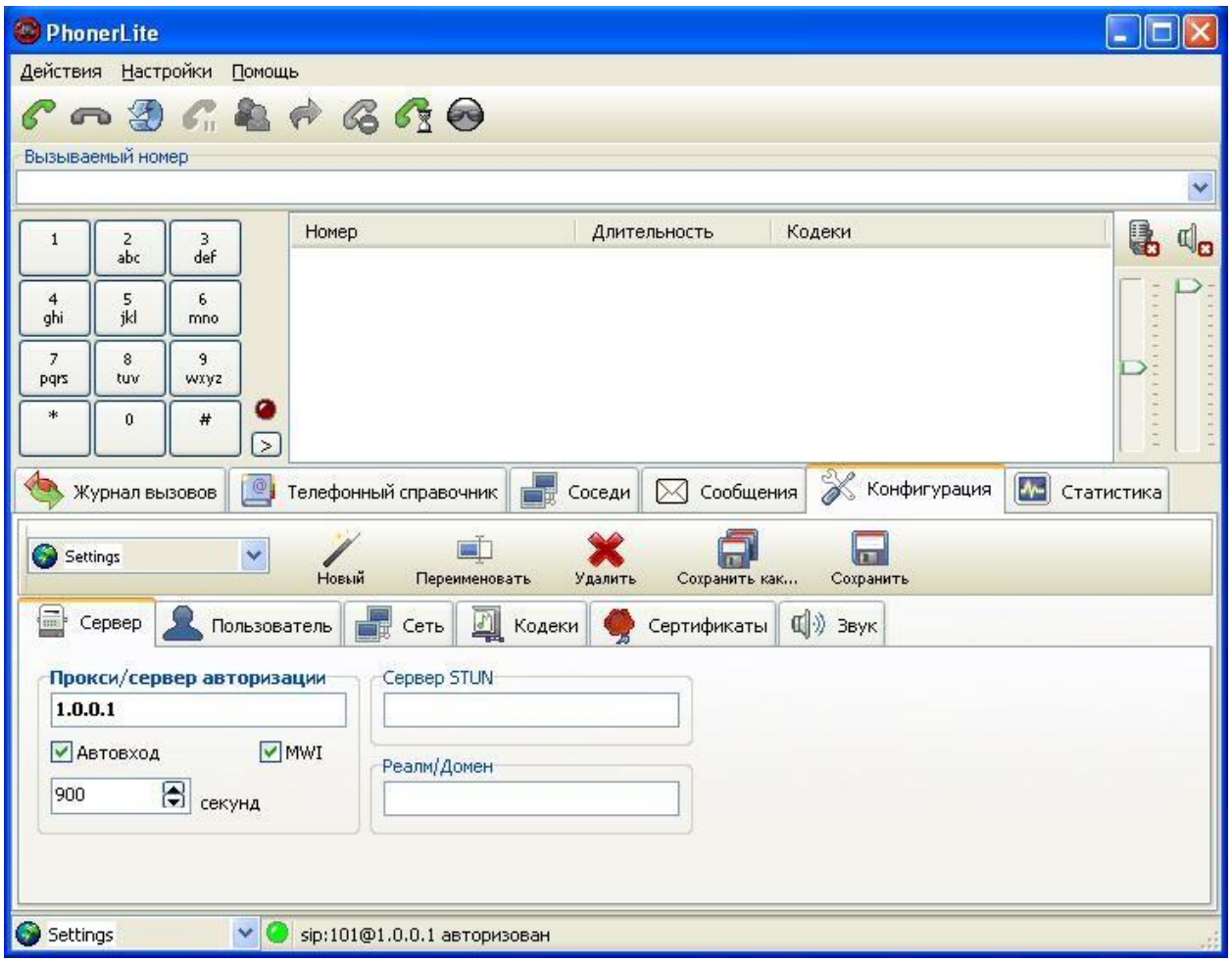


Рисунок 3.3.6 – Окно программы PhonerLite для АТС1 Осуществим вызов от одного абонента к другому.

Как видно из Рисунка 3.3.7 вызов прошел успешно.

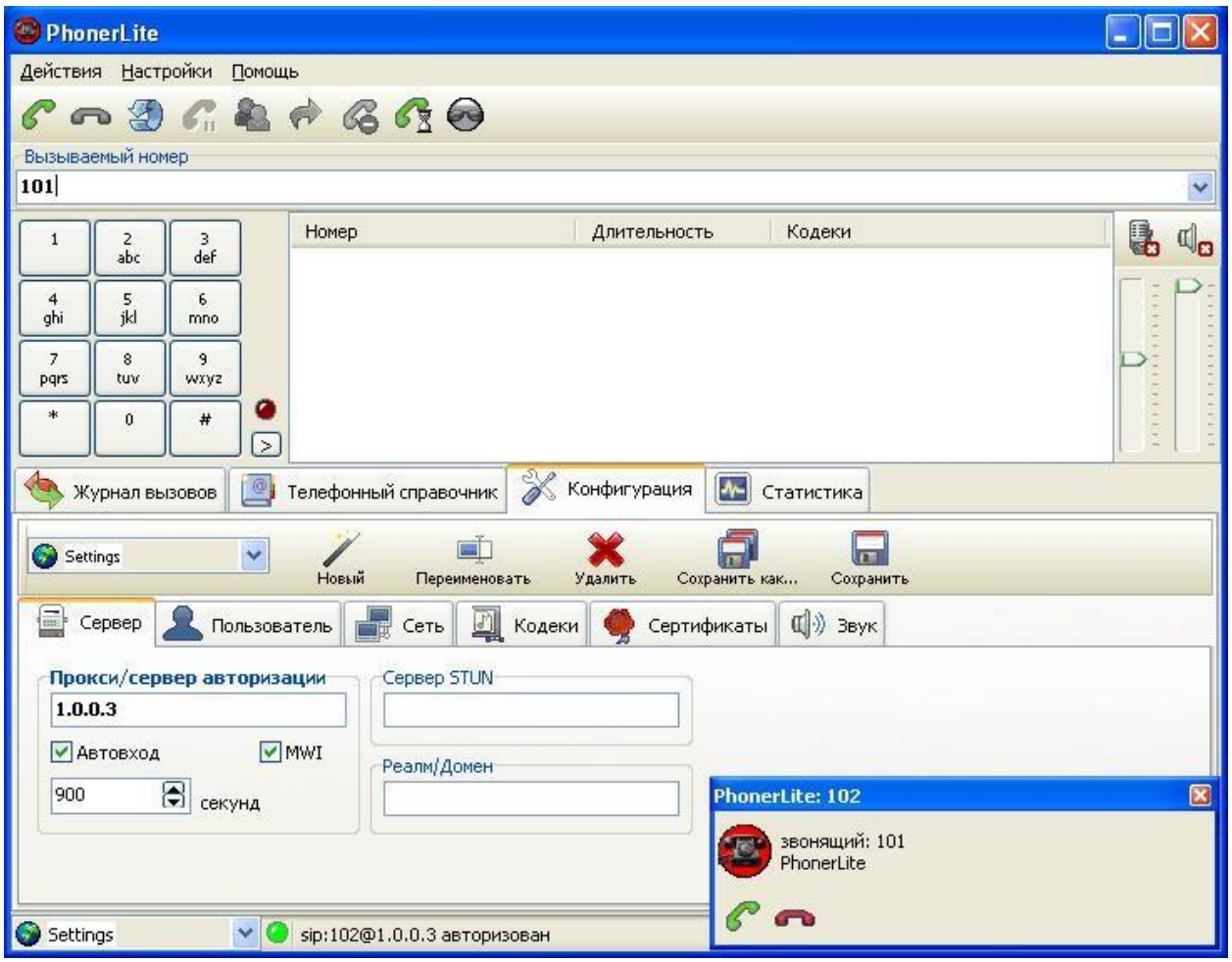


Рисунок 3.3.7 – Окно программы PhonerLite для АТС2 с входящим вызовом

Список контрольных вопросов по лабораторной работе №3.

Что лежит в основе технологии IP-телефонии?

Перечислите ее основные элементы.

Поясните архитектуру сети на базе протокола SIP.

Перечислите достоинства и недостатки протоколов H.323 и SIP. Какой из них наиболее перспективен? Почему?

Изобразите сценарий установления соединения по протоколу SIP.

Что такое офисная IP АТС? Приведите особенности таких АТС.

Расскажите о программной АТС Asterisk.

Какие виды сетей можно построить на осове АТС
Asterisk?

Расскажите о файлах конфигурации АТС Asterisk.

Расскажите о приложениях диалплана, используемых в работе.

С помощью каких команд можно настроить подключение абонента в файле sip.conf?

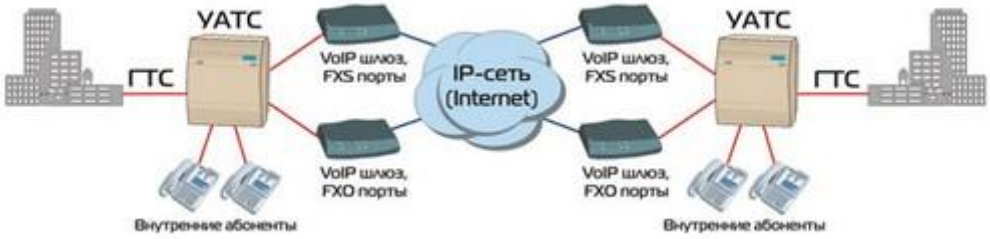
2.25. Практическая работа № 25
Установка, подключение и первоначальные настройки голосового маршрутизатора

Подключение и настройка VoIP/SIP шлюзов для связи с филиалами

Рассмотрим подключение удаленных филиалов компании с помощью VoIP/SIP шлюзов производства компании AddPac. Схема подключения выглядит следующим образом:

Как мы видим из этой схемы, полностью исключается ТфОП, как звено для связи между филиалами. К тому же появляется возможность выходить на городскую телефонную

сеть (ГТС) удаленного офиса, минуя каналы ТфОП. Например, звонить из Екатеринбурга по Москве теперь можно бесплатно через московский офис.
Далее рассмотрим простой пример подключения аналоговых телефонов через VoIP/SIP шлюз AddPac AP1100.



Для этого нам понадобятся: шлюз AddPac AP1100C (8 портов FXO, для подключения к УАТС) и шлюз AddPac AP1100B (8 портов FXS, для подключения аналоговых телефонов).
Настройку VoIP/SIP шлюзов целесообразно производить из консоли. Для подключения через консольный кабель удобно воспользоваться бесплатным программным обеспечением Putty (скачать программу Putty можно тут по адресу: chiark.greenend.org.uk)
Настройка VoIP шлюза (SIP шлюза) со стороны УАТС
Начинаем с настройки VoIP/SIP шлюза AddPac AP1100C со стороны УАТС. Для начала зададим IP-адрес шлюзу и пропишем маршрут (Route) по умолчанию:
Router# configure terminal
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip address 192.168.0.179 255.255.255.0
Router(config-if)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.1
Теперь сконфигурируем FXO порты. Включаем определитель номера:
Router(config)# voice-port 0/0
Router(config-voice-port-0/0)# caller-id enable
Router(config-voice-port-0/0)# exit
Router(config)# voice-port 0/1
Router(config-voice-port-0/1)# caller-id enable
Router(config-voice-port-0/1)# exit
Прописываем на портах горячую линию (connection plar), что бы вызов сразу отправлялся по указанному номеру и таймаут определения звонка
Router(config)# voice-port 0/0
Router(config-voice-port-0/0)#connection plar 101
Router(config-voice-port-0/0)# ring detect-timeout 50
Router(config-voice-port-0/0)#exit
Router(config)# voice-port 0/1
Router(config-voice-port-0/1)# connection plar 102
Router(config-voice-port-0/0)# ring detect-timeout 50
Router(config-voice-port-0/0)#exit
Создаем маршруты для входящих звонков для аналоговых портов FXO
Router(config)# dial-peer voice 101 pots
Router(config-dialpeer-pots-101)# destination-pattern 1101
Router(config-dialpeer-pots-101)#port 0/0
Router(config-dialpeer-pots-101)#exit
И для второго
Router(config)# dial-peer voice 102 pots
Router(config-dialpeer-pots-102)# destination-pattern 1102

Router(config-dialpeer-pots-102)#port 0/1
Router(config-dialpeer-pots-102)#exit
Мы не случайно добавили цифру «1» к номерам. С удаленной стороны тоже будет «connection plar», и чтобы вызов не заворачивался сам на себя, мы слегка изменяем номер. На физическое соединение с портом на АТС это никак не повлияет.
Теперь создадим маршрут на удаленный шлюз через VoIP
Router(config)# dial-peer voice 1000 VoIP
Router(config-dialpeer-VoIP-1000)# destination-pattern 10.F
Router(config-dialpeer-VoIP-1000)# session target 192.168.0.180
Router(config-dialpeer-VoIP-1000)# session protocol sip
Router(config-dialpeer-VoIP-1000)# dtmf-relay rtp-2833
Router(config-dialpeer-VoIP-1000)# exit
Здесь мы указали, чтобы все номера, похожие на 10X отправлялись на IP адрес 192.168.0.180 по протоколу SIP, DTMF метод RFC2833 (важный параметр).
На этом настройка первого шлюза закончена. Сохраним конфигурацию в памяти.
Router# write
Proceed with write? [confirm]
Building configuration...
[OK] Configuration saved to flash:apos.cfg
Router#

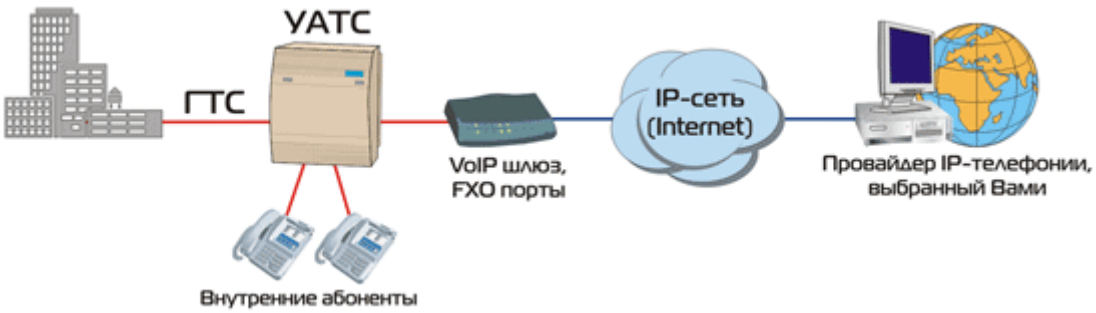
Настройка VoIP шлюза (SIP шлюзы) для подключения аналоговых телефонов
Переходим к настройке второго (удаленного) шлюза. Таким же методом, как описано выше, делаем сетевые настройки. Также настраиваем порты:
Router(config)# voice-port 1/0
Router(config-voice-port-1/0)# caller-id enable
Router(config-voice-port-1/0)#connection plar 1101
Router(config-voice-port-0/0)# exit
Router(config)# voice-port 1/1
Router(config-voice-port-1/1)# caller-id enable
Router(config-voice-port-1/1)#connection plar 1102
Создаем маршруты для входящих звонко для аналоговых портов FXS
Router(config)# dial-peer voice 101 pots
Router(config-dialpeer-pots-101)# destination-pattern 101
Router(config-dialpeer-pots-101)#port 1/0
Router(config-dialpeer-pots-101)#exit
Router(config)# dial-peer voice 102 pots
Router(config-dialpeer-pots-102)# destination-pattern 102
Router(config-dialpeer-pots-102)#port 1/1
Router(config-dialpeer-pots-102)#exit
И маршрут в сторону VoIP
Router(config)# dial-peer voice 1000 VoIP
Router(config-dialpeer-VoIP-1000)# destination-pattern 110.F
Router(config-dialpeer-VoIP-1000)# session target 192.168.0.179
Router(config-dialpeer-VoIP-1000)# session protocol sip
Router(config-dialpeer-VoIP-1000)# dtmf-relay rtp-2833
Router(config-dialpeer-VoIP-1000)# exit
Сохраняем конфигурацию:
Router# write
Proceed with write? [confirm]
Building configuration...
[OK] Configuration saved to flash:apos.cfg

Router#

На этом настройка закончена. Теперь можно проверить прохождение звонков и разнести шлюзы по удаленным сторонам. Сетевую маршрутизацию необходимо настроить так, что бы шлюзы видели друг друга по IP адресу.

Подключение и настройка VoIP шлюза (SIP шлюза) для работы с оператором IP телефонии

В настоящее время всё популярнее становятся операторы IP телефонии, предоставляющие услуги связи по протоколу SIP через сеть интернет. Уже практически все крупные операторы в дополнение к услугам IP телефонии предлагают прямой локальный входящий городской номер и организацию виртуальной АТС на своем оборудовании. В связи с этим для малых компаний, которые к тому же постоянно меняют адрес, отпадает надобность в прокладке телефонных линий по медной паре, а в случае с виртуальной АТС, в организации собственной телефонной сети. Но многие всё же оставляют свои старые аналоговые АТС и телефонные аппараты (хотя IP телефоны уже достаточно дёшевы), поскольку они стабильны и неприхотливо работают уже много лет.



Для подключения к VoIP-системам связи или оператору SIP также обычно используются VoIP/SIP шлюзы.

Рассмотрим пример подключения 2-х аналоговых телефонов через VoIP-шлюз AddPac AP1100F к популярному SIP-оператору связи SIPNET.

Для начала сетевые настройки VoIP/SIP шлюза. На этот раз дадим шлюзу получить IP адрес автоматически по DHCP:

Router# configure terminal
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip address dhcp

После того, как интерфейс LAN0 поднялся и получил IP, приступим к настройке маршрутов и аккаунта. Создадим диал-пиры для аналоговых портов

Router(config)# dial-peer voice 0 pots
Router(config-dialpeer-pots-0)#destination-pattern 0041790267 (ваш ID в SIPNET)
Router(config-dialpeer-pots-0)#port 1/0
Router(config-dialpeer-pots-0)#exit
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer-pots-1)#destination-pattern 0041790267 (ваш ID в SIPNET)
Router(config-dialpeer-pots-1)#port 1/1
Router(config-dialpeer-pots-1)#exit

Теперь диал-пир в сторону SIPNET

Router(config)# dial-peer voice 1000 VoIP
Router(config-dialpeer-VoIP-1000)# destination-pattern T
Router(config-dialpeer-VoIP-1000)# session target sip-server
Router(config-dialpeer-VoIP-1000)# session protocol sip
Router(config-dialpeer-VoIP-1000)# voice-class codec 0
Router(config-dialpeer-VoIP-1000)#exit

Добавим возможность удержания вызова (hold) и перевода звонка (transfer)

Router(config)# dial-peer call-hold h
Router(config)# dial-peer call-transfer h
Создадим класс кодеков с приоритетами
Router(config)# voice class codec 0
Router(config-vclass-codec#0)# codec preference 1 g711alaw
Router(config-vclass-codec#0)# codec preference 2 g729
Настройка sip user-agent
Router(config)# sip-ua
Router(config-sip-ua)# sip-username 0041790267 (ваш ID в SIPNET)
*Router(config-sip-ua)# sip-password ******** (ваш пароль в SIPNET)*
Router(config-sip-ua)# sip-server sipnet.ru
Router(config-sip-ua)# srv enable
Router(config-sip-ua)# register e164
Router(config-sip-ua)#exit
Сохраняем конфигурацию:
Router# write
Proceed with write? [confirm]
Building configuration...
[OK] Configuration saved to flash:apos.cfg
Router#
Подключение и настройка VoIP/SIP шлюза закончена. Теперь можно звонить с аналоговых телефонов через SIPNET. Входящие звонки из SIPNET будут приходить на порт FXS 1/0, а при его занятости на порт FXS 1/1. Также вместо телефонных аппаратов к портам FXS можно подключить линии от аналоговой мини-АТС.

2.26. Практическая работа № 26
Настройка таблицы пользователей в голосовом маршрутизаторе

Залание
Настройть таблицу пользователей в голосовом маршрутизаторе, согласно варианту выданному преподавателем.

2.27. Практическая работа № 27
Настройка групп в голосовом маршрутизаторе

Для того, чтобы настроить голосовой шлюз, нужно подключиться к интерфейсу управления устройством и выполнить несколько простых действий. Для этого необходимо сбросить настройки голосового шлюза до заводских.

1. Отключаем устройство от электросети.
2. Вооружаемся скрепкой, зажимаем и удерживаем с ее помощью кнопку ***Reset***.
3. Подключаем шлюз к электросети, продолжая удерживать кнопку ***Reset***.
4. Ждем 6 секунд, отпускаем кнопку ***Reset***.

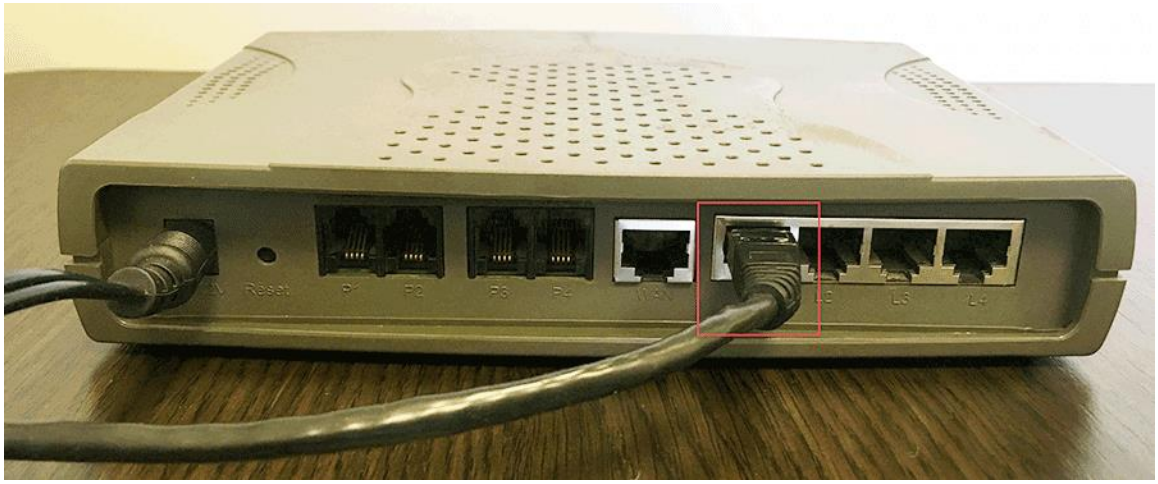
Готово!

