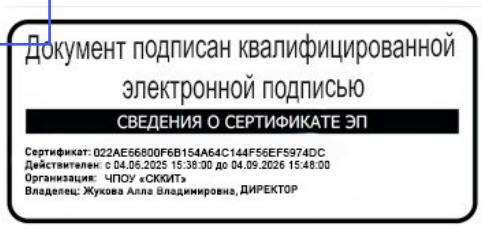
Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрена и утверждена
на Педагогическом совете
от 19.03.2026 Протокол № 03



УТВЕРЖДАЮ
Директор ЧПОУ
«СККИТ»
А.В. Жукова
«19» марта 2026

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Согласовано:
Заместитель директора по учебно - методической работе Л.И. Макарова

Составитель:
Руководитель объединения инноваций и сетевого и системного администрирования В.М. Жукова

Пятигорск-2026

Рабочая программа учебной дисциплины Эксплуатация объектов сетевой инфраструктуры разработана в соответствии с

- Приказом Минпросвещения Российской Федерации от 10 июля 2023 года № 519 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование»

Укрупненная группа специальности: 09.00.00 Информатика и вычислительная техника

Организация-разработчик: Частное профессиональное образовательное учреждение «Северо-Кавказский колледж инновационных технологий»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ЭКОНОМИКА ОТРАСЛИ

1.1. Область применения программы

Рабочая программа учебной дисциплины ОП.15 Эксплуатация объектов сетевой инфраструктуры является частью образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, квалификация – Системный администратор.

1.2 Место программы учебной дисциплины в структуре образовательной программы:

Дисциплина входит в общепрофессиональный цикл дисциплин (ОП.15) образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.3. Результаты освоения программы учебной дисциплины:

В рамках программы учебной дисциплины формируются следующие компетенции:

Код и название компетенции	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать	номенклатура информационных источников, применяемых в профессиональной деятельно-сти; приемы

информационные технологии для выполнения задач профессиональной деятельности	получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	структурирования информации; формат оформления результатов поиска информации
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятель-ности	психологические основы деятельности кол-лектива, психологические особенности лично-сти; основы проектной деятельности
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных

		систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.
ПК 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем управления ремонтом и обслуживанием Типовые сроки проведения профилактического ремонта Правила и процедуры проведения

		инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем программы учебной дисциплины и виды работы

Вид учебной работы	Объем в академических часах очная форма обучения	Объем в академических часах заочная форма обучения
Объем учебной дисциплины	184	184
в том числе реализуемый в форме практической подготовки	146	10
в том числе из объема учебной дисциплины:		
Теоретическое обучение	30	4
Практические занятия (если предусмотрено)	146	10
Самостоятельная работа (если предусмотрена)	8	170
Промежуточная аттестация/ Форма контроля	Экзамен	Экзамен

2.2. Тематический план и содержание программы учебной дисциплины

Наименование разделов и тем	Формы организации учебной деятельности обучающихся	Содержание форм организации учебной деятельности обучающихся	Объем часов (очная форма)	Объем часов (заочная форма)	Наименование синхронизированных образовательных результатов (только коды)	Уровень освоения
1	2	3	4	5	6	7
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	Теоретическое обучение	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. 2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки. 3. Полоса пропускания, паразитная нагрузка. 4. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб). 5. Наращивание длины сегментов сети; замена существующей аппаратуры. 6. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети. 7. Техническая и проектная документация. Паспорт технических устройств. 8. Физическая карта всей сети; логическая топология компьютерной сети. 9. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. 10. Проверка объектов сетевой	15	2	ОК 01,02,04,09 ПК 1.2,1.3,1.7	1

		инфраструктуры и профилактические работы 11. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках. 12. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. 13. Протокол SNMP, его характеристики, формат сообщений, набор услуг. 14. Задачи управления: анализ производительности и надежности сети. 15. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	73			
	Практическое занятие	**(в том числе в форме практической подготовки)** **Выполнение практических заданий:** 1. Оконцовка кабеля витая пара 2. Заделка кабеля витая пара в розетку 3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену 4. Тестирование кабеля 5. Поддержка пользователей сети. 6. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы) 7. Выполнение действий по устранению неисправностей 8. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.		5		2

		9. Оформление технической документации, правила оформления документов 10. Протокол управления SNMP 11. Основные характеристики протокола SNMP 12. Набор услуг (PDU) протокола SNMP 13. Формат сообщений SNMP 14. Задачи управления: анализ производительности сети 15. Задачи управления: анализ надежности сети 16. Управление безопасностью в сети. 17. Учет трафика в сети 18. Средства мониторинга компьютерных сетей 19. Средства анализа сети с помощью команд сетевой операционной системы 20. Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры. Опрос, тестовые задания, упражнения	4			
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом		85		3
Тема 1.2. Эксплуатация систем IP-телефонии	Теоретическое обучение	1. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости. 2. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP.	15	2	ОК 01,02,04,09 ПК 1.2,1.3,1.7	1

		Адресация SIP. Модель установления соединения. Планирование отказоустойчивости. 3. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация. 4. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP-абоненты. Группы абонентов. Дополнительные абонентские услуги. 5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт. 6. Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	73			
	Практическое занятие	**(в том числе в форме практической подготовки)** **Практические задания:** 1. Настройка аппаратных IP-телефонов 2. Настройка программных IP-телефонов, факсов 3. Развертывание сети с использованием VLAN для IP-телефонии		5		2

		4. Настройка шлюза 5. Установка, подключение и первоначальные настройки голосового маршрутизатора 6. Настройка таблицы пользователей в голосовом маршрутизаторе 7. Настройка групп в голосовом маршрутизаторе 8. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе 9. Настройка голосовых сообщений в маршрутизаторе 10. Настройка программно-аппаратной IP-АТС 11. Установка и настройка программной IP-АТС (например, Asterisk) 12. Тестирование кодеков. Исследование параметров качества обслуживания 13. Мониторинг и анализ соединений по различным протоколам 14. Мониторинг вызовов в программном коммутаторе 15. Создание резервных копий баз данных 16. Диагностика и устранение неисправностей в системах IP-телефонии 17. Финальная комплексная практическая работа по эксплуатации систем IP-телефонии.	4			
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом		85		3
Промежуточная аттестация (или указать формы контроля) – **Экзамен** -						
ИТОГО:			**184**	**184**		-

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – Ознакомительный (узнавание ранее изученных объектов, свойств);
2. – Репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3.– Продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация дисциплины требует наличия Лаборатории

- оснащение лаборатории

№	Наименование оборудования	Техническое описание
I. Специализированная мебель и системы хранения		
	Основное оборудование:	
	Стол ученический	регулируемый по высоте
	Стул ученический	регулируемый по высоте
	Дополнительное оборудование:	
	Магнитно-маркерная доска / флипчарт	модель подходит для письма (рисования) маркерами и для размещения бумажных материалов с помощью магнитов
II. Технические средства		
	Основное оборудование:	
	Сетевой фильтр	с предохранителем
	Интерактивный программно-аппаратный комплекс мобильный или стационарный, программное обеспечение	диагональ интерактивной доски должна составлять не менее 65” дюймов (165,1 см); для монитора персонального компьютера и ноутбука – не менее 15,6” (39,6 см), планшета – 10,5” (26,6 см)[1]
	Лаборатория «Организация и принципы построения компьютерных систем»	- Компьютеров обучающихся – 12 шт - Компьютер преподавателя - 1 шт - Аппаратное обеспечение: 2 сетевые платы, процессор Core i3, оперативная память объемом 8 Гб; HD 500 Gb - Операционная система: Windows - Пакет офисных программ, общего и профессионального назначения: FreeCAD, KiCad, EDA, FidoCadJ, Мой оффис EclipseIDEforJavaEEDevelopers, MicrosoftVisualStudio, AndroidStudio, Web – Appach, Ninja IDE, Gimp, Eclipse, Python, Web Browser – Chrome, Sublime Text 3, Notepad ++ windows и RedOS, Blender, SketchUp. Сервер в лаборатории (аппаратное обеспечение: 2 сетевые платы, 8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом 2 Тб, программное обеспечение: Windows Server 2019, лицензионная антивирусная программа (Kaspersky antivirus) , лицензионная программа восстановления данных (Hetman Partition Recovery), лицензионная