Подключение голосового шлюза к сети Интернет

Нам нужно настроить WAN-порт шлюза на работу со статическим IP-адресом, а не с динамическим. Это позволит подключаться к интерфейсу управления шлюзом и вносить изменения в конфигурацию устройства.

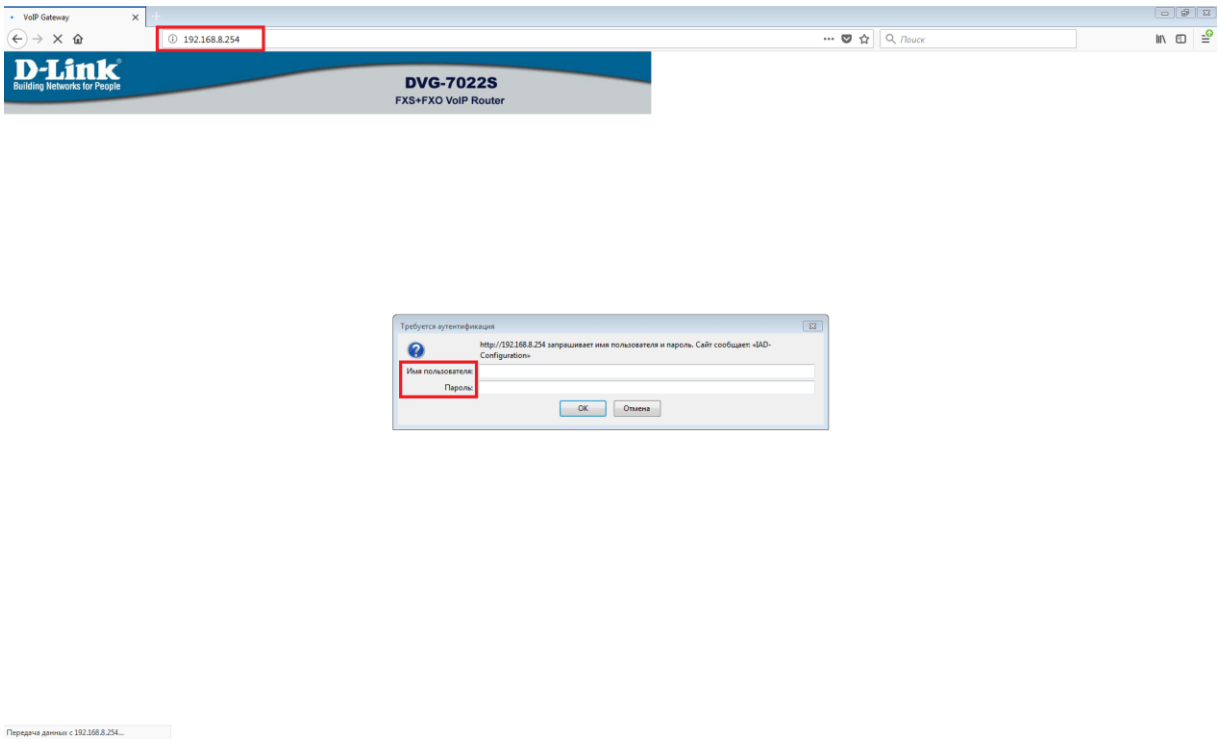
Алгоритм действий:

Подключаем патч-корд от ноутбука или компьютера к любому LAN-порту.



Подключаемся к интерфейсу управления шлюзом. Для этого в адресной строке web-браузера (Google Chrome, Firefox, Internet Explorer) набираем http://192.168.8.254/

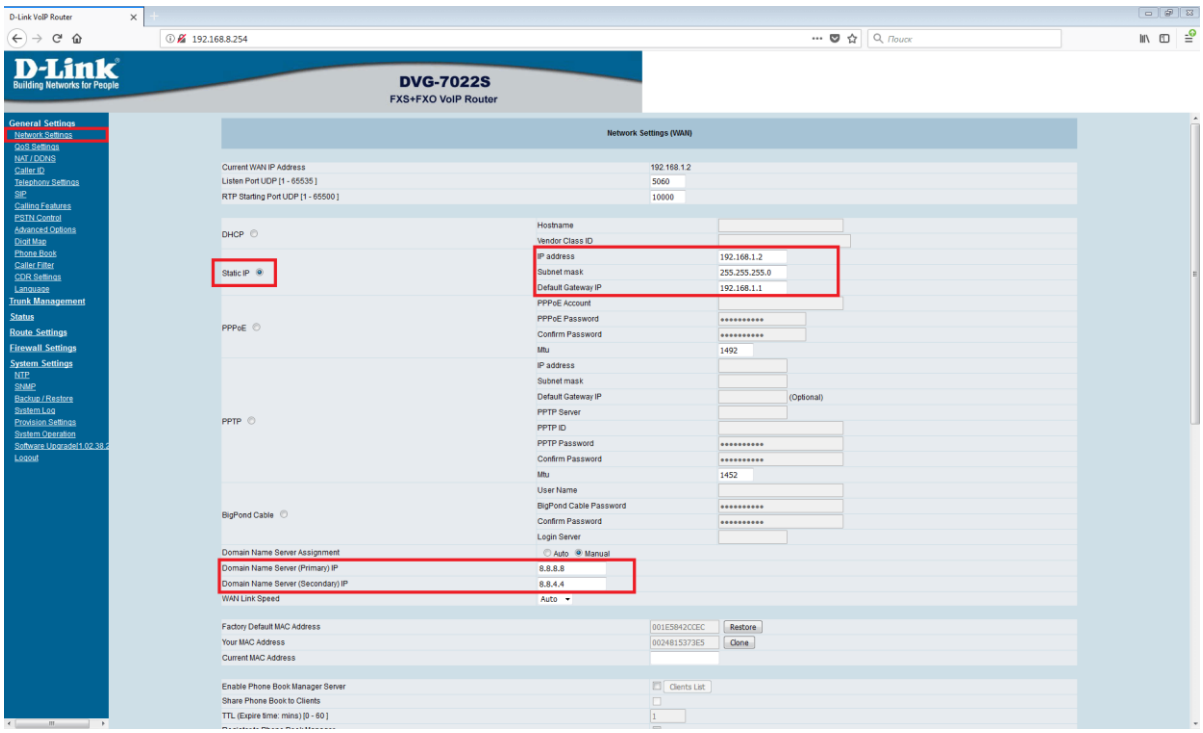
Так как ранее мы сбросили настройки шлюза до заводских, для его подключения поля **"Имя пользователя"** и **"Пароль"** при нажатии кнопки **"ОК"** нужно оставить незаполненными.



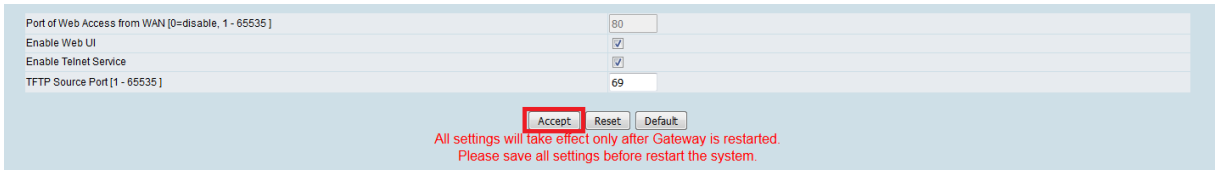
В разделе **"NetworkSettings"** задаем настройки в соответствии с адресацией локальной сети компании:

Выбираем элемент ***"StaticIP"***.
Указываем IP-адрес в поле ***"IPaddress"***. Он будет использоваться для подключения к интерфейсу управления шлюзом.
Указываем маску подсети в поле ***"SubnetMask"***. Исходное значение не придется изменять, если сетевые настройки интернет-роутера не менялись после покупки и подключения к сети Интернет.
Указываем IP-адрес шлюза по умолчанию в поле ***"DefaultGatewayIP"***. Здесь же нужно указать адрес интернет-роутера, к которому будет подключен голосовой шлюз.
Заполняем поля ***"Domain Name Server (Primary) IP"*** и ***"Domain Name Server (Secondary) IP"***. Для заполнения будем использовать IP-адреса серверов Google (8.8.8.8 и 8.8.4.4).

Никогда не подключайте голосовой шлюз к сети Интернет с публичным (внешним, белым, реальным, маршрутизируемым) IP-адресом. При таком подключении к шлюзу могут получить доступ третьи лица – мошенники, нечистоплотные конкуренты и т.д. В результате такая опрометчивость с вашей стороны может обернуться дополнительными расходами и проблемами. Очевидно, что такая публичность ни к чему хорошему не приведет. Поэтому **подключаться к Интернету с публичным IP-адресом можно только при необходимости и только в случае, если вы ответственный сотрудник понимаете, что делаете и для чего**.

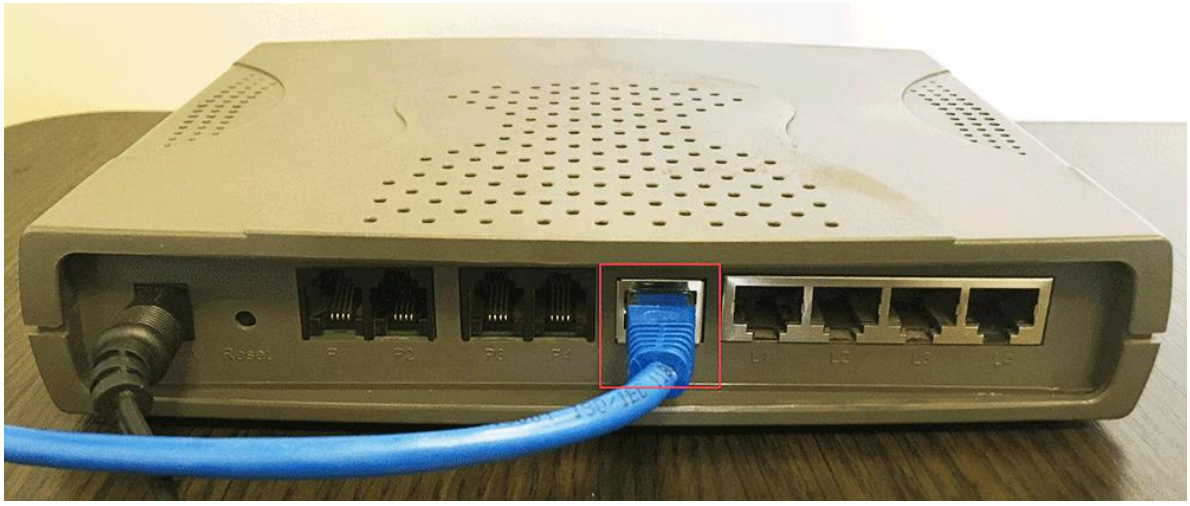


Внизу страницы нажимаем кнопку ***"Accept"*** (принять) для применения настроек.



В разделе **"SystemOperations"** выбираем опцию ***"SaveSettings"*** и нажимаем на кнопку ***"Accept"***, чтобы настройки не сбрасывались при перезагрузке, выключении и т.д.

Подключаем голосовой шлюз портом **"WAN"** к локальной сети.



Готово. Устройство подключено к сети передачи данных. Осталось только настроить порты для подключения телефонных аппаратов и телефонных линий.

 Настройка SIP и телефонных портов на голосовом шлюзе.

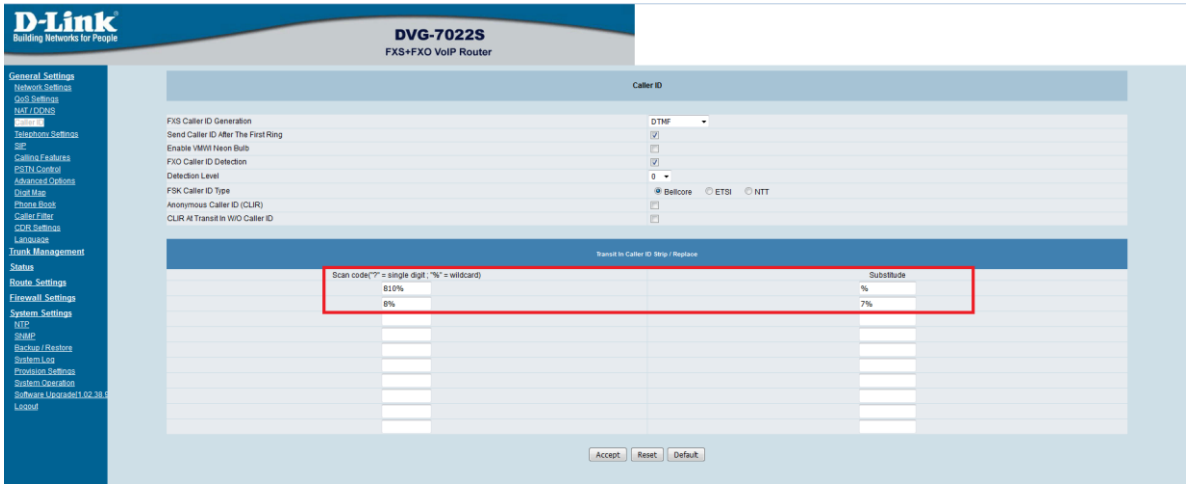
Вот мы и подошли к финальной стадии настройки голосового шлюза. Основная часть работы выполнена – осталось подключиться к интерфейсу управления устройством. Для этого будем использовать IP-адрес, который указывали при настройке порта WAN.

Настройка определения номера

Задавать нужные нам параметры будем в разделе ***"GeneralSettings"*** / ***"Caller ID"***. Чтобы номер клиента отображался на дисплее офисного телефонного аппарата и чтобы этот номер корректно передавался на Виртуальную АТС, нужно указать следующие настройки:

"FXS Caller ID Generation": DTMF;
"Send Caller ID After The First Ring": включено;
"FXOCallerIDDetection": включено.

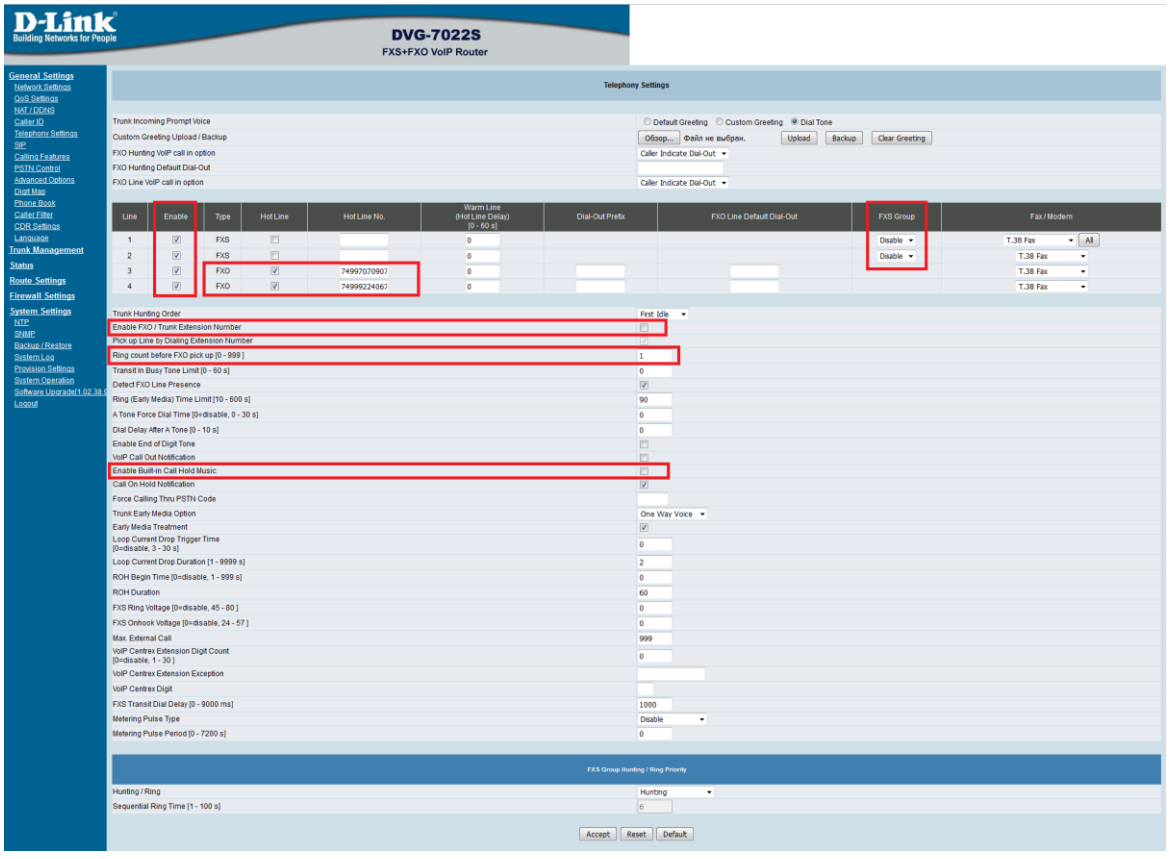
Важно: так как в городской линии номера определяются через 8-ку, перед передачей на Виртуальную АТС их нужно преобразовать в требуемый формат – префикс 810 не передавать, а префикс 8 заменить на 7.



Настройки "General Settings" / "Telephony Settings"

Для настройки портов FXS и FXO указываем следующие параметры:

"FXSGroup": Disable. Для всех портов FXS;
"HotLine": включено. Для всех портов FXO;
"HotLineNo.": городские номера, которые будут передаваться на Виртуальную АТС при звонке на действующие городские номера. Их необходимо указывать в формате E164;
"Enable FXO / Trunk Extension Number": выключено;
"Ring count before FXO pick up [0 - 999]": 1. Параметр необходим для корректного определения номера в городской телефонной линии;
"Enable Built-in Call Hold Music": выключено.



Настройки "General Settings" / "SIP"

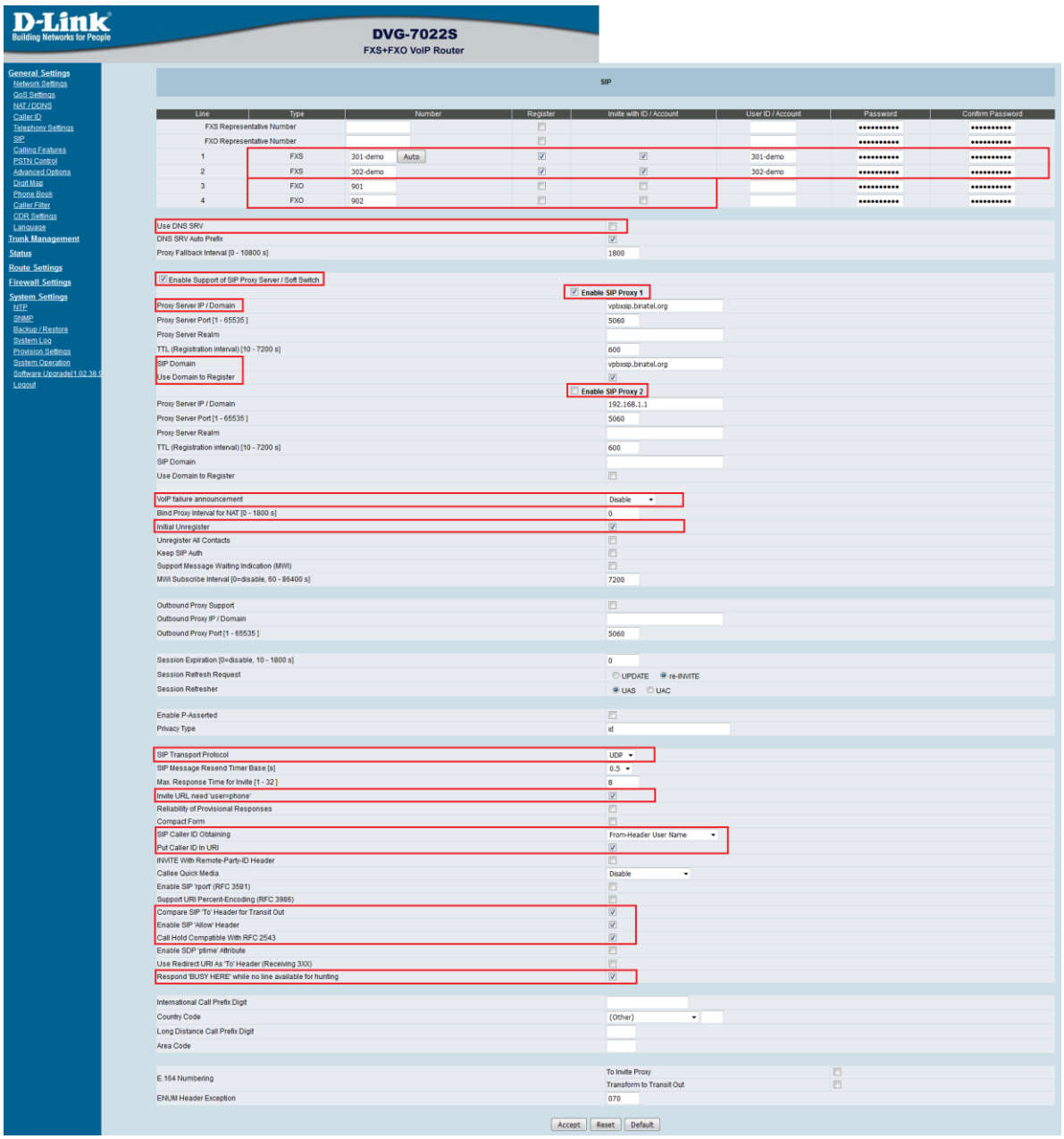
Протокол SIP используется для подключения голосового шлюза к Виртуальной АТС. Поэтому для решения стоящей перед нами задачи потребуется задать ряд настроек.

Сначала зарегистрируем порты FXS на Виртуальной АТС. Это позволит совершать и принимать вызовы на аналоговые телефонные аппараты.

Затем настроим порты FXO и укажем параметры передачи CallerID на Виртуальную АТС.

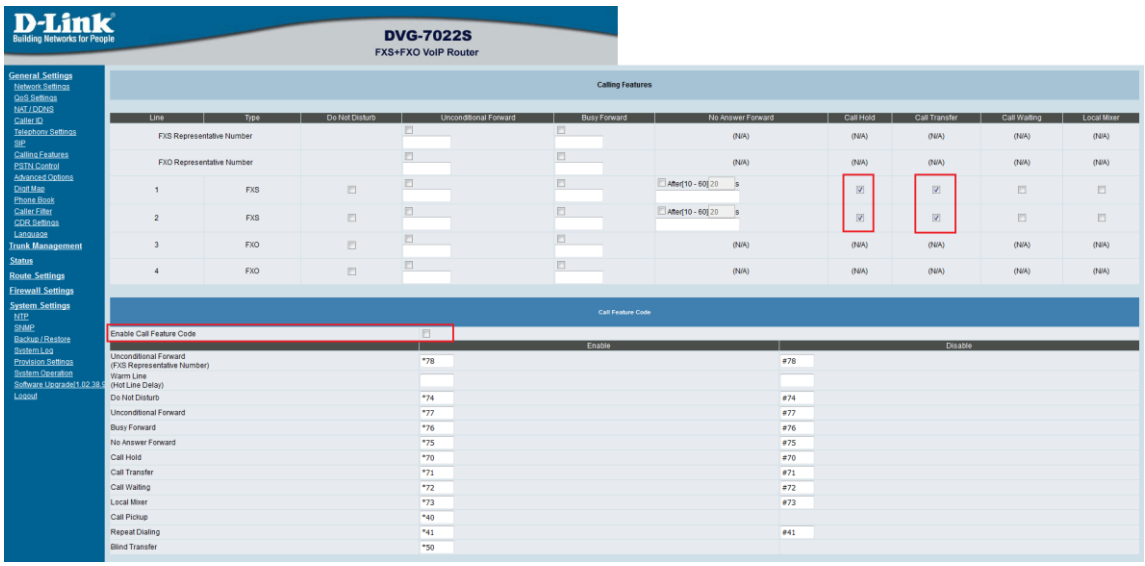
Также для корректной работы системы, помимо регистрационных данных, нужно указать следующие характеристики:

"номера для портов FXO": можно использовать те, которые не используются и не будут использоваться в будущем;
"Use DNS SRV": выключено;
"Enable Support of SIP Proxy Server / Soft Switch": включено;
"Enable SIP Proxy 1": включено;
"ProxyServerIP / Domain": SIP-сервер (vpbxsip.binatel.org) для регистрации FXS портов на Виртуальной АТС;
"SIP Domain": домен (vpbxsip.binatel.org);
"Use Domain to Register": включено;
"Enable SIP Proxy 2": выключено;
"VoIP failure announcement": disable;
"Initial Unregister": включено;
"Session Refresh Request": ReINVITE;
"SIP Transport Protocol": UDP;
"Invite URL need 'user=phone'": включено;
"SIP Caller ID Obtaining": From-Header User Name;
"Put Caller ID In URI": включено;
"Compare SIP 'To' Header for Transit Out": включено;
"Enable SIP 'Allow' Header": включено;
"Call Hold Compatible With RFC 2543": включено;
"Respond 'BUSY HERE' while no line available for hunting": включено;



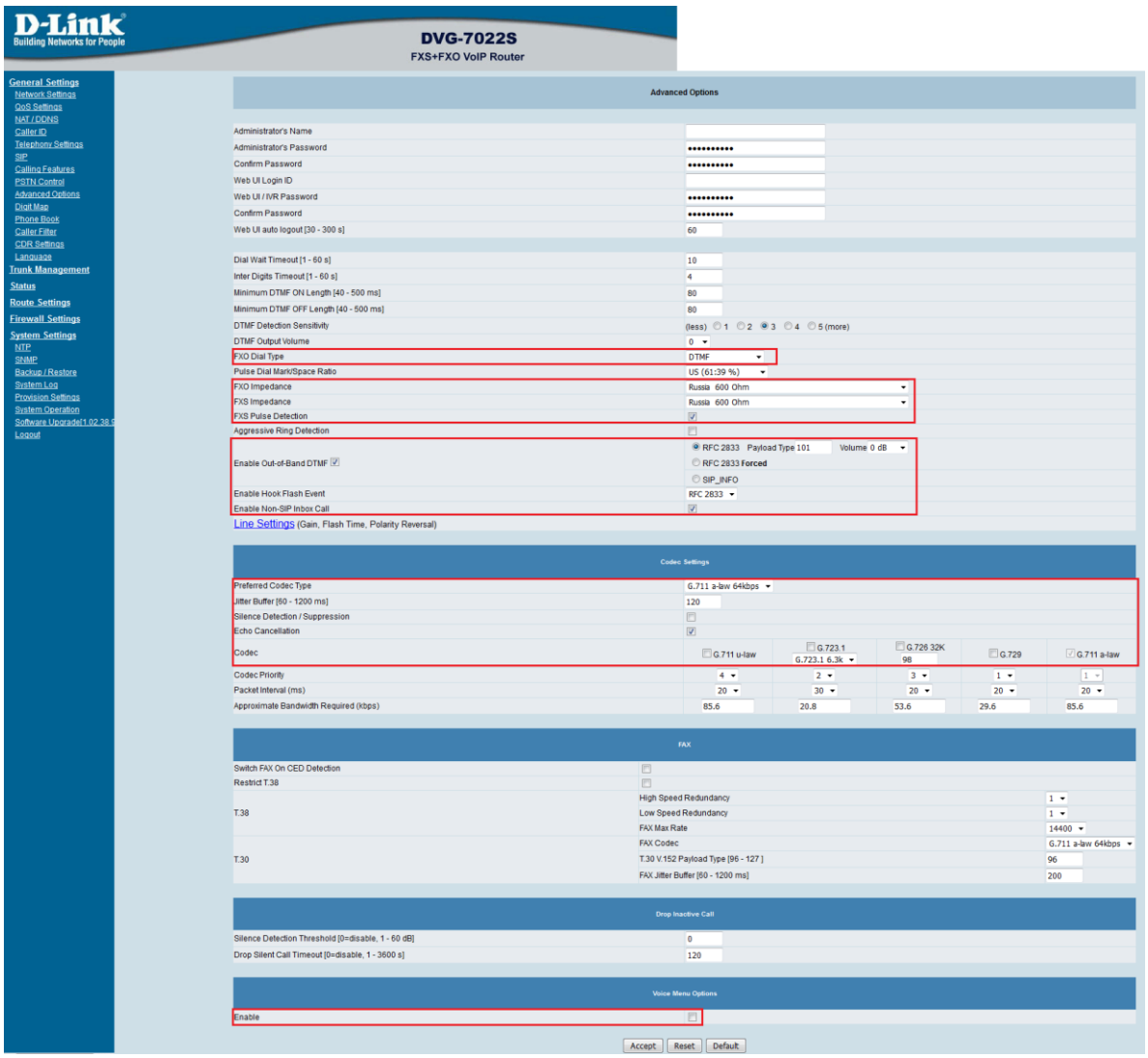
Настройки "General Settings" / "Calling Features"

"Call Hold": включено;
"Call Transfer": включено;
"Enable Call Feature Code": выключено;



Настройки "General Settings" / "Advanced Options"

"FXO Dial Type": DTMF;
"FXO Impedance": Russia 600 Ohm;
"FXS Impedance": Russia 600 Ohm;
"FXS Pulse Detection": включено;
"Enable Out-of-Band DTMF": включено, RFC2833;
"Enable Hook Flash Event": RFC2833;
"Enable Non-SIP Inbox Call": включено;
"Preferred Codec Type": G.711 a-law 64kbps;
"Silence Detection / Suppression": выключено;
"Echo Cancellation": включено;
"Voice Menu Options Enable": выключено;

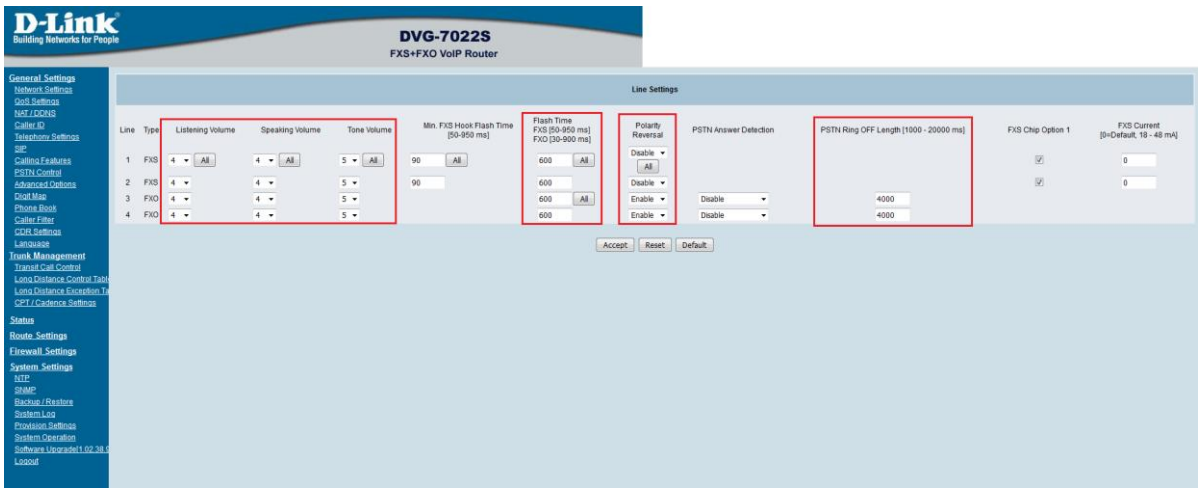


Настройки "General Settings" / "Advanced Options" / "Line Settings (Gain, Flash Time, Polarity Reversal)"

На страницу настроек линий можно перейти по ссылке, которая находится на странице **"AdvancedOptions"**.

Задаем параметры:

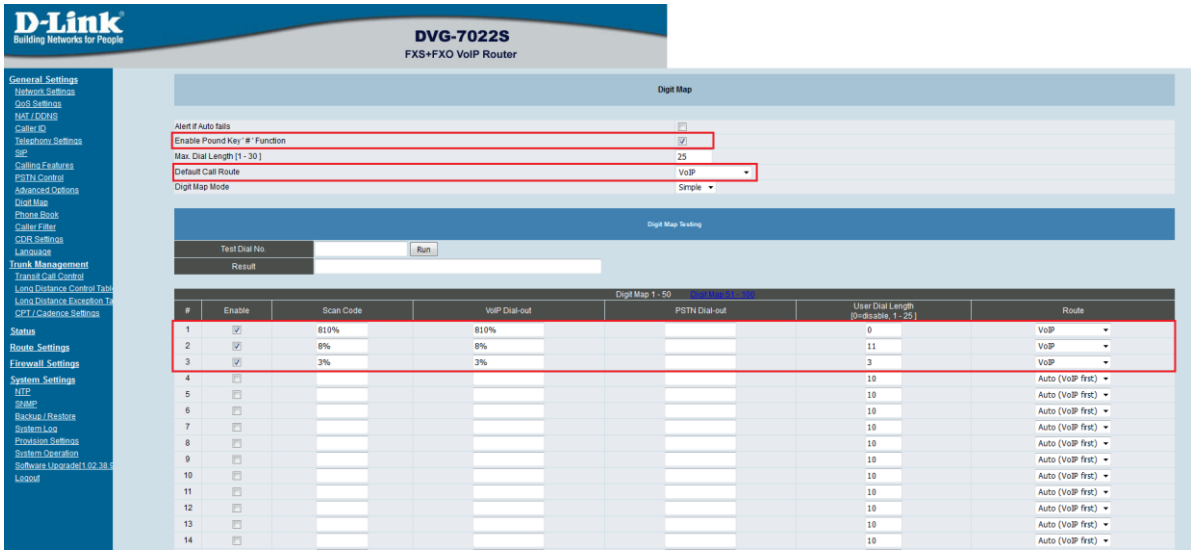
"Listening Volume": 4;
"Speaking Volume": 4;
"Tone Volume": 5;
"Flash Time": 600;
"PSTN Ring OFF Length": 4000;



Настройки "General Settings" / "Digit Map"

Теперь добавим маски для набора номеров – международных, РФ и внутренних. Так шлюз сможет определять длину номера при наборе и отправлять вызов на АТС сразу после набора последней цифры.

Если маски не использовать, то после набора номера шлюз отправит вызов на АТС только спустя 4 секунды либо после нажатия клавиши #. Такие параметры заложены в настройки по умолчанию.

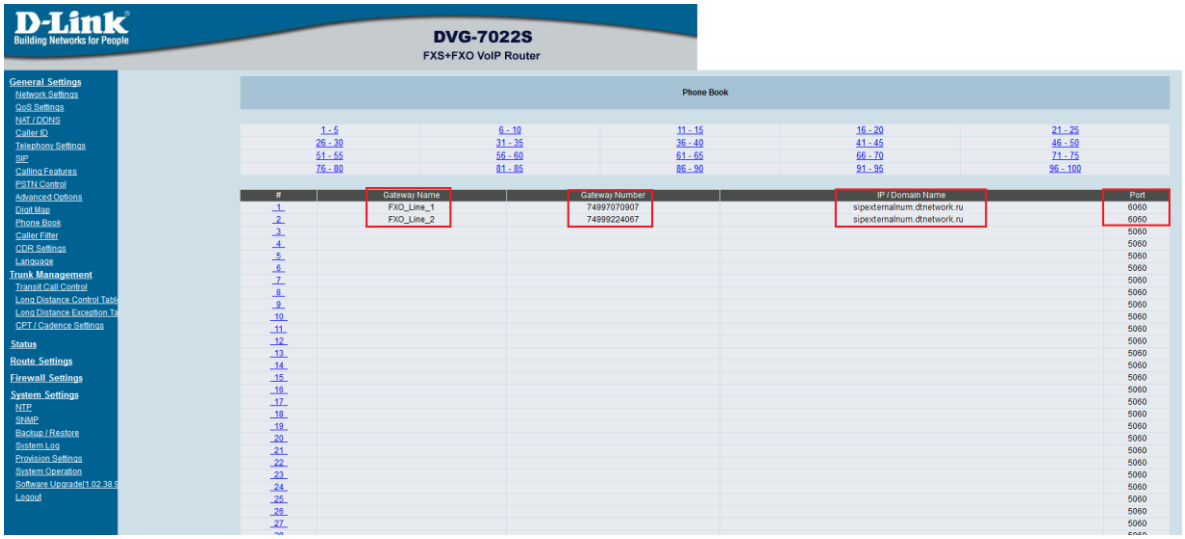


Настройки "General Settings" / "Phone Book"

Теперь направим вызовы, поступающие на городские номера, на виртуальную АТС, так они будут обрабатываться в соответствии с нашей задачей. Для этого, направим вызовы на выделенный SIP-сервер Цифра-Телеком:

"Домен": sipexternalnum.dtnetwork.ru;
"Порт": 6060;

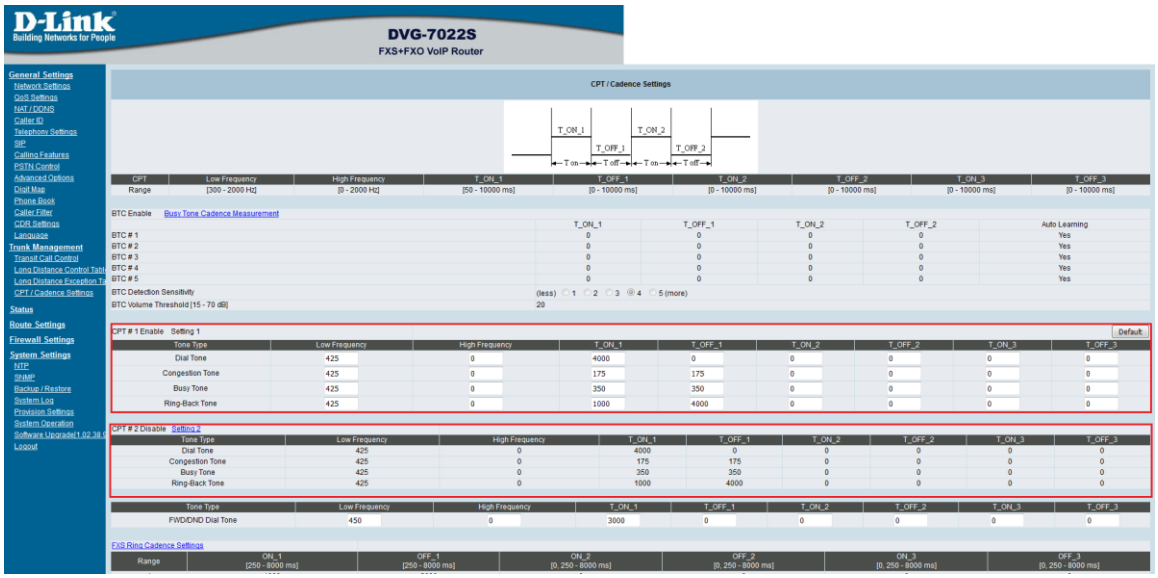
Внимание: городские номера должны быть указаны точно так же, как в настройках ***"TelephonySettings"*** для портов **FXO**.



Настройки "Trunk Management" / "CPT/Cadence Settings"

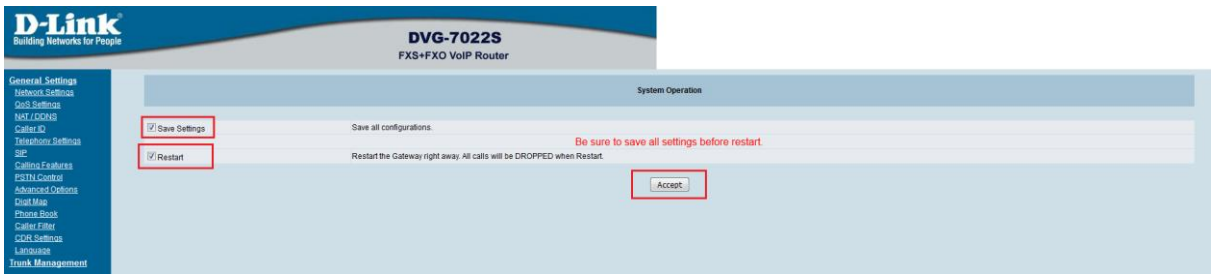
Теперь нужно задать настройки в соответствии с тонами городских линий, к которым подключается шлюз. Это поможет избежать "подвисания портов FXO" на шлюзе.

Для достижения целей, стоящих перед компанией "X", голосовой шлюз настроен для подключения к ТФоП РФ.

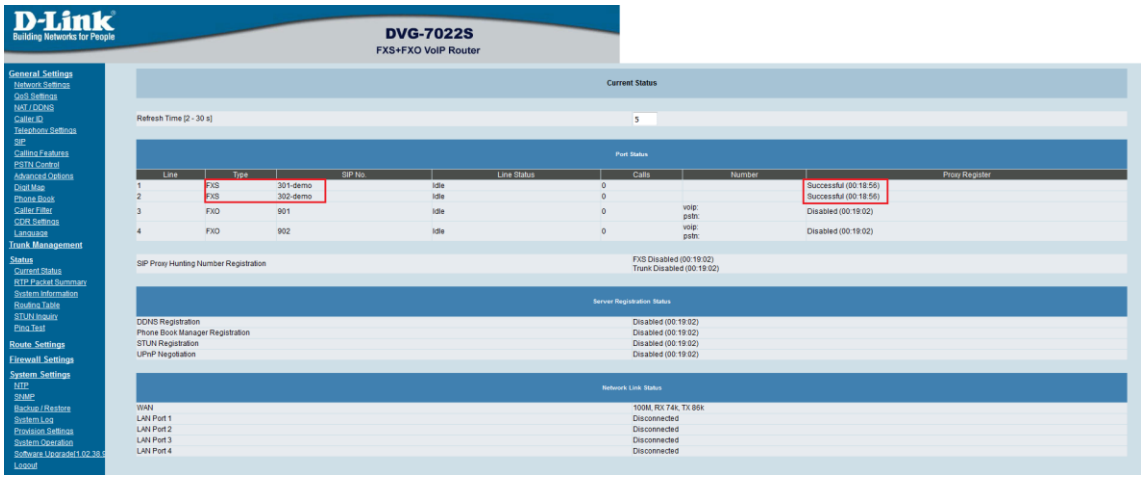


Сохранение. "System Settings" / "System Operation"

Финальный этап настройки голосового шлюза – сохранение всех внесенных параметров/изменений и перезагрузка устройства.



После перезагрузки порты FXS голосового шлюза должны быть зарегистрированы на виртуальной АТС. Для верности убедимся в их статусе регистрации, сделать это можно в разделе **"Status" / "CurrentStatus"**.



Теперь, когда городские линии подключены к портам FXO, а телефонные аппараты – к портам FXS, входящие вызовы на городские номера будут распределяться по сотрудникам. В случае, если все номера заняты или никто из работников не ответил, вызовы будут направлены на указанный номер мобильного телефона.

Базовые настройки завершены – у компании "X" есть возможность принимать и совершать вызовы.

2.28. Практическая работа № 28
Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе

Топология

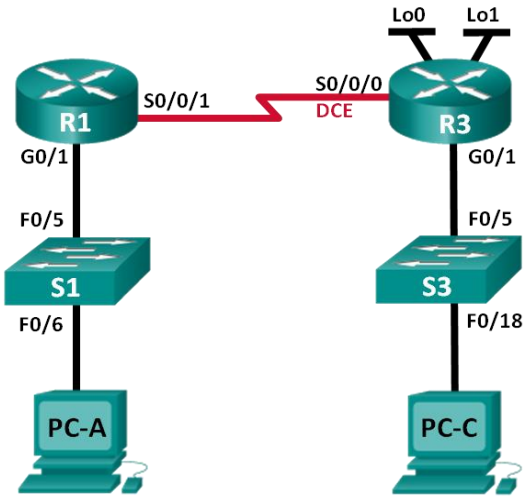


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсе-ти	Шлюз по умолчанию
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

Часть 2. Настройка базовых параметров устройств и проверка подключения

Часть 3. Настройка статических маршрутов

- Настройка рекурсивного статического маршрута.
- Настройка статического маршрута с прямым подключением.
- Настройка и удаление статических маршрутов.

Часть 4. Настройка и проверка маршрута по умолчанию

Исходные данные/сценарий

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор маршрутов, в соответствии с которыми определяется, какой шлюз или интерфейс маршрутизатор использует для достижения конкретной сети. Изначально таблица маршрутизации содер-

жит только сети с прямым подключением. Для обмена данными с удалёнными сетями, нужно определить маршруты для их достижения и внести их в таблицу маршрутизации. В данной лабораторной работе вам предстоит вручную настроить статический маршрут до конкретной удалённой сети, исходя из IP-адреса следующего перехода или выходного интерфейса. Также вы настроите статический маршрут по умолчанию. Маршрут по умолчанию — это тип статического маршрута, определяющий шлюз, который следует использовать в том случае, когда таблица маршрутизации не содержит путь до сети назначения.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки статической маршрутизации. Список требуемых команд приведён в приложении А. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

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

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

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

Необходимые ресурсы:

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

Часть 1: Настройка топологии и инициализация устройств

Шаг 1:

Подключите кабели в сети в соответствии с топологией.