[1] Постановление Главного санитарного врача Российской Федерации от 28 сентября 2020 года N 28 «Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"

		программы по виртуализации (Java 32-64 bits). - Технические средства обучения: Интерактивная доска (IQ BOARD с передвижной подставкой) , Проектор (Epson) - Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа (Cablexpert PP12-0.25M, DEXP), обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-нож, кросс-панель. - Пример проектной документации (обеспечения компьютерных сетей, программирования и баз данных) Лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности - Wireshark - 6 маршрутизаторов (WiFi роутер) -1 Коммутатор с 24 портами Ethernet со скоростью не менее 100 Мб/с и 2 портами Ethernet со скоростью не менее 1000Мб/с - телекоммуникационная стойка (сетевой фильтр на 6 гнезд, источник бесперебойного питания); - 2 беспроводных маршрутизатора Linksys E1200-EE - IP телефоны - 3 шт. - Программно-аппаратные шлюзы безопасности - 2шт. (ПО VipNet Clirnt For Windows 4.x (КС2), VipNet PCI Client 1.x) Интерактивная камера – 1 шт Рециркулятор – 1 шт
	Дополнительное оборудование:	
	Колонки	для воспроизведения звука любой модификации
	Web-камера	любой модификации
III. Демонстрационные учебно-наглядные пособия		
	Основные:	
	нет	нет
	Дополнительные:	
	настенный стенд	отражающий специфику дисциплины

- оснащение помещений, задействованных при организации самостоятельной и воспитательной работы:

помещения для организации самостоятельной и воспитательной работы должны быть оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

3.2. Требования к учебно-методическому обеспечению

Учебно-методический материал по профессиональному модулювключает: лекции; перечень практических занятий, практические задания, тестовые задания, упражнения, перечень вопросов к текущему контролю и промежуточной аттестации.

3.3. Интернет-ресурсы

https://rkn.gov.ru/?ysclid=kzax21zwwl Роскомнадзор РФ
https://digital.gov.ru/ru/?utm_referrer=https%3a%2f%2fyandex.ru%2f Министерство цифрового развития связи и массовых коммуникаций Российской Федерации
http://www.ras.ru/ Российская академия наук

3.4. Программное обеспечение, цифровые инструменты

Колледж обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Используются программы, входящие в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также реестр социальных соцсетей:«Яндекс.Диск (для Windows)», Яндекс.Почта, Power Point, ВКонтакте (vk.com), Вебинар.ру

3.5. Основная печатная или электронная литература

1.Урбанович П.П. Компьютерные сети: учебное пособие / Урбанович П.П., Романенко Д.М.. — Москва, Вологда: Инфра-Инженерия,2022.— 460с.—ISBN978-5-9729-0962-9.— Текст: электронный // IPRSMART : [сайт]. — URL: https://www.iprbookshop.ru/124197.html
2.Компьютерные сети и телекоммуникации: учебное пособие для СПО /. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022 . —103с.—ISBN978-5-4488-1445-7,978-5-4497-1445-9. — Текст:электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/115695.html

3.6. Дополнительная печатная или электронная литература

1.Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе; перевод И. В. Синицын. — 3-е изд. — Саратов: Профобразование, 2024. — 335 c. — ISBN 978-5-4488-0054-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/145916.html
2.Уймин, А. Г. Компьютерные сети. L2-технологии: практикум для СПО / А. Г. Уймин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. — 190 c. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/135231.html

3.7. Словари, справочники, энциклопедии, периодические материалы (журналы и газеты)

1.Терминологический словарь по предметам кафедры «Бизнес- информатика» / составители Я. А. Донченко [и др.]. — Симферополь: Университет экономики и управления, 2020. — 240 c. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. —URL: https://www.iprbookshop.ru/108 063.html
2.Шитова, Л. Ф. Digital Idioms = Словарь цифровых идиом / Л. Ф. Шитова. — Санкт-Петербург: Антология, 2021. — 158 c. — ISBN 978-5-94962-216-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/104021.html
3.Журнал Директор информационной службы https://www.iprbookshop.ru/76373.html
4.Журнал Прикладная информатика https://www.iprbookshop.ru/11770.html

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, выполнения практических заданий, написании докладов.

Содержание обучения	**Характеристика основных видов учебной деятельности студентов (на уровне учебных действий)**
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры Тема 1.2. Эксплуатация систем IP-телефонии	Опрос, практические задания, тестовые задания, упражнения

Результаты подготовки обучающихся при освоении рабочей программы учебной дисциплины определяются оценками:

Оценка	**Содержание**	**Проявления**
Неудовлетворительно	Студент не обладает необходимой системой знаний и умений	Обнаруживаются пробелы в знаниях основного программного материала, допускаются принципиальные ошибки в выполнении предусмотренных программой заданий
Удовлетворитель	Уровень оценки результатов обучения показывает, что студенты обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Студенты способны понимать и интерпретировать освоенную информацию, что является основой успешного формирования умений и навыков для решения практикоориентированных задач	Обнаруживаются знания основного программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности (профессии); студент справляется с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя
Хорошо	Уровень осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине; способны анализировать, проводить сравнение и обоснование	Обнаруживается полное знание программного материала; студент, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический

	выбора методов решения заданий в практико-ориентированных ситуациях	характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности
Отлично	Уровень оценки результатов обучения студентов по дисциплине является основой для формирования общих и профессиональных компетенций, соответствующих требованиям ФГОС СПО. Студенты способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях	Обнаруживается всестороннее, систематическое и глубокое знание программного материала, умение свободно выполнять задания, предусмотренные программой; студент, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании программного материала

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрена и утверждена на Педагогическом совете от 19.03.2026 Протокол № 03

УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«19» марта 2026

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Пятигорск- 2026

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

После освоения дисциплины студент должен обладать следующими компетенциями:

Код и название компетенции	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	номенклатура информационных источников, применяемых в профессиональной деятельно-сти; приемы структурирования информации; формат оформления результатов поиска информации
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятель-ности	психологические основы деятельности кол-лектива, психологические особенности лично-сти; основы проектной деятельности
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности

	связные сообщения на знакомые или интересующие профессиональные темы	произношения; правила чтения текстов профессиональной направленности
ПК 1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.
ПК 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем управления ремонтом и обслуживанием

		Типовые сроки проведения профилактического ремонта Правила и процедуры проведения инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

1 ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ

Матрица учебных заданий

№	Наименование темы	Вид контрольного задания
	МДК 03.01 Эксплуатация объектов сетевой инфраструктуры	
1.	Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий. Опрос, тестовые задания, упражнения
2	Тема 1.2. Эксплуатация систем IP-телефонии	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий.

2. ОПИСАНИЕ ОЦЕНОЧНЫХ ПРОЦЕДУР ПО ПРОГРАММЕ

Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры

Вопросы для опроса

1. Что понимается под правилами монтажа?
2. Какими действиями можно добиться значительного уменьшения искажений передаваемых сигналов?
3. Какие требования предъявляются к построению кабельных систем?
4. Какие существуют стандарты кабеля?
5. Опишите виды кабеля витая пара.
6. Какой диаметр у провода стандарта 26AWG?
7. Какой материал используется для изоляции провода, если в маркировки указаны буквы PP? И для какой цели выбран именно этот материал?
8. Опишите рабочие характеристики кабеля 6,5 и 3 категории.
9. Что это BBOSP за тип кабеля? И для каких целей он?
10. Что относится к мерам предосторожности при монтаже кабеля?
11. Какой минимальный радиус изгиба для 4-парного кабеля на основе неэкранированной витой пары проводников (UTP) в состоянии эксплуатации?
12. Какая минимальная сила натяжения для 4-парного кабеля на основе неэкранированной витой пары проводников (UTP)?
13. Какая максимальная длина кабеля между розетками или между розеткой и patch панелью?
14. При монтаже кабельной системы какой рекомендуется предусматривать запас кабеля на основе витой пары проводников ?
15. Какое минимальное расстояние между сетевым кабелем и параллельно ему проложенным силовым кабелем напряжением менее 2 КВольт?