Шаг 2:

Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: Настройка базовых параметров устройств и проверка подключения

Во второй части лабораторной работы вам необходимо настроить такие базовые параметры, как IPадреса интерфейсов, доступ к устройствам и пароли. Вам предстоит проверить подключение по локальной сети и определить маршруты, перечисленные в таблицах маршрутизации для маршрутизаторов R1 и R3.

Шаг 1:

Настройте интерфейсы ПК.
Шаг 2:

Настройте базовые параметры на маршрутизаторах.
a. Задайте устройствам имена в соответствии с топологией и таблицей адресации. b. Отключите поиск DNS.
c. Установите **class** в качестве пароля привилегированного режима. В качестве паролей консоли и виртуального терминала vty задайте **cisco**.
d. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.
Шаг 3:

Настройте IP-параметры на маршрутизаторах.
a. Настройте IP-адреса на интерфейсах маршрутизаторов R1 и R3 в соответствии с таблицей адресации.
b. Подключение S0/0/0 — это подключение DCE, которое требует выполнения команды **clock rate**. Настройка интерфейса S0/0/0 маршрутизатора R3 отображена ниже.
R3(config)# **interface s0/0/0**
R3(config-if)# **ip address 10.1.1.2 255.255.255.252**
R3(config-if)# **clock rate 128000** R3(config-if)# **no shutdown**
Шаг 4:

Проверьте подключение в локальных сетях.
a. Проверьте соединение, отправив эхо-запросы с каждого ПК на соответствующие шлюзы по умолчанию.
Успешно ли проходит эхо-запрос с узла PC-A на шлюз по умолчанию? _____
Успешно ли проходит эхо-запрос с узла PC-C на шлюз по умолчанию? _____
b. Проверьте соединение, отправив эхо-запросы между маршрутизаторами с прямым подключением.
Успешно ли проходит эхо-запрос с маршрутизатора R1 на интерфейс S0/0/0 маршрутизатора R3?
Если на какой-либо из этих вопросов вы ответили отрицательно, выявите и устраните неполадки в конфигурации.
c. Проверьте соединение между устройствами без прямого подключения.
Успешно ли проходит эхо-запрос с PC-A на PC-C? _____
Успешно ли отправляется эхо-запрос от узла PC-A на интерфейс Lo0? _____
Успешно ли проходит эхо-запрос с PC-A на Lo1? _____ Успешно ли выполнены эхо-запросы? Поясните свой ответ.
Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.
Шаг 5:

Сбор информации.

a. Проверьте состояние интерфейсов на маршрутизаторе R1 с помощью команды **show ip interface brief**.
Сколько интерфейсов активировано на маршрутизаторе R1? _____
b. Проверьте состояние интерфейсов на маршрутизаторе R3.
Сколько интерфейсов активировано на маршрутизаторе R3? _____
c. Просмотрите таблицу маршрутизации на маршрутизаторе R1 с помощью команды **show ip route**.
Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, но отсутствуют в таблице маршрутизации R1?
Просмотрите таблицу маршрутизации на маршрутизаторе R3.
Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, но отсутствуют в таблице маршрутизации R3?
_____ Почему в таблицах маршрутизации каждого из маршрутизаторов содержатся не все сети?

Часть 3: Настройка статических маршрутов

В третьей части лабораторной работы вам предстоит разными способами реализовывать статические и маршруты по умолчанию, убедиться, что маршруты были добавлены в таблицы маршрутизации маршрутизаторов R1 и R3, а также проверить подключение на основе внесённых маршрутов.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки статической маршрутизации. Список требуемых команд приведён в приложении А. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Шаг 1:

Настройка рекурсивного статического маршрута.

При использовании рекурсивного статического маршрута указывается IP-адрес следующего перехода. Поскольку задается только IP-адрес следующего перехода, перед пересылкой пакетов маршрутизатор должен несколько раз выполнить поиск в таблице маршрутизации. Для настройки рекурсивных статических маршрутов используйте следующий синтаксис:

Router(config)# **ip route** *адрес-сети маска-подсети ip-адрес*

a. На маршрутизаторе R1 настройте статический маршрут к сети 192.168.1.0, используя IP-адрес последовательного интерфейса Serial 0/0/0 маршрутизатора R3 в качестве адреса следующего перехода. Ниже напишите команду, которую вы использовали.
b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.
Как новый маршрут отображается в таблице маршрутизации?
_____ Успешно ли проходит эхо-запрос с узла PC-A на узел PC-C? _____
Эти запросы не будут успешными. Если рекурсивный статический маршрут настроен верно, эхозапрос поступает на PC-C. PC-C отправляет ответ на эхо-запрос компьютеру PC-A. Однако ответ на эхо-запрос сбрасывается на маршрутизаторе R3, поскольку R3 не обладает обратным маршрутом к сети 192.168.0.0 в таблице маршрутизации.

Шаг 2:

Настройка статического маршрута с прямым подключением.

При использовании статического маршрута с прямым подключением указывается выходной интерфейс (параметр *exit-interface*), что позволяет маршрутизатору принять ре-

шение о пересылке за один поиск. Статический маршрут с прямым подключением обычно используется с последовательным интерфейсом для соединения типа точка-точка. Для настройки статических маршрутов с прямым подключением с указанным выходным интерфейсом используйте следующий синтаксис:

Router(config)# **ip route** *адрес-сети маска-подсети выходной-интерфейс*

a. Н

а маршрутизаторе R3 настройте статический маршрут к сети 192.168.0.0, используя интерфейс S0/0/0 в качестве выходного. Ниже напишите команду, которую вы использовали.

b. П

роверьте наличие новой записи статического маршрута в таблице маршрутизации.

Как новый маршрут отображается в таблице маршрутизации?

c. У

спешно ли проходит эхо-запрос с узла PC-A на узел PC-C? _____ Эхо-запрос должен пройти успешно.

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

Шаг 3:

Настройте статический маршрут.

a. Н

а маршрутизаторе R1 настройте статический маршрут к сети 198.133.219.0, указывая один из параметров настройки статического маршрута, предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

b. Н

а маршрутизаторе R1 настройте статический маршрут к сети 209.165.200.224 маршрутизатора R3, задав другой параметр конфигурации статического маршрута из предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

c. р

оверьте наличие новой записи статического маршрута в таблице маршрутизации.

Как новый маршрут отображается в таблице маршрутизации?

d. с

пешно ли проходит эхо-запрос с узла PC-A на адреса маршрутизатора R1 198.133.219.1? _____ Эхо-запрос должен пройти успешно.

Шаг 4:

Удалите статические маршруты для loopback-адресов.

a. Н

а маршрутизаторе R1 используйте команду **no**, чтобы удалить статические маршруты для двух loopback-адресов из таблицы маршрутизации. В специально отведённом месте напишите команды, которые вы использовали.

b. р

осмотрите таблицу маршрутизации, чтобы убедиться в успешном удалении маршрутов.

Сколько маршрутов сети указано в таблице маршрутизации маршрутизатора R1? _____ Настроен ли шлюз «последней надежды»? _____

Часть 4: Настройка и проверка маршрута по умолчанию

В четвёртой части необходимо реализовать маршрут по умолчанию, проверить добавление маршрута в таблицу маршрутизации и проверить подключение, использующее внесённый маршрут.

Маршрут по умолчанию определяет шлюз, на который маршрутизатор отправляет все IP-пакеты, для которых у него нет заимствованного или статического маршрута. Стати-

ческий маршрут по умолчанию — это статический маршрут, IP-адрес назначения и маска подсети которого равны 0.0.0.0. Обычно его называют маршрутом «четырёх нолей». В маршруте по умолчанию можно указать либо IP-адрес следующего перехода, либо выходной интерфейс. Для настройки статических маршрутов по умолчанию используйте следующий синтаксис:

Router(config)# **ip route 0.0.0.0 0.0.0.0** {*ip-address or exit-intf*}

a. На маршрутизаторе R1 настройте маршрут по умолчанию, используя выходной интерфейс S0/0/1. Ниже напишите команду, которую вы использовали.

_

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.

Как новый маршрут отображается в таблице маршрутизации?

_____ Какой шлюз является шлюзом «последней надежды»?

c. Успешно ли проходит эхо-запрос с узла PC-A на адрес 209.165.200.225? _____

d. Успешно ли проходит эхо-запрос с узла PC-A на адрес 198.133.219.1? _____ Эхо-запросы должны пройти успешно.

Вопросы на закрепление

1. Новая сеть 192.168.3.0/24 подключена к интерфейсу G0/0 маршрутизатора R1. Какие команды можно использовать для настройки статического маршрута к этой сети от маршрутизатора R3?

2. Существует ли преимущество в настройке статического маршрута с прямым подключением по сравнению с настройкой рекурсивного статического маршрута?

_____ 3. Почему так важно настроить маршрут по умолчанию на маршрутизаторе?

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	Gigabit Ethernet 0/1	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

	(G0/0)	(G0/1)		

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

Приложение A: команды настройки для частей 2, 3 и 4

Команды содержатся в приложении A только для справки. Приложение не содержит все команды, необходимые для выполнения данной лабораторной работы.

Базовые параметры устройств

Настройка параметров IP на маршрутизаторе.

R3(config)# **interface s0/0/0**
R3(config-if)# **ip address 10.1.1.2 255.255.255.252**
R3(config-if)# **clock rate 128000**
R3(config-if)# **no shutdown**

Настройка статического маршрута

Настройка рекурсивного статического маршрута.

R1(config)# **ip route 192.168.1.0 255.255.255.0 10.1.1.2 Настройка статического маршрута с прямым подключением.**
R3(config)# **ip route 192.168.0.0 255.255.255.0 s0/0/0 Удаление статического маршрута.**
R1(config)# **no ip route 209.165.200.224 255.255.255.224 serial0/0/1** или
R1(config)# **no ip route 209.165.200.224 255.255.255.224 10.1.1.2** или
R1(config)# **no ip route 209.165.200.224 255.255.255.224**

Настройка маршрута по умолчанию

R1(config)# **ip route 0.0.0.0 0.0.0.0 s0/0/1**

2.29. Практическая работа № 29
Настройка голосовых сообщений в маршрутизаторе

В среде Call Manager мы можем принимать входные звонки с использованием автоответчика или IVR.

Для организации IVR у нас есть несколько путей:

- Использование **Cisco Unity Express** (в настоящее время запрет на продажу в РФ)
- Использование **Cisco Unity Connection**. Использование централизованного **UCCX**
- Использование продукта **Third Party**
- Использование **скриптов IVR**
-

Последний пункт хорош тем, что ничего не надо ставить дополнительного. Если в региональном офисе есть маршрутизатор с поддержкой голоса, на нем можно поднять простой скрипт IVR.

Скрипт IVR также накладывает и ограничение: с ним нельзя использовать **MGCP**.

приведенный ниже пример скрипта включает в себя 5 файлов:
router#show flash
25 3293 Apr 21 2011 12:22:48 +06:00 vxml-ivr/My.vxml
26 45754 Apr 21 2011 11:39:16 +06:00 vxml-ivr/newfirst_announcement.wav
27 38458 Apr 21 2011 12:37:30 +06:00 vxml-ivr/absent_number.wav
28 48058 Apr 21 2011 12:38:12 +06:00 vxml-ivr/number_busy.wav
29 45754 Apr 21 2011 12:37:52 +06:00 vxml-ivr/no_answer.wav

Работа скрипта:
При входящем звонке снимается трубка и звучит приветствие. При этом можно набрать 3-х значный внутренний номер либо дождаться ответа секретаря.
0 – Секретарь
9 – Факс

Настройка IOS:

Включение сервиса vxml
application
service ivrr flash:/vxml-ivr/My.vxml
!
global
service alternate default

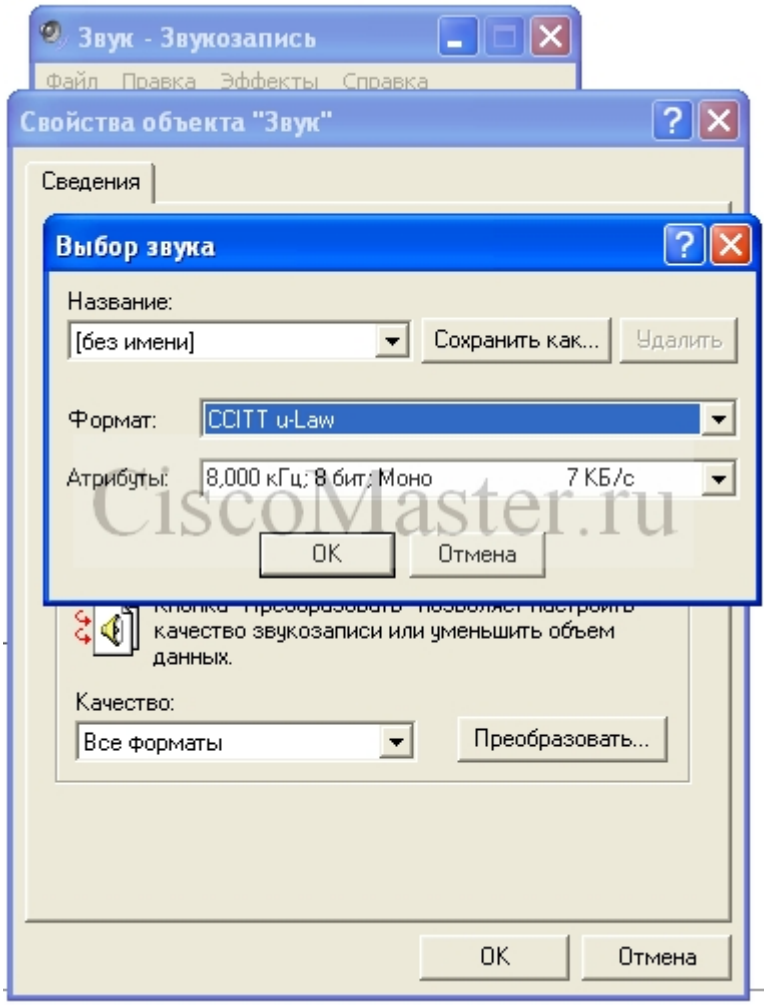
Настройка физического порта FXO. Входящий звонок будет перенаправлен на внутренний номер 550.
voice-port 1/0/8
supervisory disconnect dualtone mid-call
echo-cancel coverage 32
timeouts call-disconnect 1
timeouts ringing 20
timeouts wait-release 1
connection plar 550
caller-id enable

Данный диалпир направляет звонки на внутренний номер 550 на скрипт.
dial-peer voice 1000 pots
service ivrr
incoming called-number 550
port 1/0/8

Скрипт возвращает трехзначный номер абонента. Его отдаем на Call Manager:
dial-peer voice 3001 voip
description Short calls
destination-pattern [1-5]..
session target ipv4:10.16.0.11
dtmf-relay h245-alphanumeric
codec g711ulaw
no vad

При изменении скрипта или файлов необходимо перезапустить:
application
no service ivrr flash:/vxml-ivr/My.vxml
service ivrr flash:/vxml-ivr/My.vxml

Запись звуковых файлов:
Самое простое: приложение sndrec32, там выбираем тип формата CCITT u-Law 8,000 и приступаем к записи.



Проверка
debug voip application digitcollect
show call active voice compact

2.30. Практическая работа № 30
Настройка программно-аппаратной IP-АТС

Ознакомление с основами технологии IP-телефонии, с основным функционалом ПО FreeSWITCH и программного телефона 3CX Phone.

1.2 Рабочее задание

1.2.1 Проверить наличие учетной записи SIP на сервере FreeSWITCH в соответствии с вариантом задания.
1.2.2 Произвести настройку учетной записи программного телефона 3CX Phone в соответствии с заданным вариантом.
1.2.3 Осуществить несколько голосовых вызовов для проверки правильности настройки программного телефона.
1.2.4 Произвести настройку программируемых кнопок программного телефона 3CX Phone в соответствии с заданным вариантом и проверить их работоспособность.
1.2.5 Составить отчет о проделанной работе.

1.3 Методические указания по выполнению работы

1.3.1 Система FreeSWITCH была создана в 2006 г. Энтони Минессейлом (Anthony Minessale), одним из бывших разработчиков Asterisk. При разработке архитектуры FreeSWITCH были учтены проблемы существующих на тот период открытых программных продуктов для IP-телефонии. Поэтому новинка отличается стабильной работой и имеет возможность работать не только под управлением Linux, но и под Windows. Основным интерфейсом конфигурирования FreeSWITCH являются текстовые файлы в формате XML.
Система FreeSWITCH может быть использована в качестве коммутатора, АТС, медиа шлюза или медиа сервера для приложений IVR, использующих простые или XML скрипты для управления алгоритмом обработки звонка. FreeSWITCH поддерживает разные протоколы, такие как SIP, H.323, IAX2 и Google Talk, что позволяет взаимодействовать с sipX, OpenPBX, Bayonne, YATE, или Asterisk. FreeSWITCH поддерживает много продвинутых возможностей SIP, таких как присутствие/BLF/SLA, TCP TLS и sRTP др. Голосовые каналы и конференции могут работать на частотах 8, 16, 32 и 48 кГц и позволяют объединять каналы с разными частотами.
FreeSWITCH поддерживает широчайший набор функций, начиная от голосового меню, статистики звонков, заканчивая голосовой почтой, callцентром и многими другими. Среди ее основных достоинств выделяют:

- богатые функциональные возможности;
- поддержка разнообразных телефонных интерфейсов: аналоговых, цифровых, протоколов IP телефонии;
- простое подключение IP телефонов и высокое качество связи.

1.3.2 Запустите программу WinSCP для удаленного соединения компьютера с сервером. При помощи программы WinSCP можно соединиться с сервером SSH по протоколу SFTP (SSH File Trasfer Protocol) или SCP (Secure Copy Protocol), как правило, с машинами под ОС UNIX. В появившемся окне заполните следующие поля:
File protocol: SFTP
Host name: 192.168.1.67
Port number: 22
User name: root Password: qscaxz
1.3.3 Подтвердить ввод данных нажатием кнопки Login (рисунок 1.1).

Рисунок 1.1 – Окно подключения WinSCP

1.3.4 В открывшемся окне файлового менеджера (рисунок 1.2) на правой панели отображаются файлы, находящиеся на удаленном сервере, а на левой – файлы, находящиеся на локальном компьютере.
1.3.5 На удаленном сервере перейдите в директорию с учетными записями SIP /usr/local/freeswitch/conf/directory/default (рисунок 1.3).

1.3.6 Удостоверьтесь, что файл, соответствующий вашему варианту, существует в указанной директории. Например, если по варианту указана учетная запись 1000, то варианту соответствует файл 1000.xml.

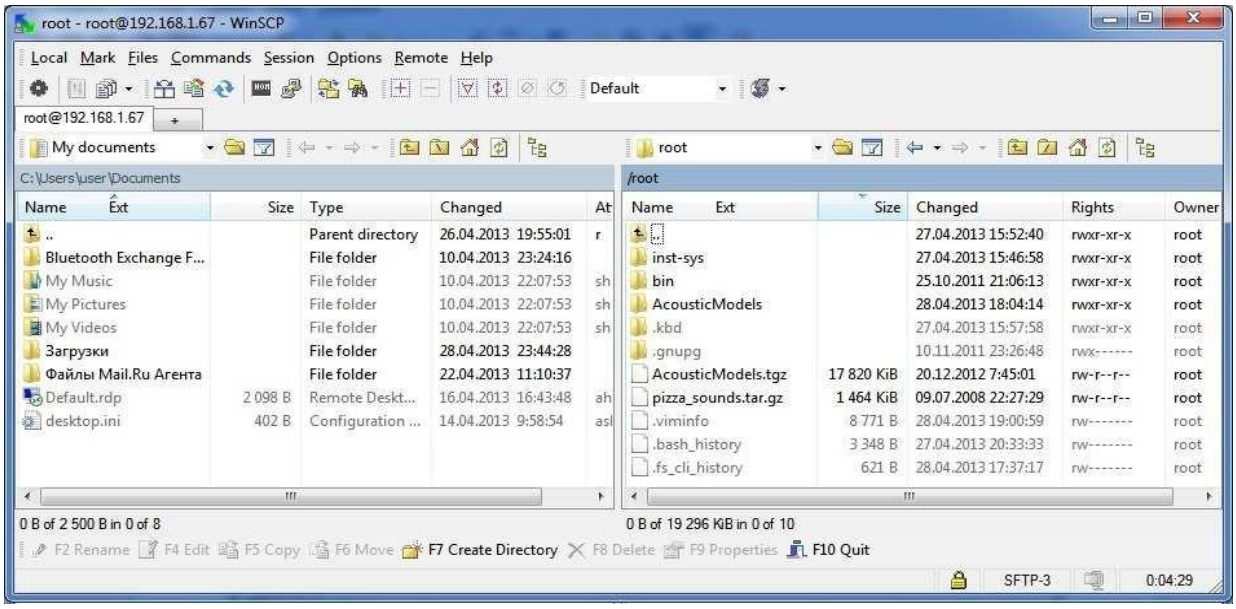


Рисунок 1.2 – Основное окно WinSCP

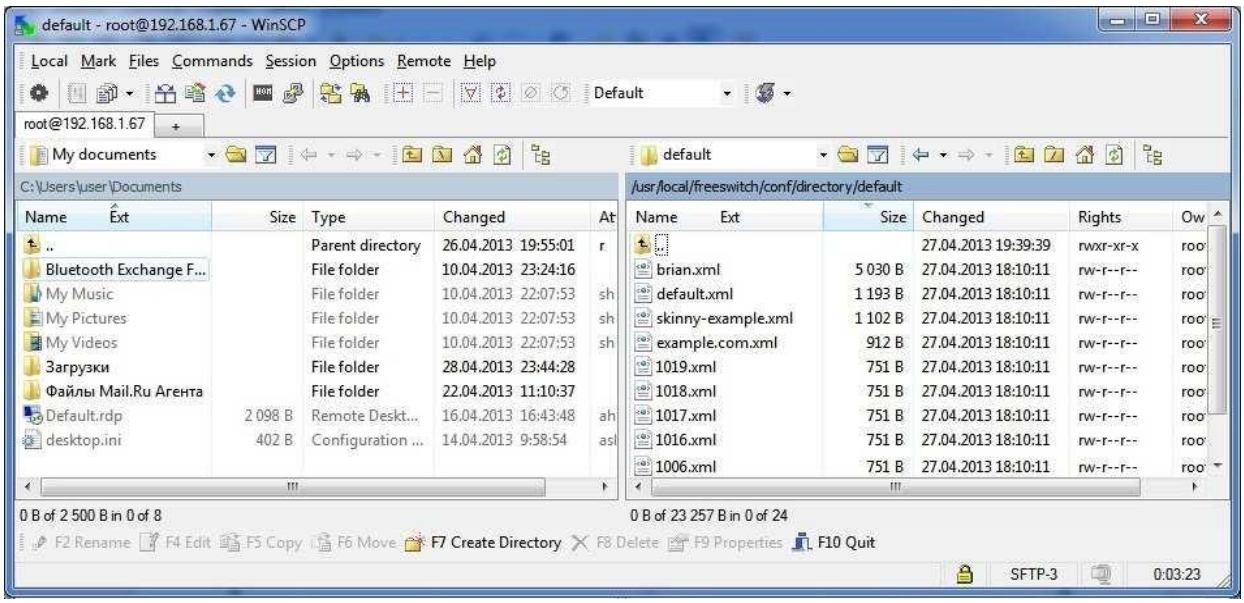


Рисунок 1.3 – Содержимое директории
/usr/local/freeswitch/conf/directory/default

1.3.7 Запустите программу 3CX Phone. В открывшемся окне (рисунок 1.4) нажмите кнопку Главное меню.
1.3.8 На появившейся панели (рисунок 1.5) нажмите кнопку Accounts.
1.3.9 В открывшемся окне (рисунок 1.6) нажмите кнопку New.

Рисунок 1.4 – Основное окно 3CX Phone до регистрации на сервере

Рисунок 1.5 – Окно главного меню 3CX Phone

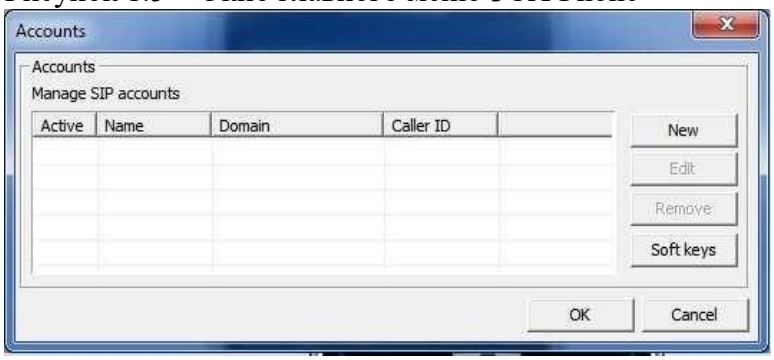


Рисунок 1.6 – Окно учетных записей 3CX Phone

1.3.9 В открывшемся окне (рисунок 1.7) укажите следующие данные
Account name: Student_XX
Caller ID: YYYY
Extension: YYYY
ID: YYYY Password: 1234 local IP 192.168.1.67
Здесь: *XX* – номер варианта; *YYYY* – учетная запись согласно варианту.

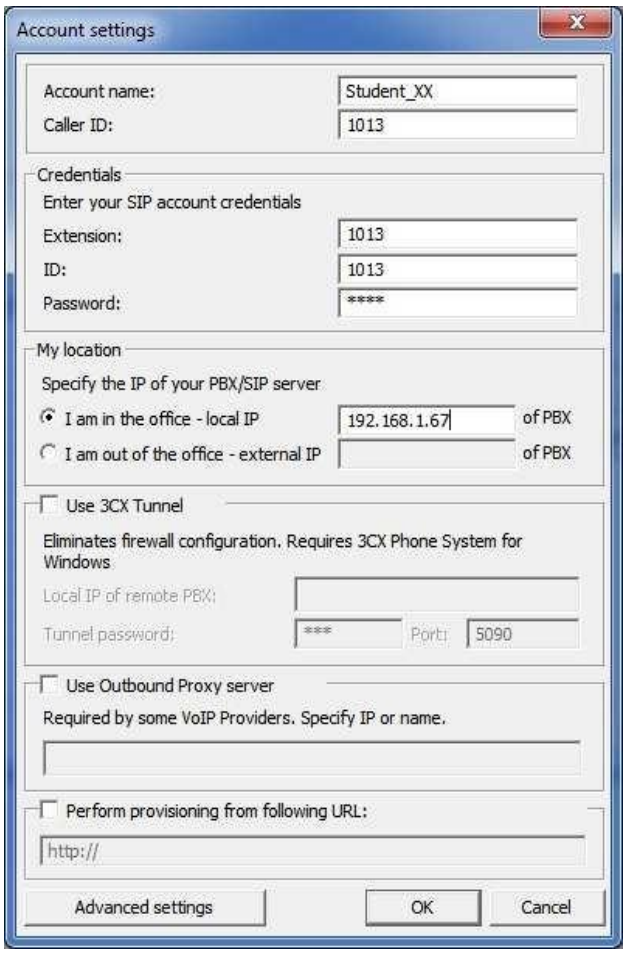


Рисунок 1.7 – Окно настройки учетной записи 3CX Phone

1.3.10 Закройте окна (рисунок 1.7, рисунок 1.6) нажатием кнопок *OK*.
1.3.11 В строке состояния должен отобразиться статус On Hook (рисунок 1.8).

Рисунок 1.8 – Основное окно 3CX Phone после регистрации на сервере

1.3.12 Совершите голосовые вызовы на несколько номеров из диапазона 1000- 1019. Удостоверьтесь, что вызовы проходят нормально.
1.3.13 Откройте панель программируемых кнопок. Нажмите на первой программируемой кнопке правой кнопкой мыши.
1.3.14 В открывшемся окне (рисунок 1.9) заполните поля Label и User ID. Закройте окно нажатием кнопки *OK*.
1.3.15 Проверьте работоспособность запрограммированной кнопки.

Рисунок 1.9 – Окно настройки программируемой кнопки
1.3.16 Составить отчет о проведенной работе. Исходные данные приведены в таблице 1.1.

Таблица 1.1 — Исходные данные

№	Уч.запись	№	Уч.запись	№	Уч.запись	№	Уч.запись
1	1000	6	1005	11	1010	16	1015
2	1001	7	1006	12	1011	17	1016
3	1002	8	1007	13	1012	18	1017
4	1003	9	1008	14	1013	19	1018
5	1004	10	1009	15	1014	20	1019

2.31. Практическая работа № 31
Установка и настройка программ-ной IP-АТС

Ознакомление с протоколом SIP и принципами его работы, с конфигурационными файлами ПО FreeSWITCH, в которых находятся настройки протокола SIP.

2.2 Рабочее задание

2.2.1 Создать учетную запись SIP на сервере FreeSWITCH в соответствии с вариантом задания.
2.2.2 Произвести настройку учетной записи программного телефона
3CX Phone в соответствии с созданной учетной записью SIP.

2.2.3 Осуществить несколько голосовых вызовов для проверки правильности настройки программного телефона и сервера.
2.2.4 Составить отчет о проделанной работе.

2.3 Методические указания по выполнению работы

2.3.1 Запустите программу Блокнот. Внесите в окно программы текст на основе шаблона (рисунок 2.1). Внести изменения в шаблон в соответствии с данными учетной записи SIP согласно варианту.

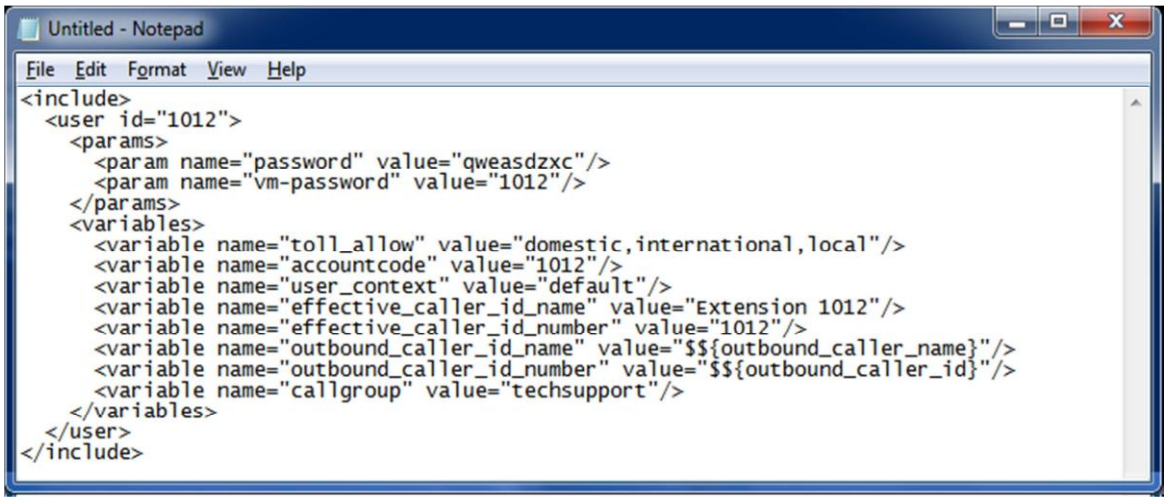


Рисунок 2.1 – Шаблон для учетной записи SIP с идентификатором 1012

2.3.2 Сохраните текст через пункт меню Файл – Сохранить как...
(рисунок 2.2).
2.3.3 В открывшемся окне (рисунок 2.3) в поле File name (Имя файла) введите *YYYY.xml*, где *YYYY* — идентификатор учетной записи SIP согласно варианту. В поле Save as type (Тип файла) укажите All files (Все файлы).
2.3.4 Нажмите кнопку Save (Сохранить).
2.3.5 Запустите программу WinSCP и подключитесь к серверу (лабораторная работа №1).
2.3.6 На удаленной стороне укажите директорию /usr/local/freeswitch/conf/directory/default.

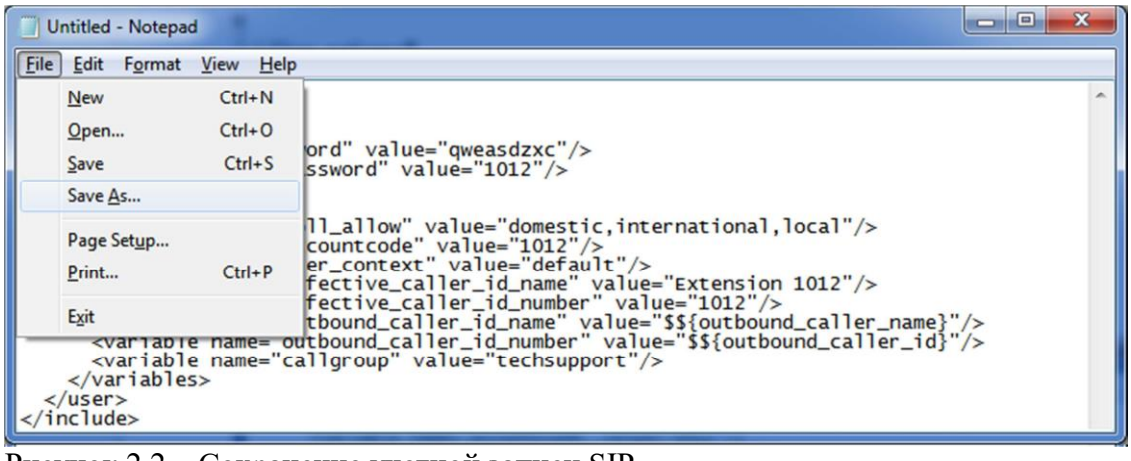


Рисунок 2.2 – Сохранение учетной записи SIP

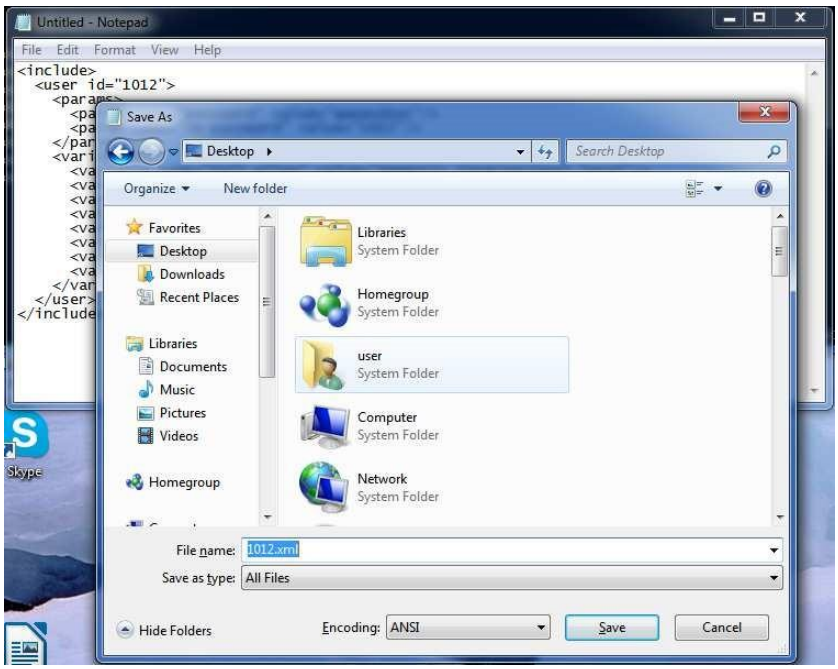


Рисунок 2.3 – Выбор типа, расширения и имени файла

2.3.7 На локальной стороне укажите директорию, в которой находится раннее сохраненный файл.
2.3.8 На локальной стороне выделите ранее сохраненный файл. Затем нажмите клавишу F5 или кнопку F5 Copy (рисунок 2.4).

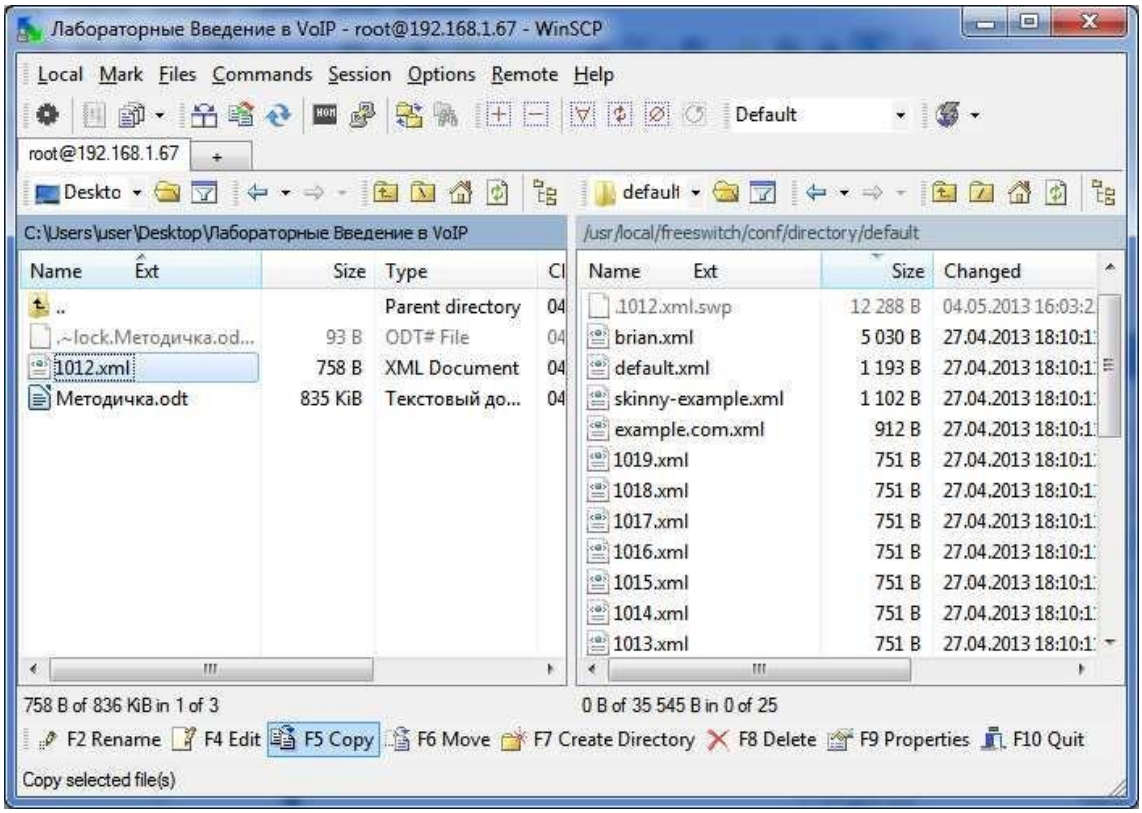


Рисунок 2.4 – Передача файла на сервер
2.3.9 Сообщите преподавателю о результате передачи файла.
2.3.10 Запустите программу 3CX Phone и произведите настройку учетной записи, используя данные из созданного файла (лабораторная работа №1). Удостоверьтесь, что регистрация на сервере пройдена успешно.

2.3.11 Совершите голосовые вызовы на несколько номеров из диапазона 1000-1019. Удостоверьтесь, что вызовы проходят нормально.
2.3.12 Составить отчет о проведенной работе. Исходные данные приведены в таблице 2.1.

Таблица 2.1 – Исходные данные

№	Учетная запись SIP	Пароль	№	Учетная запись SIP	Пароль
1	1020	qwe	11	1030	edc
2	1021	rty	12	1031	rfv
3	1022	uio	13	1032	tgb
4	1023	asd	14	1033	yhn
5	1024	fgh	15	1034	ujm
6	1025	jkl	16	1035	qaw
7	1026	zxc	17	1036	sed
8	1027	vbn	18	1037	rft
9	1028	qaz	19	1038	gyh
10	1029	wsx	20	1039	uji

2.32. Практическая работа № 32
Тестирование кодеков. Исследование параметров качества обслуживания

Ознакомление с основами нумерации в телефонных сетях, с назначением нумерационных планов и конфигурационными файлами ПО FreeSWITCH, в которых находятся настройки нумерационного плана.

3.2 Рабочее задание

3.2.1 Создать запись нумерационного плана ПО FreeSWITCH для учетной записи SIP, созданной в предыдущей лабораторной работе, в соответствии с заданным вариантом.
3.2.2 Произвести загрузку конфигурационных файлов в ПО FreeSWITCH.
3.2.3 Осуществить несколько голосовых вызовов для проверки правильности настройки нумерационного плана.
3.2.4 Составить отчет о проделанной работе.

3.3 Методические указания по выполнению работы

3.3.1 Запустите программу *Блокнот*. Внесите в окно программы текст на основе шаблона (рисунок 3.1). Внести изменения в шаблон в соответствии с данными записи нумерационного плана согласно варианту.

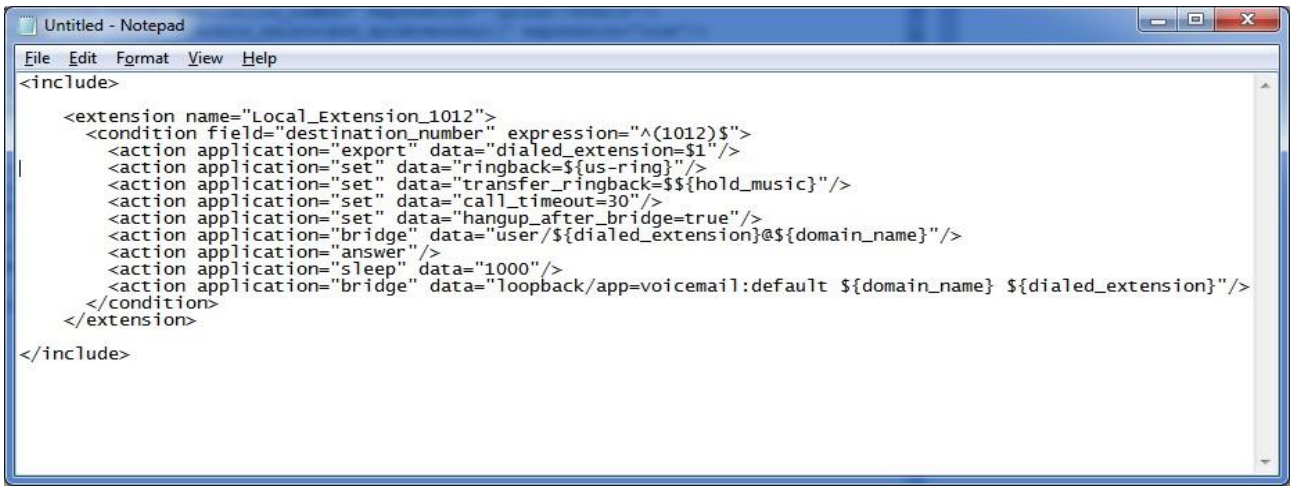


Рисунок 3.1 – Шаблон записи нумерационного плана с номером соответствия 1012 для учетной записи SIP с идентификатором 1012

3.3.2 Сохранить файл под именем *YYYYexten.xml* на локальном компьютере (лабораторная работа №2). Здесь *YYYY* – номер соответствия в записи нумерационного плана согласно варианту.
3.3.3 Скопируйте созданный файл на сервер в директорию /usr/local/freeswitch/conf/dialplan/default (лабораторная работа №2).
3.3.4 Запустите программу PuTTY. В окне параметров подключения PuTTY (рисунок 3.2) в поле *Host Name (or IP address)* укажите *192.168.1.67*. Остальные поля оставьте без изменения. Нажмите кнопку *Open*.

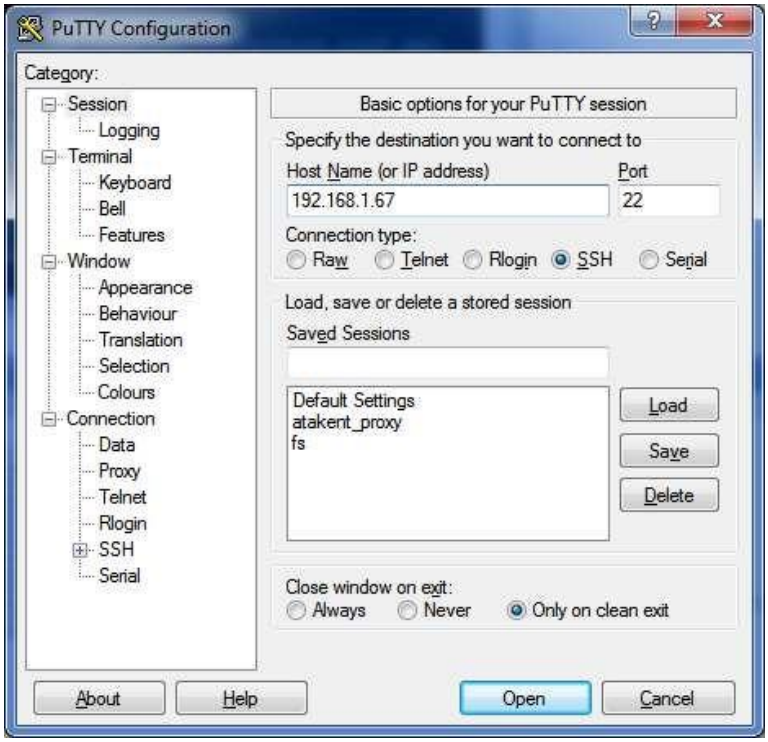


Рисунок 3.2 – Окно параметров подключения PuTTY

3.3.5 В открывшемся окне сессии PuTTY (рисунок 3.3) введите логин *root* и пароль *qscaxz*

3.3.6 После появления символа приглашения # введите команду *service freeswitch restart* для перезагрузки конфигурационных файлов FreeSWITCH.