Практическое задание: *Оконцовка кабеля витая пара*

Цель: получить представления о системе стандартов кабелей, разбираться в маркировке кабелей, получитьпервичные знания о монтаже кабеля витой пары
Правила монтажа кабельной системы

1 Общие положения Назначением системы требований и рекомендаций по монтажу кабельных систем является гарантиясохранения исходных рабочих характеристик отдельных компонентов, собранных в линии, каналы исистемы. понимают методы и аккуратность выполнения соединений компонентов и организаций кабельных потоков.

Значительного уменьшения искажений передаваемых сигналов можно добиться при:

использовании специальных методов подготовки кабеля;

терминировании сред передачи на коммутационном оборудовании в соответствии с инструкциямипроизводителя;

упорядочении организации кабельных потоков;

правильном пространственном расположении оборудования;

выполнении правил монтажа и требований производителей к монтажутелекоммуникационногооборудования.

Установленная кабельная система на основе витой пары проводников классифицируется на основаниипроизводительности компонента линии или канала, обладающего наихудшими рабочими характеристикамипередачи.

Требования к построению кабельных систем:

целостность и последовательность в проектировании и монтаже;

гарантия соответствия требованиям к рабочим характеристикам передачи и физическим параметрамлиний;

гарантия возможности выполнения расширения системы и проведения в ней различных изменений;

стандартная схема документирования и администрирования.

Монтаж всех компонентов и элементов СКС должен быть выполнен с соблюдением инструкцийпроизводителя компонентов по монтажу и требований настоящего стандарта.

2 Монтаж кабелей

Кабели на основе витой пары проводников

Сегодня наиболее употребительными стандартами в мировой практике являются следующие:

Американский стандарт EIA/TIA-568A, который был разработан совместными усилиями несколькихорганизаций: ANSI, EIA/TIA и лабораторией Underwriters Labs (UL) .

Стандарт EIA/TIA-568 разработан на основе предыдущей версии стандарта EIA/TIA-568 и дополнений кэтому стандарту TSB-36 и TSB-40A.

Международный стандарт ISO/IEC 11801.

Европейский стандарт EN50173.

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольгивокруг скрученных пар, определяют разновидности данной технологии:

неэкранированная витая пара (англ. UTP — Unshielded twisted pair) — без защитного экрана;фольгированная витая пара (англ. FTP — Foiled twisted pair), также известна как F/UTP) —присутствует один общий внешний экран в виде фольги;

экранированная витая пара (англ. STP — Shielded twisted pair) — присутствует защита в видеэкрана для каждой пары и общий внешний экран в виде сетки;

фольгированная экранированная витая пара (англ. S/FTP — ScreenedFoiledtwistedpair) — внешнийэкран из медной оплетки и каждая пара в фольгированной оплетке;

незащищенная экранированная витая пара (SF/UTP — или с англ. Screened Foiled Unshielded twistedpair).Отличие от других типов витых пар заключается в наличии двойного внешнего экрана,сделанного из медной оплётки, а также фольги. Витопарный кабель состоит из нескольких витыхпар. Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,4—0,6 мм.Кроме метрической, применяется американская система AWG, в которой эти величины составляют26AWG или 22AWG соответственно. В стандартных 4-х парных кабелях в основном используютсяпроводники диаметром 0,51 мм (24AWG). Толщина изоляции проводника — около 0,2 мм, материалобычно

поливинилхлорид (английское сокращение PVC), для более качественных образцов 5категории — полипропилен (PP), полиэтилен (PE). Особенно высококачественные кабели имеютизоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрическиепотери, или тефлона, обеспечивающего широкий рабочий диапазон температур

Рабочие характеристики передачи В СКС используют кабельные компоненты с рабочими характеристикамипередачи следующих категорий: 6 — неэкранированные (UTP) и экранированные (ScTP, FTP, SFTP) кабели на основе витой пары проводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до250 МГц; 5е — неэкранированные (UTP) и экранированные (ScTP, FTP, SFTP) кабели на основе витой пары проводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до 100 МГц; 5 — неэкранированные (UTP) и экранированные (ScTP, FTP) многопарные кабели на основе витой пары проводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до 100 МГц; 3 — неэкранированные (UTP) многопарные кабели на основе витой пары проводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до 16 МГц. • Многопарные кабели на основе витой пары проводников с рабочими характеристиками передачи категорий 3 и 5 могут быть использованы только в магистральных подсистемах СКС для передачи сигналов низкоскоростных приложений (например, аналоговая и цифровая телефония). • Исключение из приведенных выше правил представляют многопарные кабели для внешней прокладки, рабочие характеристики которых обычно не выходят за рамки первого и второго уровней. Такие кабели состоят из одножильных медных проводников калибров 19 AW G (0,9 мм), 22 AW G (0,64 мм), 24 AW G (0,5 мм) или 26 AW G (0,4 мм) в термопластиковой изоляции и предназначены для передачи сигналов приложений передачи речи и низкоскоростных данных (кабели типа OSP) или приложений передачи речи, высокоскоростных данных и видео (широкополосные кабели типа BBOSP) 2.1 Общие положения Рабочие характеристики кабеля и коммутационного оборудования могут существенно изменяться вследствие нарушения правил монтажа и последующих манипуляций с кабельными потоками. Правила монтажа и обслуживания фиксированных кабельных сегментов горизонтальной и магистральной подсистем отличаются от правил организации коммутационных кабелей в кроссах. Кроссировочные соединения предназначены для обеспечения гибкости проведения изменений в схеме коммутации. К мерам предосторожности, соблюдаемым при монтаже и организации кабельных потоков, относится предотвращение различных механических напряжений в кабеле, вызываемых натяжением, резкими изгибами и чрезмерным стягиванием пучков кабелей. При монтаже кабелей в трассах и телек проводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до 100 МГц; 5 —неэкранированные (UTP) и экранированные (ScTP, FTP) многопарные кабели на основе витой парыпроводников с волновым сопротивлением 100 Ом и рабочим диапазоном частот до 100 МГц; 3 —неэкранированные (UTP) многопарные кабели на основе витой пары проводников с волновымопротивлением 100 Ом и рабочим диапазоном частот до 16 МГц.

Многопарные кабели на основе витой пары проводников с рабочими характеристиками передачикатегорий 3 и 5 могут быть использованы только в магистральных подсистемах СКС для передачисигналов низкоскоростных приложений (например, аналоговая и цифровая телефония).

Исключение из приведенных выше правил представляют многопарные кабели для внешней

прокладки, рабочие характеристики которых обычно не выходят за рамки первого и второго

уровней. Такие кабели состоят из одножильных медных проводников калибров 19 AW G (0,9 мм),22 AW G (0,64 мм), 24 AW G (0,5 мм) или 26 AW G (0,4 мм) в термопластиковой изоляции ипредназначены для передачи сигналов приложений передачи речи и

низкоскоростных данных(кабели типа OSP) или приложений передачи речи, высокоскоростных данных и видео(широкополосные кабели типа BBOSP)

2.1 Общие положения

Рабочие характеристики кабеля и коммутационного оборудования могут существенно изменятьсявследствие нарушения правил монтажа и последующих манипуляций с кабельными потоками. Правиламонтажа и обслуживания фиксированных кабельных сегментов горизонтальной и магистральной подсистемотличаются от правил организации коммутационных кабелей в кроссах. Кроссировочные соединенияпредназначены для обеспечения гибкости проведения изменений в схеме коммутации. К мерам предосторожности, соблюдаемым при монтаже и организации кабельных потоков, относитсяпредотвращение различных механических напряжений в кабеле, вызываемых натяжением, резкимиизгибами и чрезмерным стягиванием пучков кабелей. При монтаже кабелей в трассах и телекоммуникационных помещениях следует использовать средства маршрутизации кабельных потоков, их крепления и фиксации. Кабельные хомуты (стяжки, бандаж и т. п.), используемые для формирования кабельных пучков, должнырасполагаться на пучке так, чтобы хомут мог свободно перемещаться в продольном и поперечномнаправлениях. Не допускается затягивание хомутов, приводящее к деформации оболочки кабелей. Не допускается крепление телекоммуникационных кабелей с помощью скоб.

Не допускается использование лифтовых шахт для монтажа кабелей на основе любого разрешенного типасреды передачи.

2.2 Минимальный радиус изгиба

Необходимость сохранения минимального радиуса изгиба кабеля на основе витой пары проводниковобусловлена тем, что при резких изгибах пары внутри кабеля деформируются и нарушается однородностьсимметричной среды передачи. Это ведет, в первую очередь, к серьезным изменениям такого параметра, какNEXT. Последующее распрямление изгиба может не только не восстановить форму пары, но и привести кеще худшим результатам.