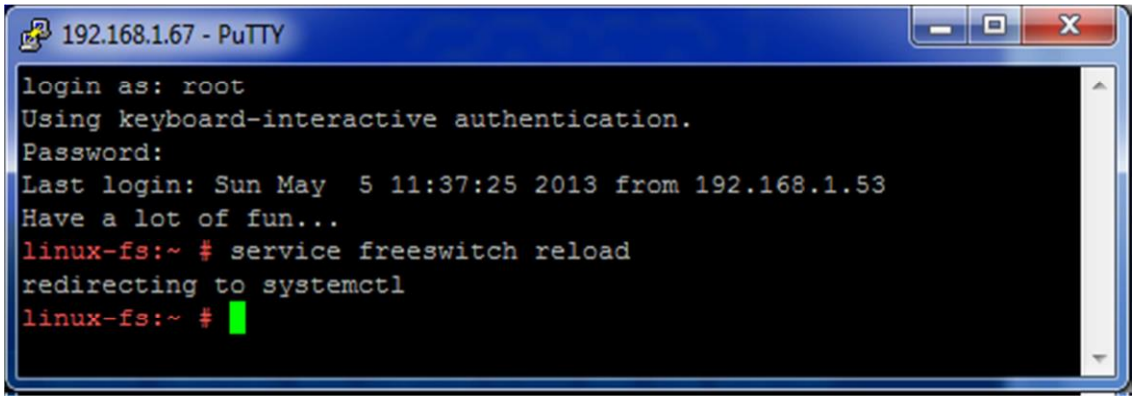


Рисунок 3.3 – Окно сессии PuTTY

3.3.7 Запустите программу 3CX Phone и произведите настройку учетной записи, используя данные из файла, созданного при выполнении лабораторной работы №2 (лабораторные работы №1,2). Удостоверьтесь, что регистрация на сервере пройдена успешно.
3.3.8 Совершите голосовые вызовы на несколько номеров из диапазона 1020 - 1039. Удостоверьтесь, что вызовы проходят нормально.
3.3.9 Составить отчет о проведенной работе. Исходные данные приведены в таблице 3.1.

Таблица 3.1 – Исходные данные

№	Номер нумерационного плана	Идентиф. учетной записи SIP	№	Номер нумерационного плана	Идентиф. учетной записи SIP
1	1020	1020	11	1030	1030
2	1021	1021	12	1031	1031
3	1022	1022	13	1032	1032
4	1023	1023	14	1033	1033
5	1024	1024	15	1034	1034
6	1025	1025	16	1035	1035
7	1026	1026	17	1036	1036
8	1027	1027	18	1037	1037
9	1028	1028	19	1038	1038
10	1029	1029	20	1039	1039

2.33. Практическая работа № 33
Мониторинг и анализ соединений по различным протоколам

Ознакомление с кодеками, используемыми для видеовызовов, и их характеристиками, с основами аудиоконференцсвязи и конфигурационными файлами FreeSWITCH, в которых находятся настройки аудиоконференций.

4.2 Рабочее задание

4.2.1 Осуществить несколько видеовызовов между программными телефонами с различными настройками кодеков в соответствии с заданным вариантом.
4.2.2 Произвести подключение к предварительно настроенным аудиоконференциям в соответствии с заданным вариантом.
4.2.3 Сравнить качество звука в различных аудиоконференциях.
4.2.4 Составить отчет о проделанной работе.

4.3 Методические указания по выполнению работы

4.3.1 Запустите программу 3CX Phone и произведите настройку учетной записи, используя данные из файла, созданного при выполнении лабораторной работы 2 (лабораторные работы №1,2). Удостоверьтесь, что регистрация на сервере пройдена успешно.
4.3.2 Откройте окно настройки учетной записи 3CX Phone (рисунок 1.7, лабораторная работа №1) на вызывающей стороне. В данном окне нажмите кнопку Advanced settings.
4.3.3 В открывшемся окне (рисунок 4.1) в разделе Video formats произведите настройку приоритетов форматов видео согласно варианту. Закройте окно нажатием кнопки *OK*.
4.3.4 Произведите действия пунктов 4.3.2 - 4.3.3 для вызываемой стороны.
4.3.5 Нажмите Кнопку открытия панели Видео. Удостоверьтесь, что телефон подключился к локальной web-камере (рисунок 4.2).

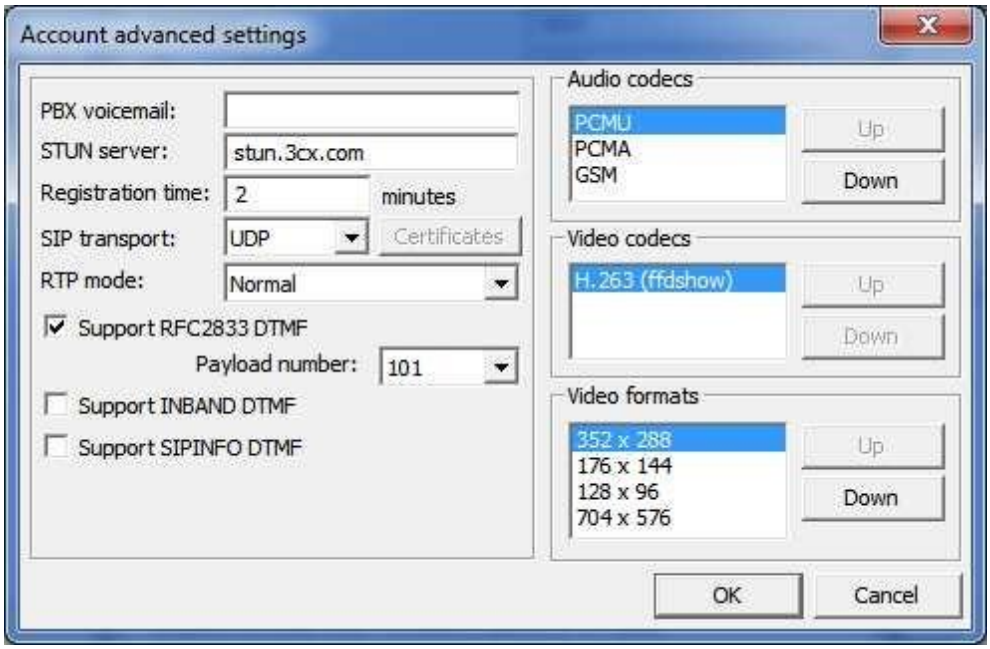


Рисунок 4.1 – Окно расширенных настроек учетной записи 3CX Phone

Рисунок 4.2 – Основное окно 3CX Phone с открытой панелью Видео

4.3.6 На вызывающей стороне наберите номер вызываемой стороны и осуществите вызов. Удостоверьтесь, что установлена двухсторонняя аудио/видео связь (рисунок 4.3). Зафиксируйте используемый формат видео.
4.3.8 Измените порядок приоритетов форматов видео вызываемой и вызывающей сторон (рисунок 4.1) по своему усмотрению. Повторно осуществите видеовызов. Зафиксируйте используемый формат видео.
4.3.9 В ПО FreeSWITCH предварительно настроено три группы статических конференций, различающихся используемыми кодеками:

- статические конференции с узкополосными кодеками. Сто конференций имеют телефонные номера от 3000 до 3099;
- статические конференции с широкополосными кодеками. Сто конференций имеют телефонные номера от 3100 до 3199;
- статические конференции со сверхширокополосными кодеками. Сто конференций имеют телефонные номера от 3200 до 3299.

Рисунок 4.3 – Основное окно 3CX Phone при активном видеовызове
4.3.10 Осуществите голосовой вызов с двух или более телефонов на номера статических конференций согласно варианту. Оцените и сравните качество звука в задействованных статических конференциях.
4.3.9 Составить отчет о проведенной работе. Исходные данные приведены в таблице 4.1.

Таблица 4.1 – Исходные данные

№	Приоритеты форматов видео вызывающей стороны	Приоритеты форматов видео вызываемой стороны	Список номеров статических конференций
1	704 x 576; 352 x 288; 176 x 144; 128 x 96	704 x 576; 352 x 288; 176 x 144; 128 x 96	3001, 3101, 3201
2	704 x 576; 352 x 288; 176 x 144; 128 x 96	352 x 288; 176 x 144; 128 x 96; 704 x 576	3002, 3102, 3202
3	704 x 576; 352 x 288; 176 x 144; 128 x 96	176 x 144; 128 x 96; 704 x 576; 352 x 288	3003, 3103, 3203
4	704 x 576; 352 x 288; 176 x 144; 128 x 96	128 x 96; 704 x 576; 352 x 288; 176 x 144	3004, 3104, 3204
5	352 x 288; 176 x 144; 128 x 96; 704 x 576	704 x 576; 352 x 288; 176 x 144; 128 x 96	3005, 3105, 3205
6	352 x 288; 176 x 144; 128 x 96; 704 x 576	352 x 288; 176 x 144; 128 x 96; 704 x 576	3006, 3106, 3206
7	352 x 288; 176 x 144; 128 x 96; 704 x 576	176 x 144; 128 x 96 704 x 576; 352 x 288	3007, 3107, 3207
8	352 x 288; 176 x 144; 128 x 96; 704 x 576	128 x 96; 704 x 576; 352 x 288; 176 x 144	3008, 3108, 3208
9	176 x 144; 128 x 96; 704 x 576; 352 x 288	704 x 576; 352 x 288; 176 x 144; 128 x 96	3009, 3109, 3209
10	176 x 144; 128 x 96; 704 x 576; 352 x 288	352 x 288; 176 x 144; 128 x 96; 704 x 576	3010, 3110, 3210

2.34. Практическая работа № 34
Мониторинг вызовов в программ-ном коммутаторе

Ознакомление с элементами IP-сети (коммутатором второго уровня, шлюзом, программным телефоном 3CX Phone и прикладным процессом Asterisk) и с особенностями и возможностями операционной системы Linux (идеология файловой системы, структура каталогов, основные дистрибутивы, основные команды по конфигурированию и настройке сервисов).

Рабочее задание

5.2.1 Соберите схему с использованием шлюза VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом
3CX Phone.
5.2.2 Присвоить ПК IP-адрес и маску подсети.
5.2.3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
5.2.4 Ознакомиться с выполнением различных процедур и команд.
5.2.5 Подключить мультимедийные приставки в ПК.
5.2.6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу.
5.2.6 Осуществите тестовые звонки между ПК.
5.2.7 Составьте отчет о результатах выполнения работы.

5.3 Методические указания по выполнению работы

5.3.1 Прикладной процесс Asterisk – это программная АТС, способная коммутировать как VoIP вызовы, так и вызовы, осуществляемые между IPтелефонами и традиционной телефонной сетью общего пользования. Количество абонентов в сети может достигать 2000 и ограничено только мощностью сервера.
Asterisk поддерживает следующие протоколы:

- IAX;
- SIP;
- H.323;
- Skinny;

- UNIStim.

Программное обеспечение Asterisk поддерживает следующие кодеки:

- G.711 (ulaw и alaw);
- G.722;
- G.723;
- G.729;
- GSM;
- iLBC;
- LPC-10; - Speex.

В основу принципов построения универсального шлюза VRX-1010-E1 положены гибкость и масштабируемость как программных, так и аппаратных средств.
VoIP-шлюз VRX-1010-E1 подключается к аналоговым и цифровым офисным АТС практически любых производителей (Panasonic, LG, Samsung,
Siemens и др.).
Универсальный VoIP VRX-1010-E1 шлюз реализован в виде законченного конструктива. Контроллер шлюза выполнен на основе мощного однокристального телекоммуникационного процессора и, по сути, представляет собой промышленный компьютер, функционирующий под управлением встроенной операционной системы Linux.
Программа управления шлюзом реализован как сервис (демоны) операционной системы Linux, что позволяет программе управления системой функционировать как на отдельно устанавливаемом специализированном сервере, так и непосредственно на плате универсального шлюза.
Между собой программы управления шлюзом и программа управления системой взаимодействуют через стек протоколов TCP-IP, что позволяет строить распределенные системы любой степени сложности. Поддерживает следующие основные протоколы управления/сигнализации:

- поддержка протоколов SIP и H.323;
- расширенные функции QoS;
- функции безопасности (авторизация пользователей, списки доступа);
- прием/передача факсов (FAX over IP); - конфигурирование через web-интерфейс.

Универсальный шлюз VRX-1010-E1 – модульное цифровое устройство, которое обладает мощным специализированным процессором для трансляции 2х мегабитных потоков E1 от АТС (УАТС) до SIP сервера (SIP АТС.
Универсальный VoIP шлюз позволит объединить в единое целое среды передачи для сетей передачи данных и традиционной телефонной сети.
5.3.2 Осуществите соединение сетевых устройств в соответствии схемы, представленной на рисунке 5.1.
5.3.3 Пропишите на ПК IP-адрес и маску в соответствии с вариантом (таблица 1.1). В качестве шлюза по умолчанию установите IP-адрес шлюза VRX-1010-E1.
5.3.4 Подключитесь к консоли шлюза VRX-1010-E1 через SSH-клиент
5.3.5 Приведите содержимое файла /etc/asterisk/asterisk.conf к следующему виду:

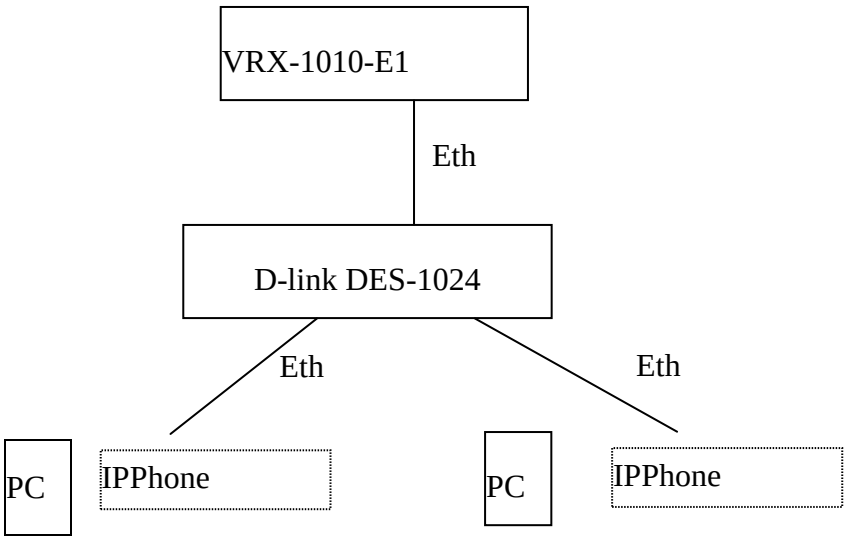


Рисунок 5.1 – Схема сети

[directories](!) astetcdir => /etc/asterisk astmoddir => /usr/lib64/asterisk/modules
astvarlibdir => /var/lib/asterisk astdbdir => /var/lib/asterisk astkeydir => /var/lib/asterisk
astdatadir => /usr/share/asterisk astagidir => /usr/share/asterisk/agi-bin astspooldir =>
/var/spool/asterisk astrundir => /run/asterisk
astlogdir => /var/log/asterisk

[options] languageprefix = yes runuser = asterisk rungroup = asterisk
documentation_language = en_US

[compat] pbx_realtime=1.6 res_agi=1.6
app_set=1.6

5.3.6 Приведите содержимое файла /etc/asterisk/sip.conf к следующему виду
[general] context=default allowoverlap=no udpenable=yes udpbindaddr=0.0.0.0 tcpenable=no srvlookup=yes videosupport=yes

5.3.7 Приведите содержимое файла /etc/asterisk/extensions.conf к следующему виду

[general] static=yes writeprotect=no clearglobalvars=no
[globals]
CONSOLE=Console/dsp
IAXINFO=guest
TRUNKMSD=1

[office]

5.3.8 Добавьте в файл /etc/asterisk/sip.conf следующие строки

[<X>] type=friend dtmfmode=rfc2833 host=dynamic secret=<pass> context=office

Здесь <X> и <pass> - логин и пароль в соответствии с вариантом.

5.3.9 Добавьте к содержимому файла /etc/asterisk/extensions.conf следующие строки

exten => <X>,1,Dial(SIP/<X>) same => n,HangUp()

Здесь <X> - логин в соответствии с вариантом.

5.3.10 В консоли введите следующие команды
service asterisk restart service iptables stop
5.3.11 На ПК запустите программу 3CX Phone и выполните её настройку для подключения к шлюзу.
5.3.12 Выполните тестовые вызовы между ПК
5.3.13 Составьте отчет о результатах выполнения работы.

Таблица 5.1 – Исходные данные

№	Сетевой адрес	№	Сетевой адрес	№	Сетевой адрес
1	168.192.1.1	8	168.192.1.8	15	168.192.1.15
2	168.192.1.2	9	168.192.1.9	16	168.192.1.16
3	168.192.1.3	10	168.192.1.10	17	168.192.1.17
4	168.192.1.4	11	168.192.1.11	18	168.192.1.18
5	168.192.1.5	12	168.192.1.12	19	168.192.1.19
6	168.192.1.6	13	168.192.1.13	20	168.192.1.20
7	168.192.1.7	14	168.192.1.14		

2.35. Практическая работа № 35
Создание резервных копий баз данных

Ознакомление с первичным интерфейсом PRI, выполняющим роль соединительной линии между двумя IP PBX Asterisk.

6.2 Рабочее задание

6.2.1 Соберите схему с использованием шлюзов VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом
3CX Phone.

6.2.2 Присвоить ПК IP-адрес и маску подсети.
6.2.3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
6.2.4 Ознакомиться с выполнением различных процедур и команд.
6.2.5 Подключить мультимедийные приставки в ПК.
6.2.6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу.
6.2.6 Осуществите тестовые звонки между ПК через соединительную линию связи на основе интерфейса PRI.
6.2.7 Составьте отчет о результатах выполнения работы.

6.3 Методические указания по выполнению работы

6.3.1 Современные учрежденческие АТС (УАТС) имеют следующие интерфейсы:

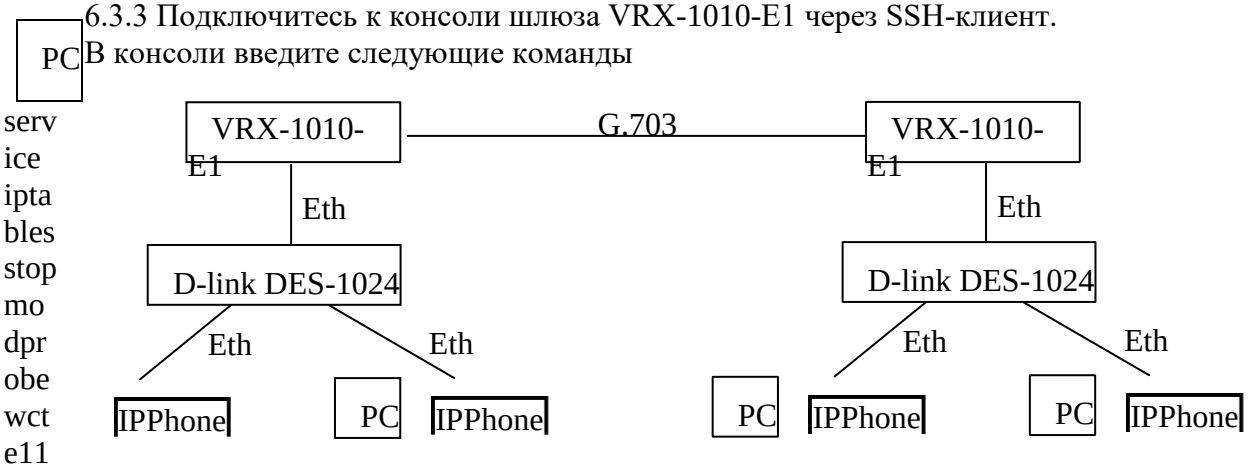
- Z (двухпроводный);
- BRI (основной);
- PRI (первичный);
- E1 (цифровой поток со скоростью 2048 кбит/с) для подключений с другими устройствами.

В свою очередь для связи с сетью передачи данных можно использовать интерфейсы PRI и E1.
Осуществите соединение сетевых устройств в соответствии схемы, представленной на рисунке 6.1.

Рисунок 6.1 – Схема сети

6.3.2 Пропишите на ПК IP-адрес и маску в соответствии с вариантом
(таблица 1.1). В качестве шлюза по умолчанию установите IP-адрес шлюза VRX-1010-E1 (проведите настройки согласно лабораторной работе 1 для каждого шлюза VRX-1010-E1).

6.3.3 Подключитесь к консоли шлюза VRX-1010-E1 через SSH-клиент.
В консоли введите следующие команды




```
service iptables stop
modprobe wcte11xp
dahdi_genconf
```

6.3.4 Приведите содержимое файла /etc/dahdi/system.conf к следующему виду
span=1,1,0,ccs,hdb3,crc4 bchan=1-15,17-31 dchan=16 loadzone=ru defaultzone=ru
6.3.5 В консоли введите следующую команду service dahdi start

6.3.6 Приведите содержимое файла /etc/asterisk/chan_dahdi.conf к следующему виду group=1 context=office echocancel=yes echocancelwhenbridged=no echotraining=yes switchtype=euroisdn signaling=pri_cpe ;pri_net channel => 1-15,17-31
6.3.7 Добавьте в файл /etc/asterisk/extensions.conf следующие строки exten => _9X.,1,Dial(DAHDI/g1/{EXTEN:1}) same => n,HangUp()
6.3.8 В консоли введите следующие команды service asterisk restart asterisk -r
6.3.9 Проверьте статус подсистемы DAHDI, выполнив команды dahdi show status
6.3.10 Выполните тестовые вызовы между ПК на разных шлюзах через префикс 9 (таблица 5.1).
6.3.11 Составьте отчет о результатах выполнения работы.