Радиусы изгиба кабелей горизонтальной и магистральной подсистем не должны быть менее:

4 внешних диаметров кабеля для 4-парных кабелей на основе неэкранированной витой пары
проводников (UTP) в состоянии эксплуатации;

8 внешних диаметров кабеля для 4-парных кабелей на основе неэкранированной витой пары
проводников (UTP) в процессе монтажа;

8 внешних диаметров кабеля для 4-парных кабелей на основе экранированной витой пары проводников (FTP, ScTP, SFTP) в состоянии эксплуатации;

10 внешних диаметров кабеля для 4-парных кабелей на основе экранированной витой пары
проводников (FTP, ScTP, SFTP) в процессе монтажа;

10 внешних диаметров кабеля для многопарных кабелей на основе витой пары проводников всостоянии эксплуатации;

15 внешних диаметров кабеля для многопарных кабелей на основе витой пары проводников впроцессе монтажа;

25 мм для волоконно-оптических кабелей внутреннего применения с количеством волокон 2 и 4 всостоянии эксплуатации;

50 мм для волоконно-оптических кабелей внутреннего применения с количеством волокон 2 и 4 впроцессе монтажа;

10 внешних диаметров кабеля для волоконно-оптических кабелей внутреннего применения сколичеством волокон более 4 в состоянии эксплуатации;

15 внешних диаметров кабеля для волоконно-оптических кабелей внутреннего применения сколичеством волокон более 4 в процессе монтажа; оммуникационных

помещениях следует использовать средства маршрутизации кабельных потоков, их крепления и фиксации. Кабельные хомуты (стяжки, бандаж и т. п.), используемые для формирования кабельных пучков, должны располагаться на пучке так, чтобы хомут мог свободно перемещаться в продольном и поперечном направлениях. Не допускается затягивание хомутов, приводящее к деформации оболочки кабелей. Не допускается крепление телекоммуникационных кабелей с помощью скоб. Не допускается использование лифтовых шахт для монтажа кабелей на основе любого разрешенного типа среды передачи. 2.2 Минимальный радиус изгиба Необходимость сохранения минимального радиуса изгиба кабеля на основе витой пары проводников обусловлена тем, что при резких изгибах пары внутри кабеля деформируются и нарушается однородность симметричной среды передачи. Это ведет, в первую очередь, к серьезным изменениям такого параметра, как NEXT. Последующее распрямление изгиба может не только не восстановить форму пары, но и привести к еще худшим результатам. Радиусы изгиба кабелей горизонтальной и магистральной подсистем не должны быть менее: • 4 внешних диаметров кабеля для 4-парных кабелей на основе неэкранированной витой пары проводников (UTP) в состоянии эксплуатации; • 8 внешних диаметров кабеля для 4-парных кабелей на основе неэкранированной витой пары проводников (UTP) в процессе монтажа; • 8 внешних диаметров кабеля для 4-парных кабелей на основе экранированной витой пары проводников (FTP, ScTP, SFTP) в состоянии эксплуатации; • 10 внешних диаметров кабеля для 4-парных кабелей на основе экранированной витой пары проводников (FTP, ScTP, SFTP) в процессе монтажа; • 10 внешних диаметров кабеля для многопарных кабелей на основе витой пары проводников в состоянии эксплуатации; • 15 внешних диаметров кабеля для многопарных кабелей на основе витой пары проводников в процессе монтажа; • 25 мм для волоконно-оптических кабелей внутреннего применения с количеством волокон 2 и 4 в состоянии эксплуатации; • 50 мм для волоконно-оптических кабелей внутреннего применения с количеством волокон 2 и 4 в процессе монтажа; • 10 внешних диаметров кабеля для волоконно-оптических кабелей внутреннего применения с количеством волокон более 4 в состоянии эксплуатации; • 15 внешних диаметров кабеля для волоконно-оптических кабелей внутреннего применения с количеством волокон более 4 в процессе монтажа;10 внешних диаметров кабеля для волоконно-оптических кабелей внешнего применения всостоянии эксплуатации;

- 20 внешних диаметров кабеля для волоконно-оптических кабелей внешнего применения в процессемонтажа.

В случае, если требования производителя к минимальному радиусу изгиба конкретного кабеля болеежесткие, чем приведенные выше, они должны быть выполнены.

Для предотвращения возникновения растяжения, резких перегибов и перекручивания шнуров должныиспользоваться специальные средства и приспособления, такие как горизонтальные и вертикальныенаправляющие, устройства, регулирующие длину. В то же время должен быть обеспечен быстрый и простойдоступ к шнурам для внесения изменений в систему коммутации и идентификации соединений.

Рекомендуется поддерживать радиус изгиба коммутационных и аппаратных кабелей (шнуров) в процессеэксплуатации не менее:

- 4 внешних диаметров кабеля —для 4-парных шнуров на основе неэкранированной и экранированной витой пары проводников;
- 25 мм — для волоконно-оптических шнуров.

Для выполнения этих правил рекомендуется использовать специально предназначенные для этих целейсредства, приспособления и устройства.

В общем случаи:

Минимальный радиус изгиба для кабеля - четыре диаметра кабеля (или 1 дюйм=2,5 см), носуществуют рекомендации размещать кабель таким образом, чтобы обеспечивать изгиб радиусом 2дюйма (5 см.).

2.3 Максимальная сила натяжения

При монтаже кабелей и в некоторых случаях в процессе их эксплуатации (вертикальные сегменты) на нихдействуют силы натяжения, способные привести к деформации пар в кабелях на основе витой парыпроводников и механическому повреждению волокон в волоконно-оптических кабелях. Поэтому одним изосновных требований, предъявляемых к монтажу, наряду с соблюдением радиуса изгиба являетсясоблюдение предельно допустимой силы натяжения кабелей. В тех случаях, когда предполагается сложный монтаж с приложением к кабелю повышенных усилий,например при протяжке кабеля через закрытую трассу длиной свыше 30 м или трассу, имеющую более двухповоротов с углами 90°, рекомендуется использовать динамометр или калиброванный вертлюг. После монтажа не должно быть натяжения кабеля за исключением вертикальных сегментов, когда остаточноенатяжение может быть вызвано собственной массой кабеля. Сила натяжения кабелей горизонтальной и магистральной подсистем во время монтажа и в процессеэксплуатации не должна быть более:

- 110 Н—для 4-парных кабелей на основе неэкранированной и экранированной витой парыпроводников;
- спецификации производителя —для многопарных кабелей на основе витой пары проводников;
- 220 Н или спецификации производителя в случае, если они более жесткие для волоконнооптических кабелей внутреннего применения с количеством волокон 2 и 4;
- спецификации производителя —для волоконно-оптических кабелей внутреннего применения сколичеством волокон более 4;
- 2700 Н или спецификации производителя в случае, если они более жесткие для волоконнооптических кабелей внешнего применения.

2.4 Запас кабеля

При монтаже кабельной системы рекомендуется предусматривать создание запаса кабеля на обоих концахкабельных сегментов с целью обеспечения возможности внесения изменений в будущем. Рекомендуется
оставлять следующий запас кабеля в TR, ER и EF:

- кабель на основе витой пары проводников — 3 м;
- волоконно-оптический кабель — 3 м; на WA:
- кабель на основе витой пары проводников — 0,3 м;
- волоконно-оптический кабель—1 м.

Запас кабеля должен учитываться в общей длине сегментов горизонтальной и магистральной кабельныхподсистем.

Предпочтительно запас делать в виде «U»-образных петель с соблюдением минимального радиуса изгиба.Петли в виде «8» с большим радиусом также могут обеспечить хорошие результаты. Не рекомендуетсяделать запас кабеля в виде бухты небольшого диаметра (до 30 см).