Таблица 6.1 – Исходные данные

№	SIPадреса	№	SIPадреса	№	SIPадреса	№	SIPадреса
1	1000	6	1005	11	1010	16	1015
2	1001	7	1006	12	1011	17	1016
3	1002	8	1007	13	1012	18	1017
4	1003	9	1008	14	1013	19	1018
5	1004	10	1009	15	1014	20	1019

2.36. Практическая работа № 36
Диагностика и устранение неисправностей в системах IP-телефонии

Ознакомление с настройкой резервирования SIP-транка, транка ISDN PRI в сети с ПО Asterisk при передаче голосовых сигналов.

8.2 Рабочее задание

8.2.1 Соберите схему с использованием шлюзов VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом
3CX Phone.
8.2.2 Присвоить ПК IP-адрес и маску подсети.
8.2.3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
8.2.4 Ознакомиться с выполнением различных процедур и команд.
8.2.5 Подключить мультимедийные приставки в ПК.
8.2.6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу.
8.2.7 Осуществите тестовые звонки между ПК с помощью сигнального протокола по соединительной линии связи на основе интерфейса PRI.
8.2.8 Составьте отчет о результатах выполнения работы.

8.4 Методические указания по выполнению работы

8.4.1 Соберите схему согласно рисунку 8.1

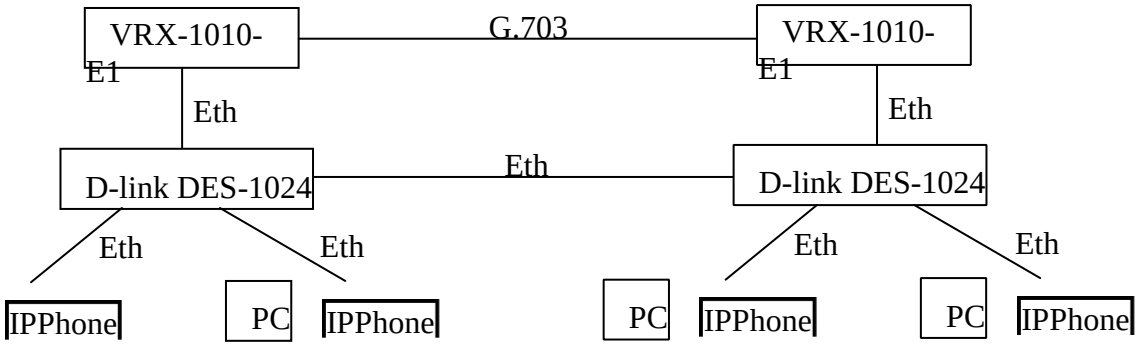
Рисунок 8.1 – Схема сети

8.4.2 Проведите настройки согласно лабораторной работе 2 для каждого шлюза VRX-1010-E1.

8.4.3 Проведите настройки согласно лабораторной работе 3 для каждого шлюза VRX-1010-E1.

8.4.4 Добавьте в файл /etc/asterisk/extensions.conf следующие строки

PC exten => _8X.,1,Dial(SIP/<X>/{EXTEN:1}) same => n,Dial(DAHDI/g1/{EXTEN:1}) same => n,HangUp() exten => _7X.,1,Dial(DAHDI/g1/{EXTEN:1}) same => n,Dial(SIP/<X>/{EXTEN:1}) same => n,HangUp()



Здесь <X> - имя удаленного шлюза в соответствии с вариантом.

8.4.5 В консоли введите следующую команду

service asterisk restart

8.4.6 Выполните тестовые вызовы между ПК на разных шлюзах через префиксы 7, 8, 9, 0. При этом разъедините каналы E1, Ethernet поочередно.

8.4.7 Составьте отчет о результатах выполнения работы.

Таблица 8.1 – Исходные данные

№	SIP-адреса	№	SIP-адреса	№	SIP-адреса
1	1000 GW1	8	1007 GW2	15	1014 GW1
2	1001 GW2	9	1008 GW1	16	1015 GW2
3	1002 GW1	10	1009 GW2	17	1016 GW1
4	1003 GW2	11	1010 GW1	18	1017 GW2
5	1004 GW1	12	1011 GW2	19	1018 GW1
6	1005 GW2	13	1012 GW1	20	1019 GW2
7	1006 GW1	14	1013 GW2		

2.37. Практическая работа № 37
Эксплуатация систем IP-телефонии

Ознакомление с протоколом SIP, его роль при передаче голосых сигналов.

7.2 Рабочее задание

7.2.1 Соберите схему с использованием шлюзов VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом
3CX Phone.
7.2.2 Присвоить ПК IP-адрес и маску подсети.
7.2.3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
7.2.4 Ознакомиться с выполнением различных процедур и команд.
7.2.5 Подключить мультимедийные приставки в ПК.
7.2.6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу.
7.2.6 Осуществите тестовые звонки между ПК с помощью сигнального протокола по соединительной линии связи на основе интерфейса PRI.
7.2.7 Составьте отчет о результатах выполнения работы.

7.3 Методические указания по выполнению работы

7.3.1 Соберите схему согласно рисунку 7.1.
7.3.2 Проведите настройки согласно лабораторной работе 5 для каждого шлюза VRX-1010-E1.
7.3.3 Добавьте в файл /etc/asterisk/sip.conf следующие строки:
[<X>] type=peer dtmfmode=rfc2833 host=<remoteIP> secret=<pass> context=office Здесь <X> - имя удаленного шлюза в соответствии с вариантом,
<remoteIP> - IP-адрес удаленного шлюза, <pass> - общий с удаленным шлюзом пароль.

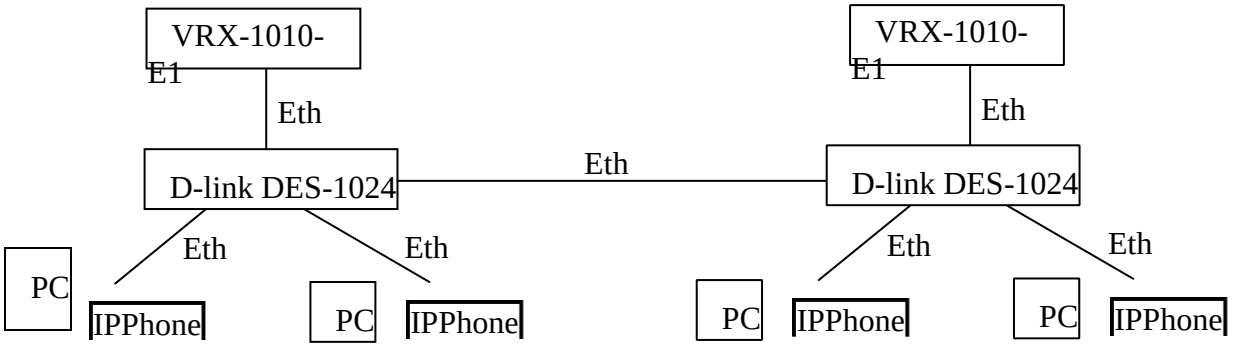


Рисунок 7.1 – Схема сети

7.3.4 Добавьте в файл /etc/asterisk/extensions.conf следующие строки
exten => _0X.,1,Dial(SIP/<X>/{EXTEN:1}) same => n,HangUp()

Здесь <X> - имя удаленного шлюза в соответствии с вариантом.
7.3.5 В консоли введите следующую команду service asterisk restart
7.3.6 Выполните тестовые вызовы между ПК на разных шлюзах через префикс 0 (таблица 6.1).
7.3.7 Составьте отчет о результатах выполнения работы.

Таблица 7.1 – Исходные данные

№	SIP-адреса	№	SIP-адреса	№	SIP-адреса
1	1000 GW1	8	1007 GW2	15	1014 GW1

2	1001 GW2	9	1008 GW1	16	1015 GW2
3	1002 GW1	10	1009 GW2	17	1016 GW1
4	1003 GW2	11	1010 GW1	18	1017 GW2
5	1004 GW1	12	1011 GW2	19	1018 GW1
6	1005 GW2	13	1012 GW1	20	1019 GW2
7	1006 GW1	14	1013 GW2		

2.38. Практическая работа № 38
Обследование и модернизация сетевой инфраструктуры

Компьютерная сеть – совокупность программных и аппаратных средств и среды передачи, служащая для обмена информацией между участниками.
Локальная сеть – система для непосредственного соединения многих компьютеров. При этом подразумевается, что информация передается от компьютера к компьютеру без каких–либо посредников и по единой среде передачи. Однако говорить о единой среде передачи в современной локальной сети не приходится. Например, в пределах одной сети могут использоваться как электрические кабели различных типов (витая пара, коаксиальный кабель), так и оптоволоконные кабели.
Определение передачи «без посредников» также не корректно, ведь в современных локальных сетях используются репитеры, трансиверы, концентраторы, коммутаторы, маршрутизаторы, мосты, которые порой производят довольно сложную обработку передаваемой информации. Не совсем понятно, можно ли считать их посредниками или нет, можно ли считать подобную сеть локальной. Из этого можно сделать вывод, что компьютеры, связанные локальной сетью, объединяются, в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер.
Сформулировать отличительные признаки локальной сети можно следующим образом:
1Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость сейчас – не менее 10 Мбит/с.
Низкий уровень ошибок передачи (или, что то же самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка 10–8 – 10–12.
Эффективный, быстродействующий механизм управления обменом по сети.
Заранее четко ограниченное количество компьютеров, подключаемых к сети. При таком определении понятно, что глобальные сети отличаются от локальных прежде всего тем, что они рассчитаны на неограниченное число абонентов. Кроме того, они используют (или могут использовать) не слишком качественные каналы связи и сравнительно низкую скорость передачи. А механизм управления обменом в них не может быть гарантированно быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования. Однако сети имеют и довольно существенные недостатки, о которых всегда следует помнить: 1Сеть требует дополнительных, иногда значительных материальных затрат на покупку сетевого оборудования, программного обеспечения, на прокладку соединительных кабелей и обучение персонала.
Сеть требует приема на работу специалиста (администратора сети), который будет заниматься контролем работы сети, ее модернизацией, управлением доступом к ресурсам, устранением возможных неисправностей, защитой информации и резервным копированием. Для больших сетей может понадобиться целая бригада администраторов.

Сеть ограничивает возможности перемещения компьютеров, подключенных к ней, так как при этом может понадобиться перекладка соединительных кабелей.
Сети представляют собой прекрасную среду для распространения компьютерных вирусов, поэтому вопросам защиты от них придется уделять гораздо больше внимания, чем в случае автономного использования компьютеров. Ведь достаточно инфицировать один и все компьютеры сети будут поражены.
Сеть резко повышает опасность несанкционированного доступа к информации с целью ее кражи или уничтожения, Информационная защита требует проведения целого комплекса технических и организационных мероприятий.
Здесь же следует упомянуть о таких важнейших понятиях теории сетей, как абонент, сервер, клиент. Абонент (узел, хост, станция) – это устройство, подключенное к сети и активно участвующее в информационном обмене.
Чаще всего абонентом (узлом) сети является компьютер, но абонентом также может быть, например, сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети. Далее в тексте книги вместо термина «абонент» для простоты будет использоваться термин «компьютер».
Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует их ресурсы. Таким образом, он обслуживает сеть. Серверов в сети может быть несколько, и совсем не обязательно, что сервер – самый мощный компьютер. Выделенный (dedicated) сервер – это сервер, занимающийся только сетевыми задачами. Невыделенный сервер может помимо обслуживания сети выполнять и другие задачи. Специфический тип сервера – это сетевой принтер.
Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает, а он ей только пользуется. Компьютер–клиент также часто называют рабочей станцией. В принципе каждый компьютер может быть одновременно как клиентом, так и сервером.
Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами – клиентом

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

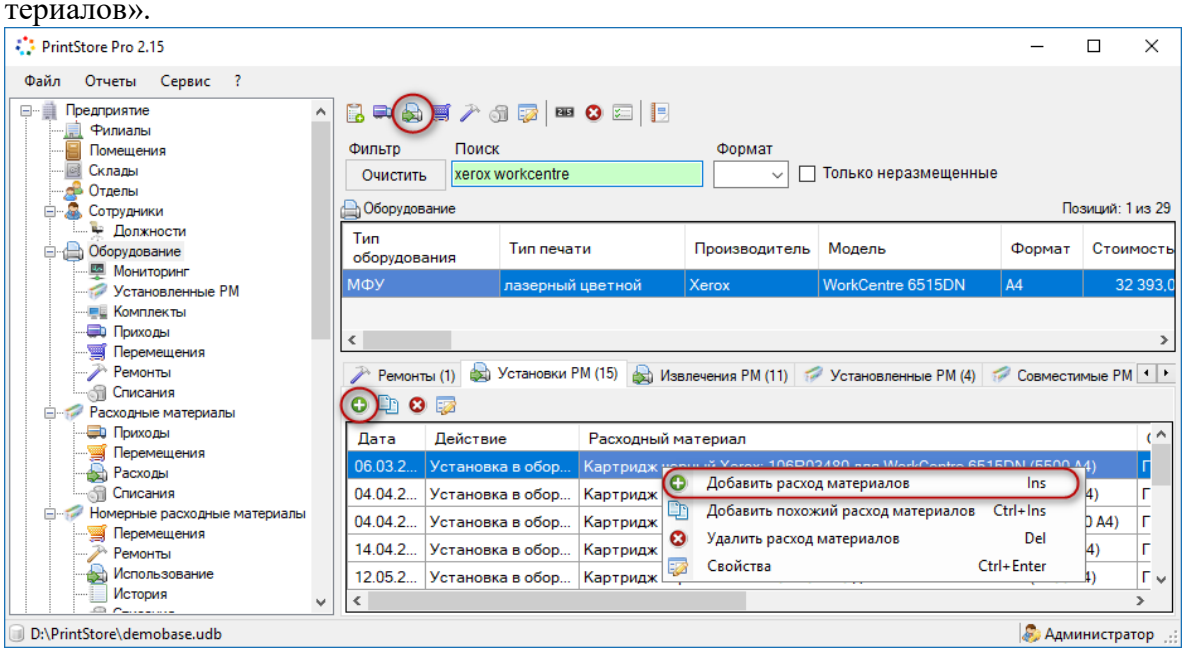
Выполните задания

Построить схему сети и ее модель с указанием топологии сетей и стандартов линий связи. Основными критерием выбора должны быть: экономичность и достаточная пропускная способность. Разрешается, при необходимости, использовать дополнительное аппаратное обеспечение и дополнительные компьютеры. Сеть техникума должна объединить: Корпус №1: администрацию, компьютерный класс «А» на 15 рабочих мест, компьютерный класс «Б» на 15 рабочих мест. Персональный компьютер в преподавательской №1. Корпус №2: компьютерный класс «В» на 15 рабочих мест. компьютерный класс «Г» на 30 рабочих мест. Персональный компьютер в преподавательской №2. Два персональных компьютера в преподавательской №3.
Предусмотреть выход в Интернет через двух провайдеров.
Объяснить, чем Вы руководствовались при выборе тех или иных элементов сети и указать их преимущества.

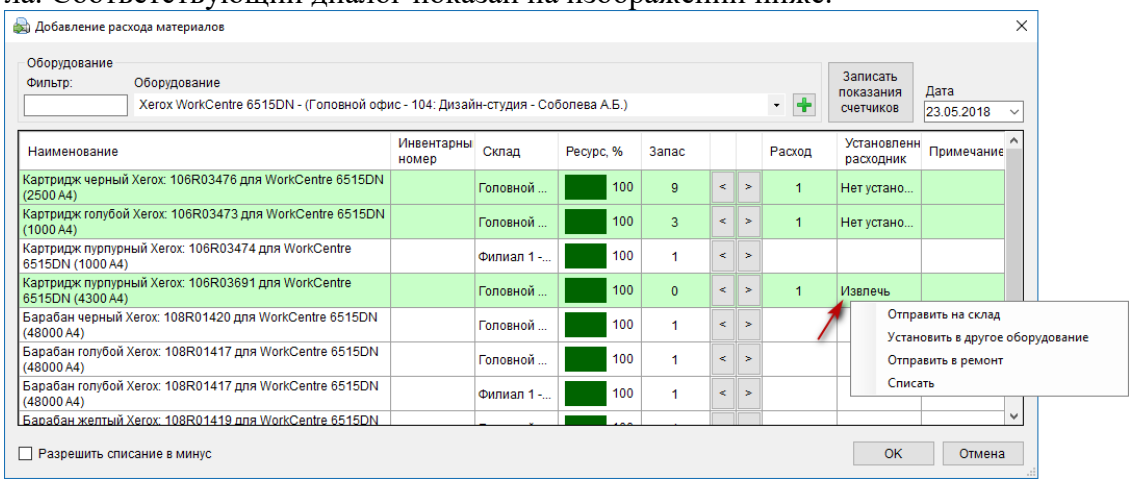
2.39. Практическая работа № 39
Замена расходных материалов и мелкий ремонт периферийного оборудования

Задание
Ознакомиться с специализированным ПО по учету и контролю расходных материалов.

Установка расходных материалов в оборудование
В PrintStore необходимо фиксировать все действия по замене расходных материалов в оборудовании. Важно, чтобы данные об установленных в печатных устройствах расходниках соответствовали действительности. В этом случае программа сможет отображать актуальную информацию о материалах, используемых в оборудовании на текущий момент, и корректно рассчитывать остаток ресурса в них, например, запас чернил (тонера) в каждом картридже.
Запись об установке расходного материала в оборудование можно добавить в нескольких разделах программы: «Оборудование», «Расходные материалы», «Номерные расходные материалы», а также на соответствующих закладках. Удобнее всего оформлять установку расходника в конкретное устройство через раздел «Оборудование» и на закладке «Установки РМ» данного раздела. Для этого следует выделить в таблице нужное устройство (принтер, МФУ и т.п.) и выбрать кнопку / команду «Добавить расход материалов».



Установка в оборудование учитывается, как расход, использование материала. Соответствующий диалог показан на изображении ниже.

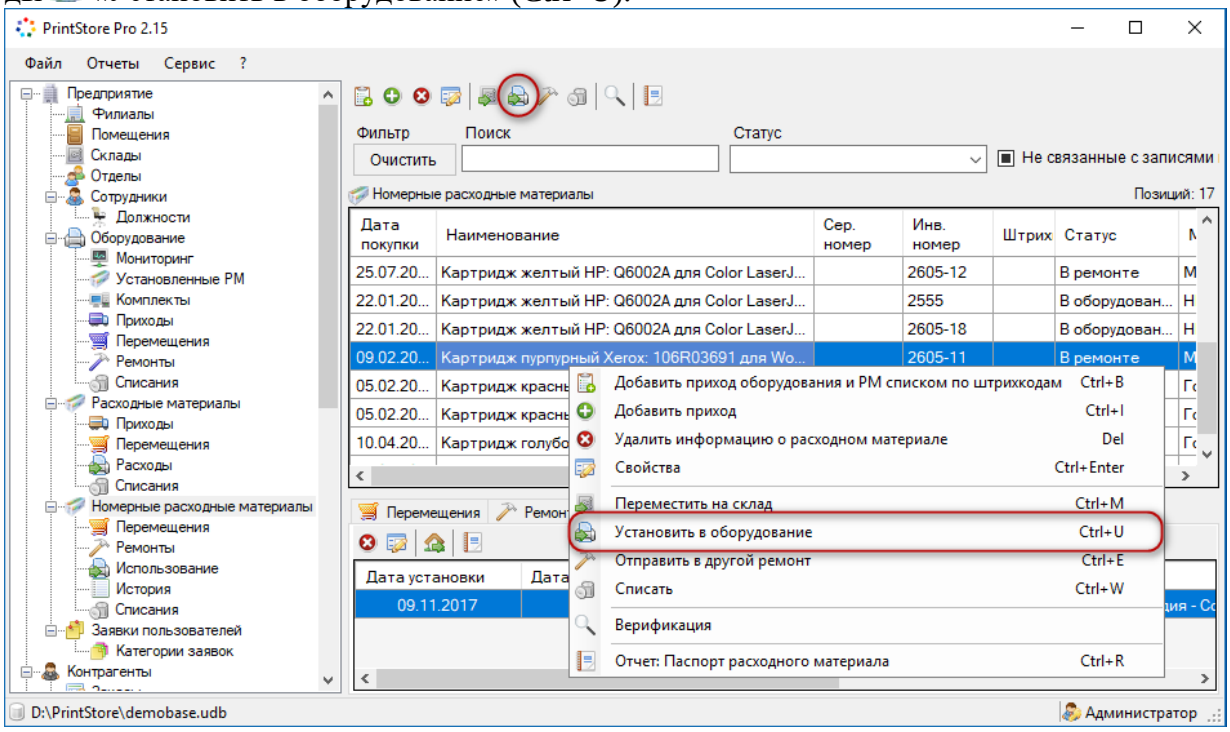


Программа автоматически учитывает совместимость расходных материалов с моделью и слотами выбранного устройства и предлагает для установки перечень подходящих ему картриджей и других расходников из имеющихся в наличии. В столбце «Запас» представлена информация об остатках РМ на складах на выбранную дату.
Номерные расходные материалы (НРМ) указаны отдельно в конце списка, у них присутствуют серийные / инвентарные номера. По каждому НРМ отображается текущий остаток ресурса (краски, тонера и т.п.) на выбранную дату. У обычных материалов (не номерных) остаток ресурса всегда равен 100%, т.к. предполагается, что со склада в оборудование всегда устанавливают новые картриджи, а возможность возвращать на склад частично использованные материалы доступна только для НРМ.
Для того чтобы установить расходник в оборудование, необходимо нажать кнопку > напротив соответствующего материала. При установке картриджа в пустой слот в столбце «Установленный расходник» появится подсказка об отсутствии в данном слоте предыдущего РМ — «Нет установленных расходников». В случае замены картриджей **старый расходник должен быть обязательно извлечен из оборудования** следующим образом: в столбце «Установленный расходник» появится кнопка «Извлечь» (отмечена стрелкой на изображении выше), нажав на которую следует выбрать требуемое действие с извлекаемым РМ. Как правило, это списание. Номерной материал также может быть отправлен на склад, установлен в другое устройство или отправлен на перезаправку (в ремонт).
Кнопка «Записать показания счетчиков» позволяет внести в программу текущие значения счетчиков печати у оборудования при замене расходных материалов, например, количество отпечатанных страниц.
По умолчанию установка расходных материалов оформляется на текущую дату. В случае изменения даты соответствующим образом изменятся и значения в столбце «Расход». В нем будет показан расход материалов за выбранный день. При необходимости расход может быть отредактирован «задним числом». Опция «Разрешить списание в минус» позволяет добавлять записи расхода «задним числом» независимо от текущего остатка на складах. Однако следует помнить, что при подобном ведении учета возможны ошибки. Вовремя их обнаружить и исправить помогает процедура верификации.
Обратите внимание, что в программе существует ограничение на одно однотипное действие в день. Т.е. установить картридж в один и тот же слот принтера можно только 1 раз за сутки.