В общем случаи:

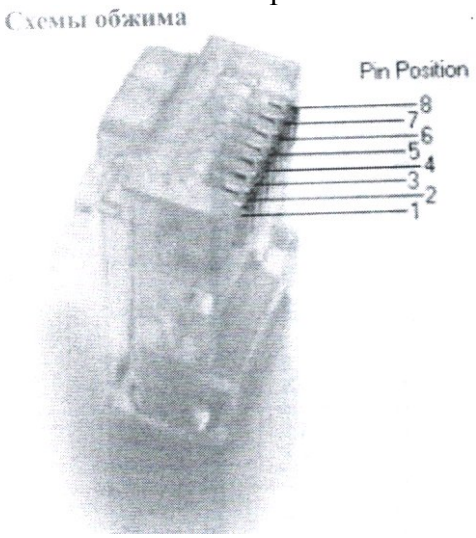
Максимальная длина кабеля между розетками или между розеткой и patch панелью - 90 метров. Этоправило разработано исходя из ограничения максимального расстояния в 100 метров между DTE(компьютер) и хабом.

Запас волоконно-оптического кабеля может быть выполнен как в оболочке, так и отдельными волокнамипри условии обеспечения их адекватными мерами защиты. При этом должны быть выполнены требования кдопустимым радиусам изгиба и силе натяжения. Запас кабеля может быть создан в специальныхконтейнерах или на стенах телекоммуникационных помещений. Хранение запаса волокон допускаетсятолько в специальных защитных контейнерах.

Минимальное расстояние между сетевым кабелем и параллельно ему проложенным силовымкабелем

В общем случаи:

Минимальное расстояние между сетевым кабелем и параллельно ему проложенным силовымкабелем напряжением менее 2 КВольт - 12,5 сантиметров (5 дюймов).



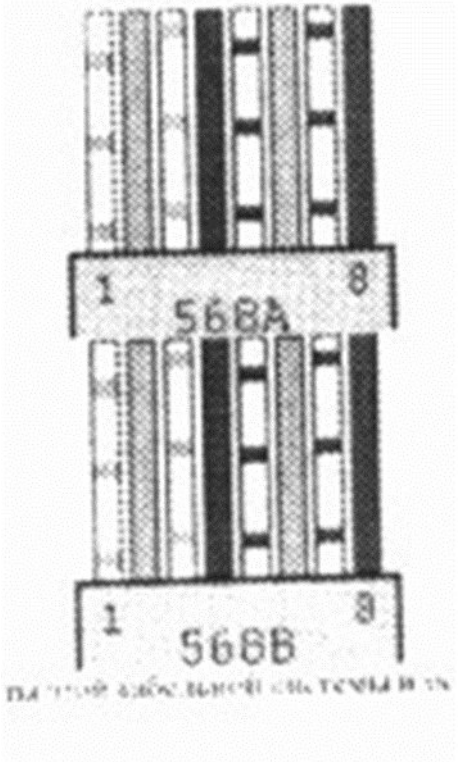
Нумерация в штекере 8P8C

Существует два варианта обжима разъёма на кабеле:

- для создания прямого кабеля — для соединения порта сетевой карты с коммутатором иликонцентратором,
- для создания перекрёстного (использующего кроссированный MDI, англ. MDI-X) кабеля, имеющегоинвертированную разводку контактов разъёма для соединения напрямую двух сетевых плат,

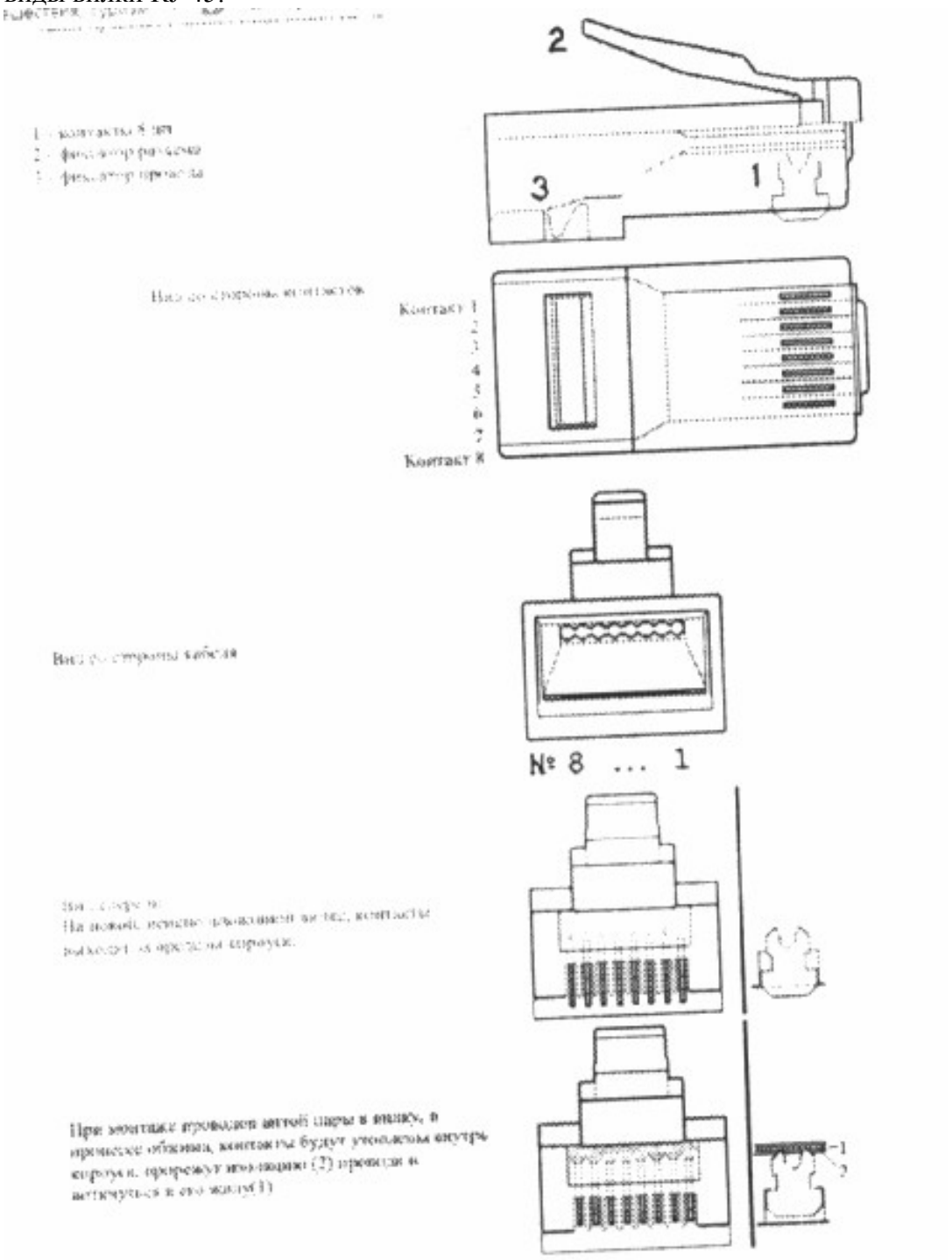
установленных в компьютеры, а также для соединения некоторых старых моделей концентраторовили коммутаторов (uplink-порт).

Обжимается разъём RJ45.разводка проводов UTP действующего стандарта EIA-568A.

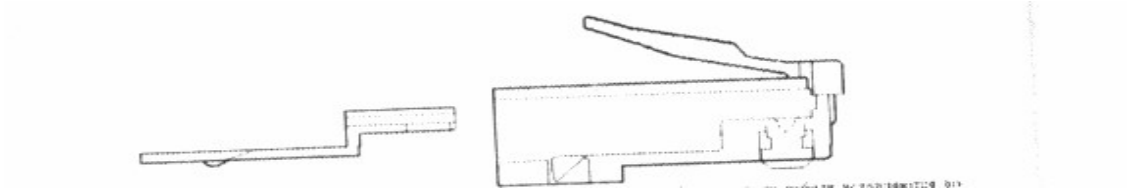


Давайте сейчас рассмотри компоненты этой кабельной системы и основные приемы монтажа витой пары. Соединители (connectors). Для подключения витой пары к компьютеру используются телефонные коннекторы RJ-45. На первый взгляд, они похожи на RJ-11, но в действительности между ними есть существенные отличия. Во-первых, вилка RJ-45 чуть больше по размерам и не подходит для гнезда RJ- 11. Во- вторых,

коннектор RJ-45 имеет восемь контактов, а RJ-11 - только четыре. Ниже приведен главные виды вилки RJ-45:

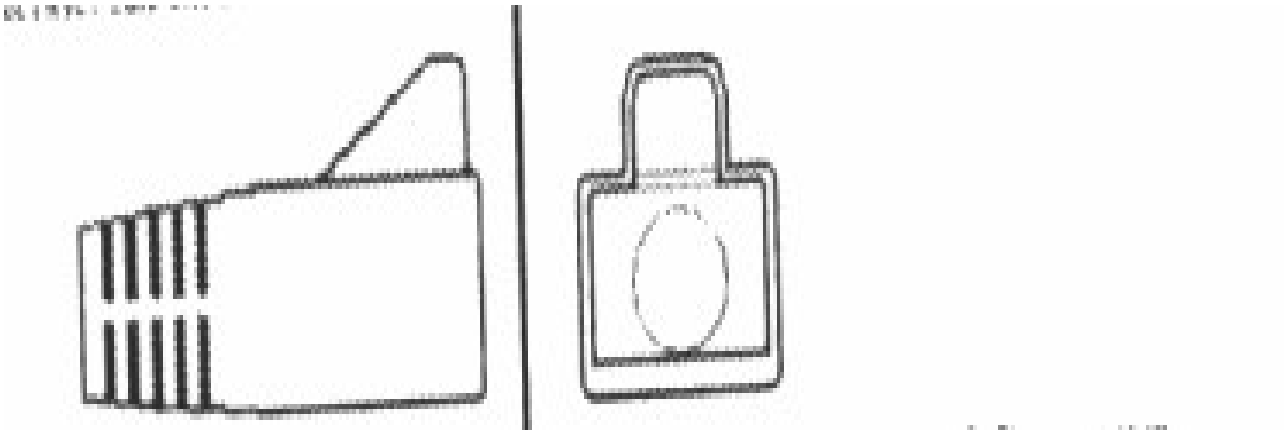


Есть другой тип вилки RJ-45 - вилка со вставкой:

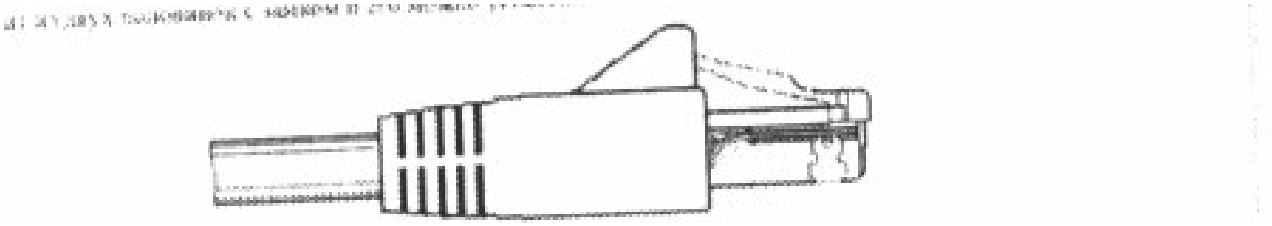


Расплетенные и расположенные в соответствии с выбранным способом, провода кабеля вставляются во вставку до упора, лишнее обрезается, затем вставка вместе с кабелем вставляется в вилку. Вилка обжимается. При данном способе монтажа длина расплетения

получается минимальной, монтаж проще и быстрее, чем при использовании обычной вилки без вставки. Но такая вилка несколько дороже чем обычная. Для вилки RJ-45 существует еще специальный защитный колпачок.

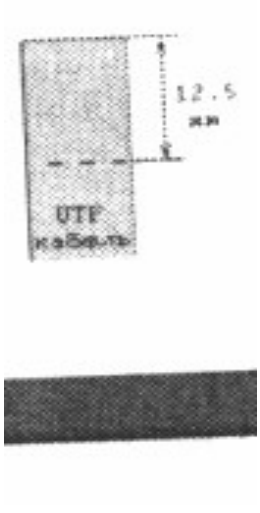


Он нужен для защиты кабеля от возможного переломления в месте крепления вилки RJ-45. Выпускается различных цветов, что удобно для маркировки кабеля и бывает как разборного, так и неразборного типа. Колпачок неразборного типа необходимо надевать на кабель до установки вилки. Разборный колпачок состоит из двух половинок с замком и его можно установить после монтажа вилки на кабель.

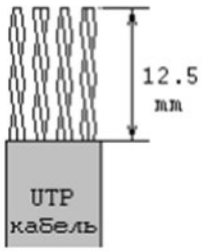


Давайте подробнее посмотрим, как проводят монтаж выбранного типа вилки RJ-45 на кабель витой пары. Лучше всего пользовать специальным обжимным инструментом. В крайнем случае, несколько разъемов можно обжать отверткой. Монтаж производится одинаковым способом или для 568A, или для 568B с двух сторон кабеля.

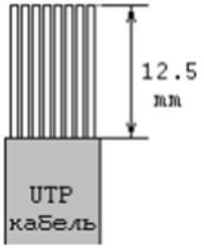
1. Удалите внешнюю оболочку кабеля, на длину 12,5 мм (1/2 дюйма). В обжимном инструменте имеется специальный нож и ограничитель для этой операции.

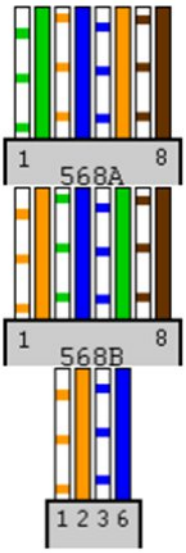


Провода зачищать не надо

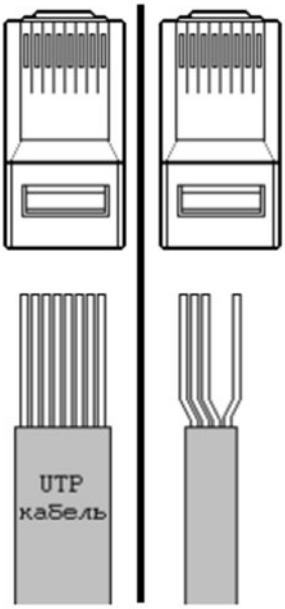


Расплетите кабель и расположите провода в соответствии с выбранной вами схемой заделки, причем длина расплетения не должна превышать 12,5 мм.

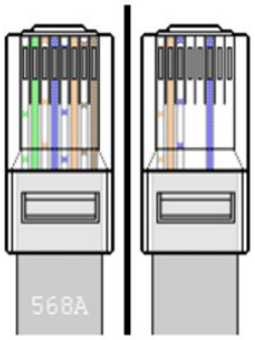




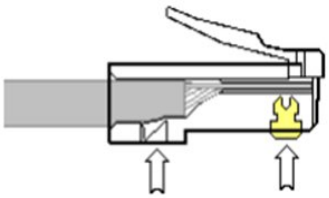
Поверните вилку контактами к себе, как на рисунке, и аккуратно надвиньте на кабель до упора , чтобы провода прошли под контактами.



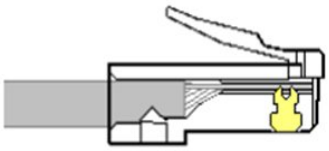
Вилка, с кабелем внутри.



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



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



Вот так происходит монтаж витой пары.

Надо отметить, что кроме кабелей **категории 5**, существуют еще кабели **категорий 6 и 7**, их промышленность начала выпускать сравнительно недавно.

Для кабеля **категории 6** характеристики определяются до частоты 200 МГц, а для кабелей **категории 7** - до 600 МГц.

Кабели **категории 7** обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель **категории 6** может быть как экранированным, так и неэкранированным.

Практическое задание: *Заделка кабеля витая пара в розетку*

Цель работы:

- Изучить основные этапы монтажа кабельных систем Ethernet.
- Отработать навыки монтажа сети на основе витой пары.

Теоретическая часть

Прокладывание локальной сети на основе коаксиального кабеля

В нашей стране наиболее распространены три типа разъемов BNC: «под пайку» отечественного производства марки «СР», предназначенные для использования в сетях с волновым сопротивлением 50 Ом и частотой до 10 ГГц, а также «под обжим» и «под накрутку» импортного производства. Существует несколько разновидностей отечественных разъемов «под пайку», отличающихся, в основном, используемыми при их изготовлении материалами, их маркировка состоит из обозначения СР-50-XX-Y, где значение 50 указывает величину волнового сопротивления, XX — число, обозначающее тип разъема, а Y — буква, определяющая материал, из которого выполнена опорная шайба: Ф — фенопласт, С — полистирол, К — керамика, П — полиэтилен, В — высокочастотный пресс-порошок. Разъемы «под пайку» обычно не обеспечивают должного качества соединения, поскольку малейшая неосторожность в припаивании

контакта центральной жилы или экрана приводит к тому, что при случайном шевелении кабеля сеть перестает работать, и локализовать сбойный участок оказывается крайне сложно. Поэтому опытные специалисты рекомендуют приобретать разъемы BNC «под обжим», которые не только полностью соответствуют стандарту Ethernet 10Base2, но и крайне просты в монтаже (рис. 1).

Такой разъем состоит из трех элементов, продающихся в виде комплекта разделенных деталей, запаянных, как правило, в полиэтиленовую упаковку: это сам разъем с рифленой контактной площадкой заземления, контакт центрального провода и металлическое цилиндрическое кольцо — манжета. Помимо самого разъема вам понадобится также специальный обжимной инструмент (кримпер) для коаксиального кабеля (рис. 2).

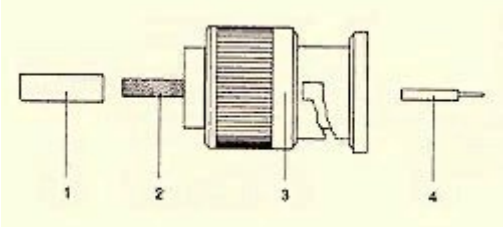


Рис.1. Разъем BNC «под обжим»: манжета; 2— контактная площадка заземления; 3— разъем; 4 — контакт центрального провода

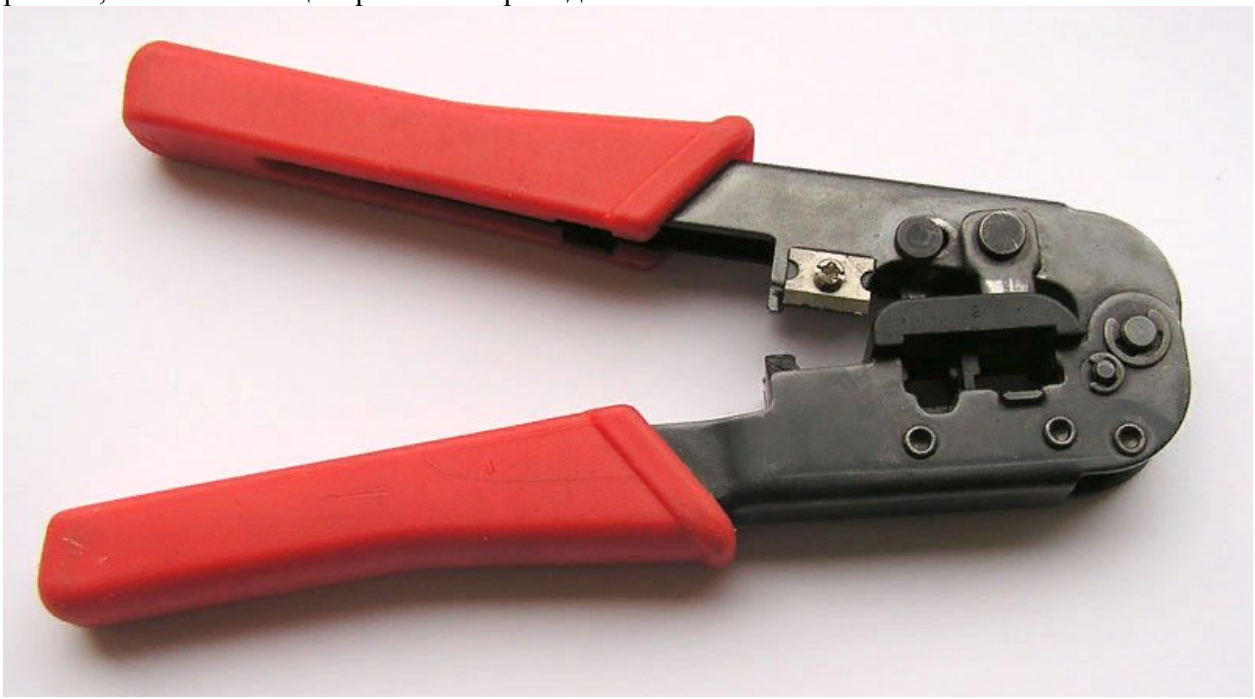


Рис. 2. Обжимной инструмент для коаксиального кабеля

Если обжимного инструмента нет под рукой, можно воспользоваться обыкновенными пассатижами, но в этом случае при монтаже следует проявлять особую осторожность. Итак, для того чтобы смонтировать на коаксиальном кабеле разъем BNC, необходимо выполнить такую последовательность действий (рис. 3).

1. Ровно обрежьте край коаксиального кабеля таким образом, чтобы на его торце не было зазубрин и скосов. Наденьте на кабель металлическую муфту разъема BNC.

2. При помощи острого ножа или скальпеля удалите верхний защитный изоляционный слой коаксиального кабеля на расстояние приблизительно 20-25 мм от края. Проделывайте эту процедуру крайне осторожно, чтобы не повредить расположенную под защитным слоем металлическую оплетку. Аккуратно расплетите оплетку экрана и разведите ее в стороны.

3. Стараясь не повредить центральный проводник, снимите острым ножом или скальпелем защитный слой проводящей жилы коаксиального кабеля на расстояние примерно 5-8 мм. Зачистите центральный проводник ножом или кусочком наждачной бумаги таким образом, чтобы на нем не осталось следов защитного покрытия. Наденьте на проводящую жилу контакт центрального провода.

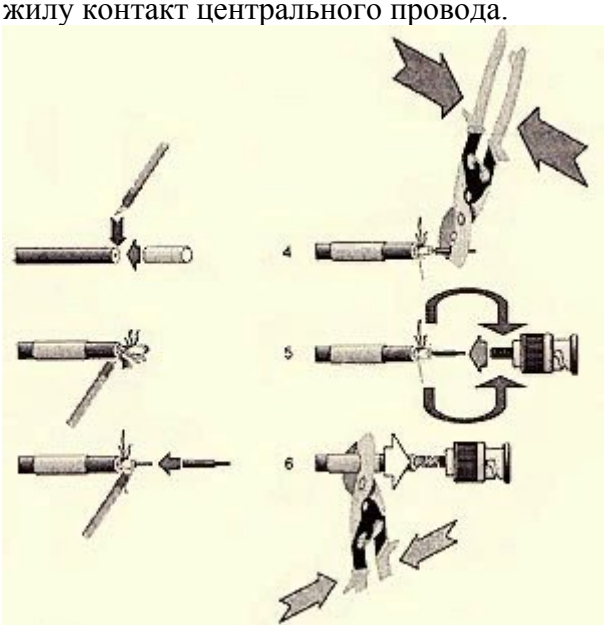


Рис.3. Порядок монтажа разъема BNC

4. Посредством обжимного инструмента или тонких плоскогубцев зажмите цилиндрическую часть контакта центрального провода таким образом, чтобы он надежно зафиксировался на проводящей жиле. При отсутствии обжимного инструмента контакт центрального провода можно припаять к проводящей жиле, но при пайке следует проявлять особую аккуратность, внимательно следя за тем, чтобы соединение было надежным.

5. Наденьте на кабель разъем до щелчка таким образом, чтобы контакт центрального провода показался из соответствующего отверстия во внутренней части разъема. Равномерно обмотайте ранее расплетенные вами проводники экранирующей оплетки вокруг рифленой контактной площадки заземления. Если волокна экранирующей оплетки окажутся слишком длинными, их можно обрезать на требуемое расстояние.

6. Надвиньте на контактную площадку заземления с обмотанным вокруг нее экранирующим проводником металлическую муфту разъема и надежно зафиксируйте ее при помощи обжимного инструмента или плоскогубцев. Разъем готов к работе.

Повторите эту процедуру необходимое количество раз, смонтировав разъемы BNC на обоих окончаниях каждого из подготовленных вами отрезков коаксиального кабеля.