Автоматическое определение замены расходных материалов
Программа может автоматически обнаружить замену расходного материала у оборудования, находящегося в мониторинге, при изменении ресурса установленного РМ в бОльшую сторону. Например, остаток тонера в картридже был 0%, а стал 100%. Для этого должны быть соблюдены несколько условий, которые подробно описаны здесь.
При обнаружении замены РМ в подраздел «Расходные материалы — Расходы» автоматически будет добавлена соответствующая запись о расходе РМ со склада, сопоставленного с данным оборудованием. Сопоставление можно настроить по филиалам, отделам, помещениям и т.д. Например, чтобы при замене РМ в принтерах из бухгалтерии, расход этих РМ автоматически оформлялся с основного склада. Настройка сопоставлений производится в диалоге свойств склада на закладке «Автоматическое списание РМ» (раздел «Склады»).

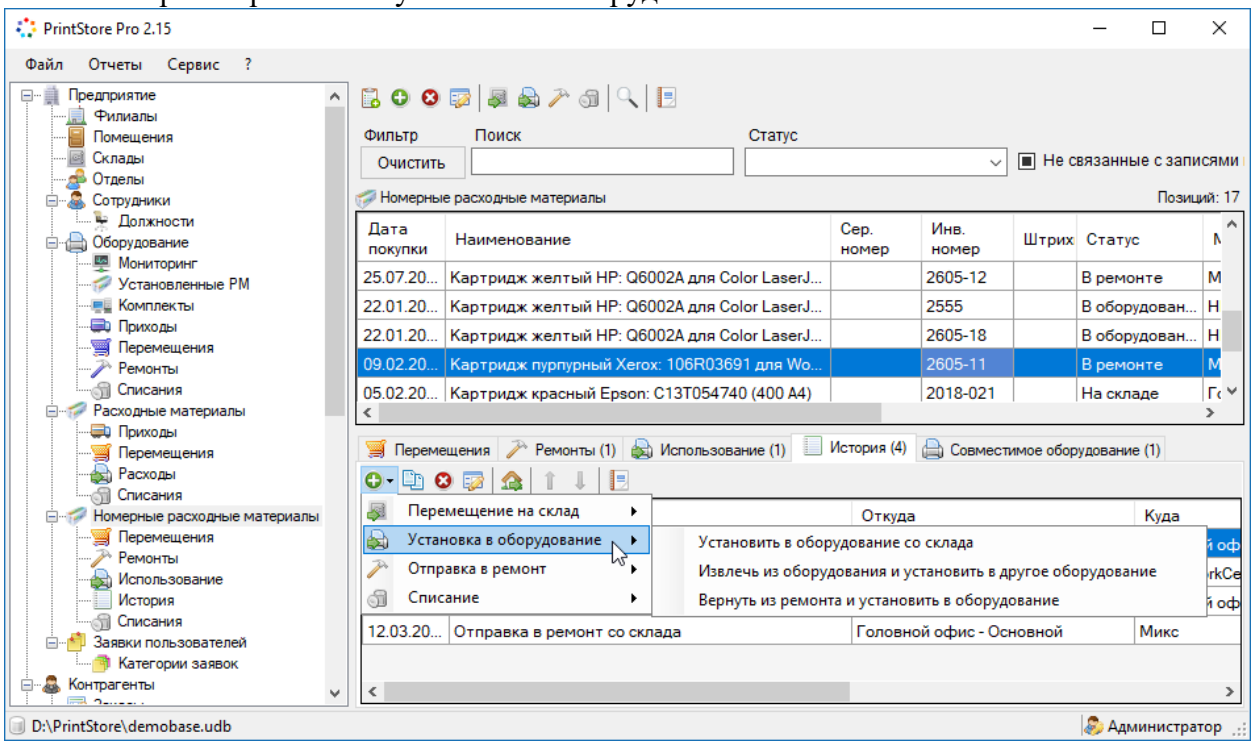
Установка в оборудование номерных материалов
Рассмотренный выше способ установки материалов в оборудование применим как к обычным, так и к номерным расходникам (они представлены в одном диалоге). Однако НРМ может быть установлен в печатное устройство не только со склада, но и после извлечения из другого оборудования или возврата из сервиса. Оформить запись о расхо-

де НРМ можно в разделе «Номерные расходные материалы» с помощью кнопки / команды «Установить в оборудование» (Ctrl+U).



Создать запись о расходе номерного материала также возможно на закладке «История» данного раздела с помощью кнопки / команды «Добавить действие...». Возможные варианты:

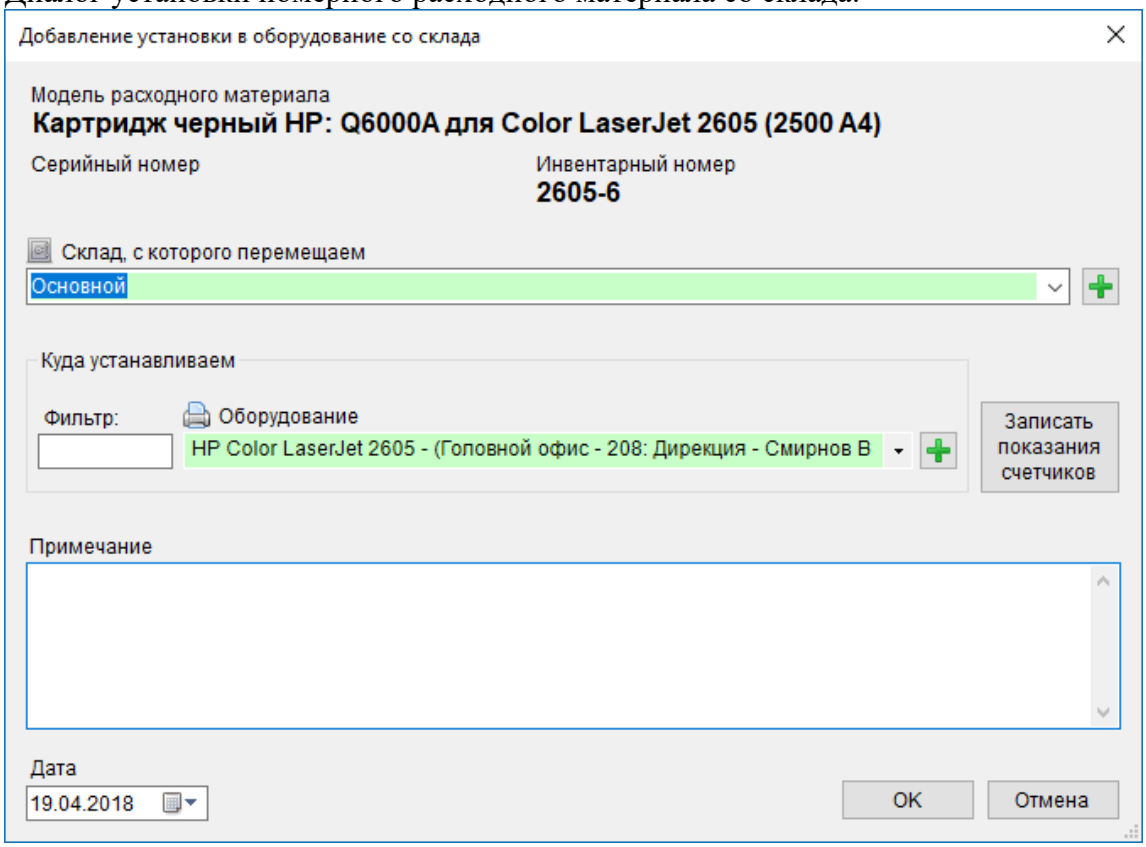
- установка в оборудование со склада;
- извлечение из одного оборудования и установка в другое;
- возврат из ремонта и установка в оборудование.



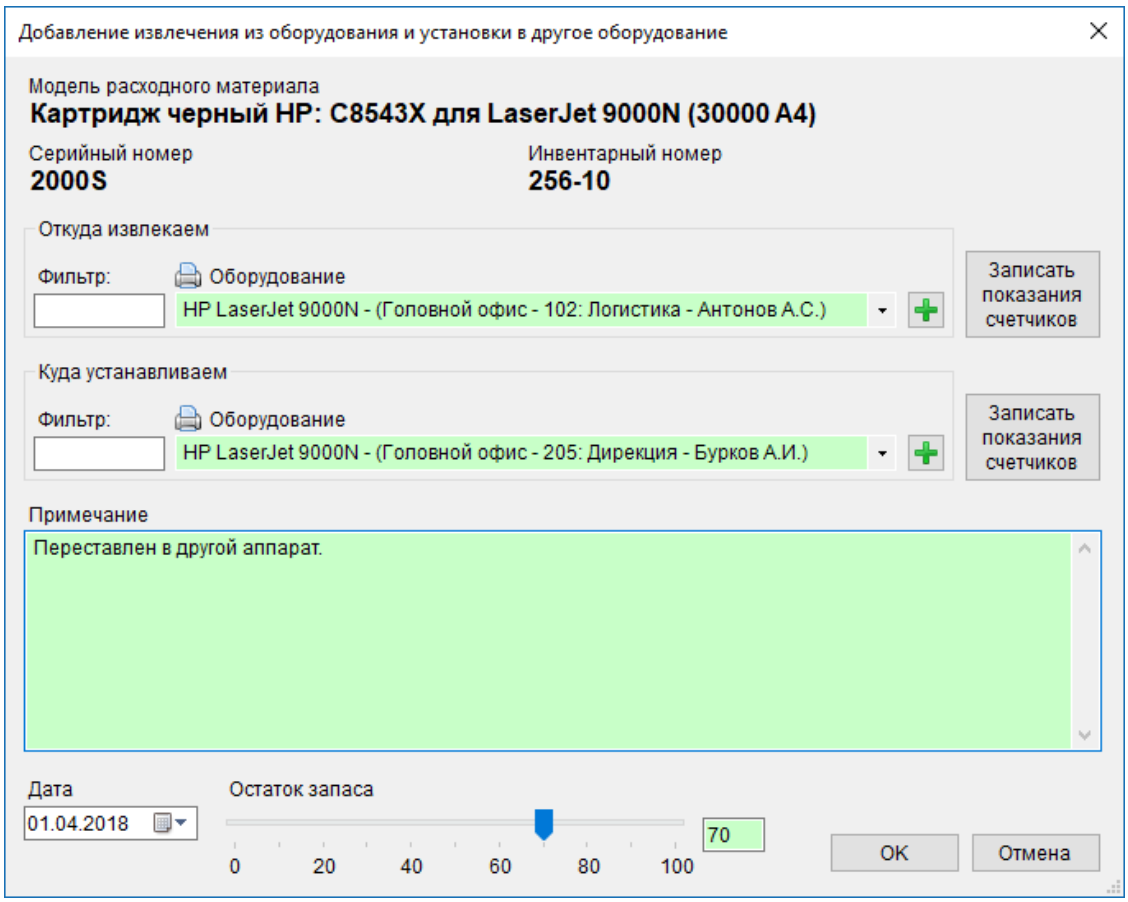
В каждом случае откроется соответствующий диалог, в котором следует выбрать совместимое оборудование для установки расходного материала. По умолчанию установка оформляется текущей датой, которую при необходимости можно изменить. Кнопка «Записать показания счетчиков» в каждом диалоге позволяет внести показания счетчиков

печати у оборудования на момент замены расходника, например, текущее количество отпечатанных страниц.

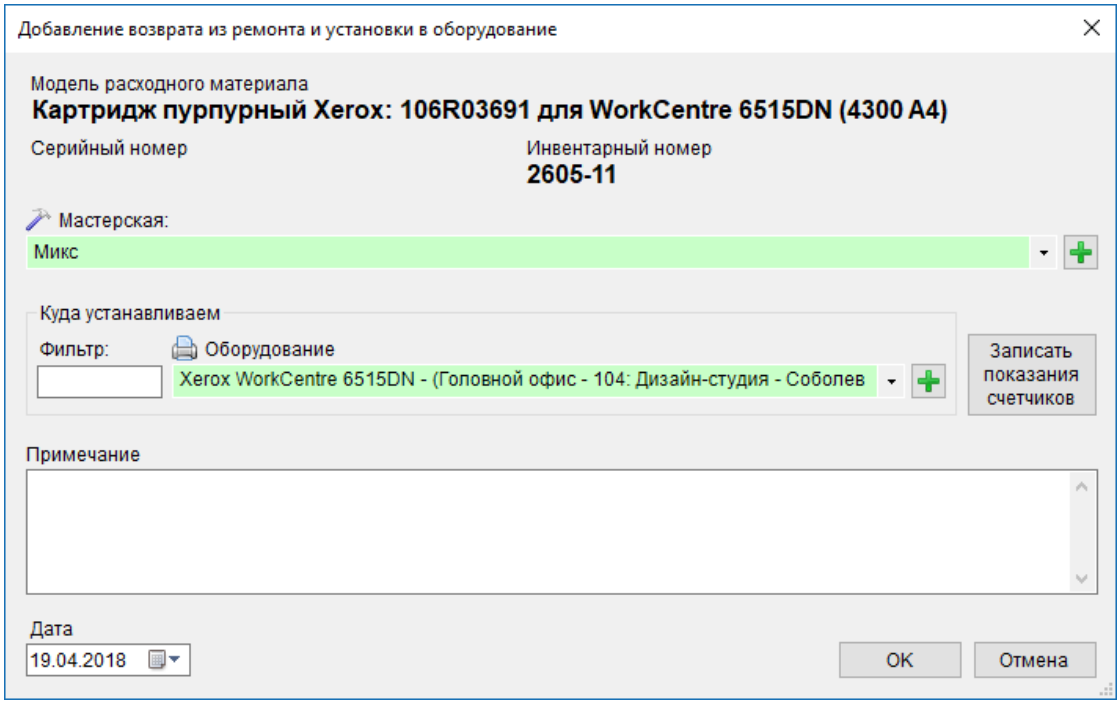
Диалог установки номерного расходного материала со склада.



Диалог извлечения номерного расходного материала из одного оборудования и установки в другое. Имеется возможность указать запас ресурса в НРМ на момент перестановки, например, остаток тонера (чернил) в процентах.



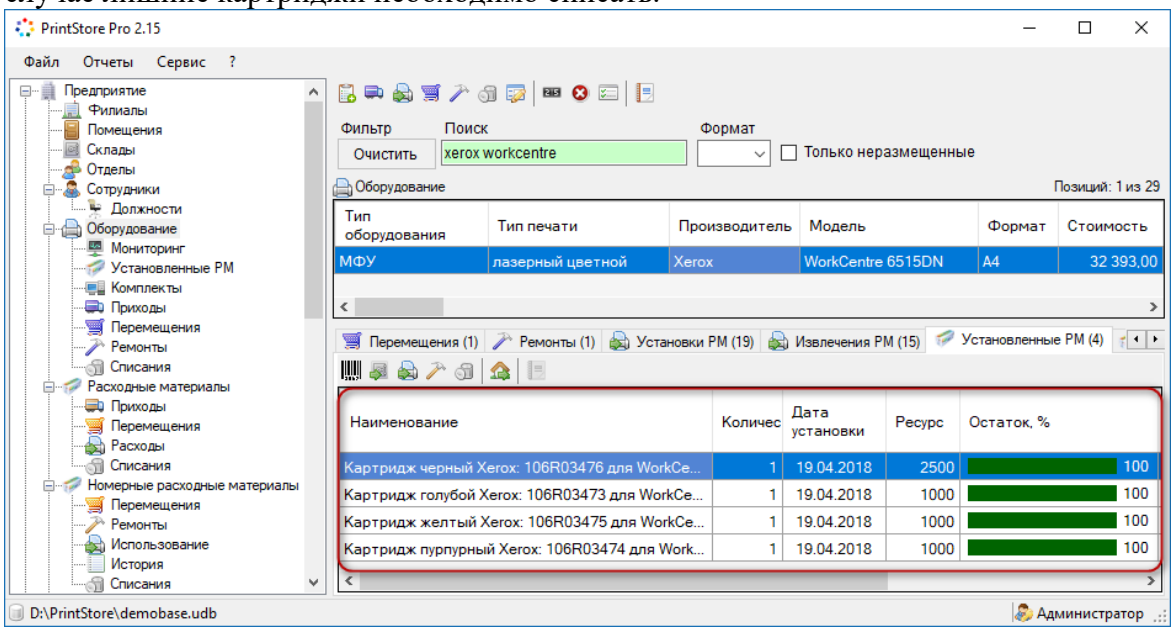
Диалог возврата номерного расходного материала из ремонта и установки в оборудование.



Просмотр установленных материалов

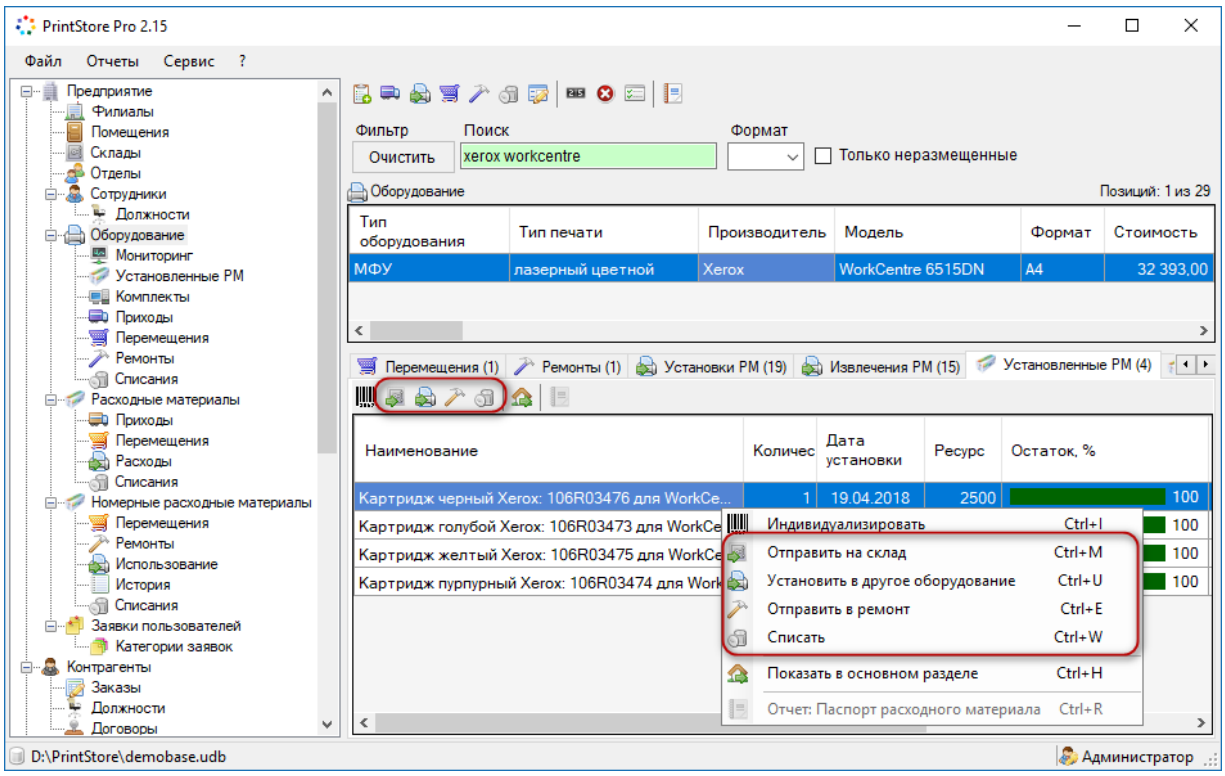
Установленные в конкретное устройство расходные материалы отображаются в разделе «Оборудование» на закладке «Установленные РМ». Расходные материалы у находящегося в мониторинге оборудования можно просмотреть в подразделе «Оборудование — Мониторинг». Перечень всех расходных материалов, установленных в оборудовании предприятия на данный момент, представлен в подразде-

ле «Оборудование — Установленные РМ». По каждому материалу отслеживается скорость расхода и текущий остаток ресурса, например, тонера или чернил.
Обратите внимание, что количество установленных расходных материалов должно соответствовать количеству слотов в данном устройстве. Например, если в принтере 4 слота — для черного, желтого, пурпурного и голубого картриджей, то на закладке «Установленные РМ» по этому устройству должно отображаться 4 картриджа. Если их больше, это означает, что при установке какого-либо картриджа старый не был извлечен. В этом случае лишние картриджи необходимо списать.



Извлечение материалов из оборудования

Установленный в оборудовании материал обычно извлекают при замене расходников. На закладке «Установленные РМ» и в одноименном подразделе раздела «Оборудование» также имеется возможность извлечь расходный материал из оборудования при помощи соответствующих кнопок на панели инструментов и команд контекстного меню. Извлеченный расходник может быть списан, а номерной материал дополнительно отправлен на склад, в сервис или переставлен в другое устройство.



История установок РМ и отчеты

Программа хранит историю установок и извлечений расходных материалов по каждому устройству, которая доступна на закладках «Установки РМ» и «Извлечения РМ» раздела «Оборудование».

История установок по всем расходникам представлена в подразделе «Расходные материалы — Расходы», по номерным материалам — «Номерные расходные материалы — Использование». Статистику использования в оборудовании материалов конкретной модели можно просмотреть на закладке «Расходы материалов» в разделе «Расходные материалы». История установок и извлечений отдельного номерного материала представлена на закладках «Использование» и «История» раздела «Номерные расходные материалы».

При необходимости можно отредактировать или удалить отдельную запись об установке или извлечении материала. В случае удаления записи, установка / извлечение будет отменено.

В программе доступен ряд отчетов по материалам, находящимся в оборудовании. Отчет «Расход материалов» позволяет просмотреть информацию об использовании расходных материалов в оборудовании за указанный период времени. Отчет «Номерные расходные материалы в оборудовании» содержит перечень НРМ, которые на текущий момент установлены в оборудовании. Наконец, в отчете «Использование номерных расходных материалов» представлена история установок и извлечений номерных материалов за выбранный период времени.

При просмотре записей об использовании материалов и отчетов действуют настройки доступа текущего пользователя программы. Если пользователю ограничен просмотр информации отдельных филиалов, то эта информация не отображается.