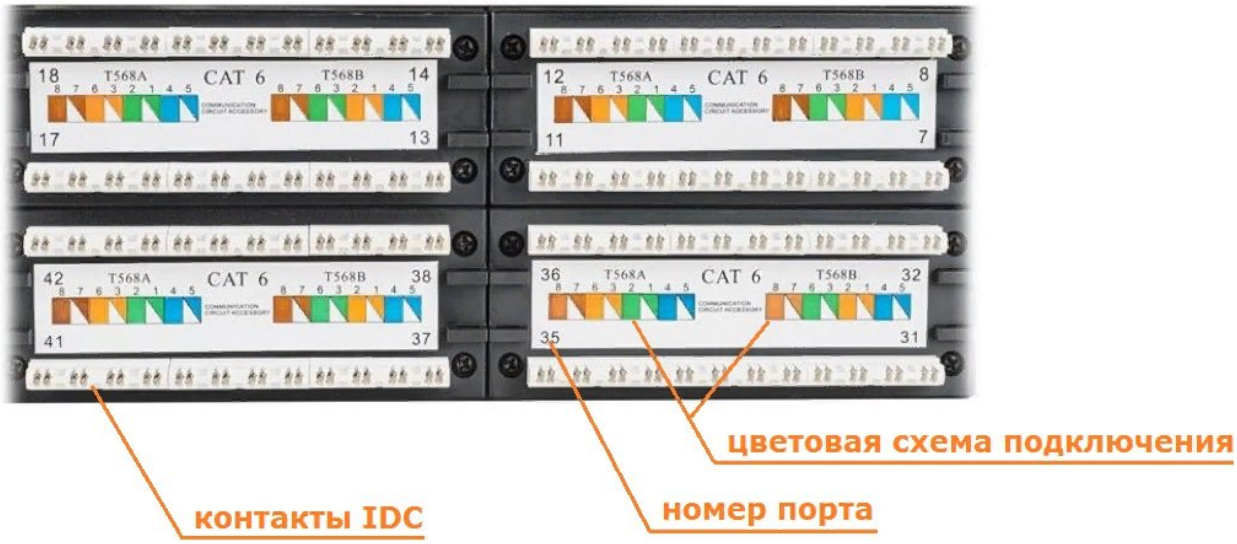
Практическое задание:*Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену*

Цель научится монтажу патч-панели в коммутационный шкаф, на стену

Как подключить патч-панель?

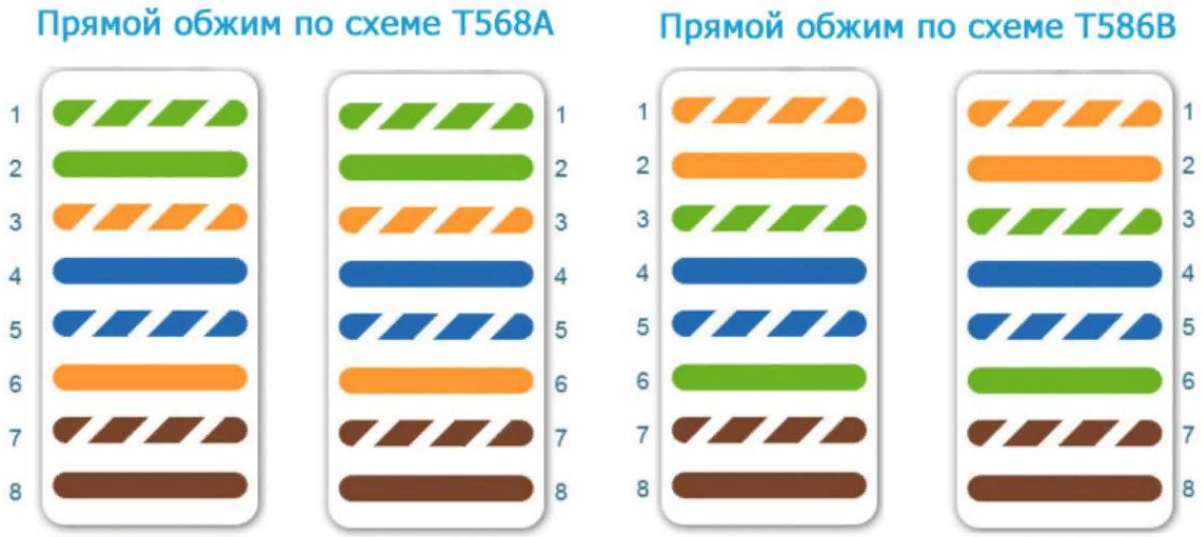
инструкция от Hypernet

Итак, у Вас есть патч-панель которую необходимо правильно "подключить" к витой паре. Точнее витую пару подключить к патч-панели.
Далее в результате Ваших действий, электрический сигнал из проводников кабеля соединенных с контактами путем так называемого "соединения со смещением изоляции", оно же IDC, будет передаваться на порты RJ-45, которые находятся на передней части патчпанели.
Рассмотрим подробнее как же подключить патч-панель...
Первое что мы видим, планируя осуществить задуманное - это задняя часть патч-панели сплощадками на которых размещаются забивные контаткы, с их помощью мы и будемподключать патч-панель



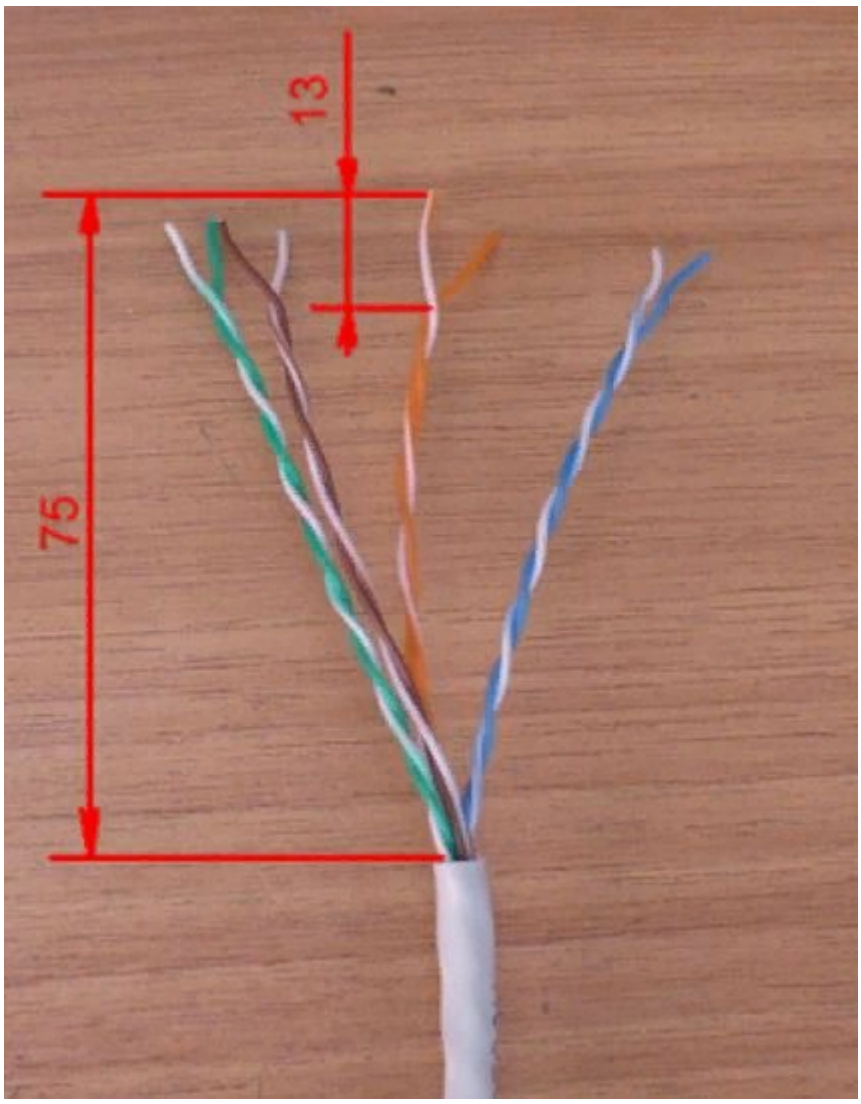
Информация, располагающаяся на наклейке-схеме, дает нам знать:

- Номер порта RJ-45 на лицевой части к которому относится близлежащая планка с 8-ю врезными контактами
- Цветовые схемы T568A и T568B показывающие в каком порядке должны быть расположены и заделаны проводники витой пары. Чаще всего используют стандарт T568B. Цветовая схема актуальна для порядка размещения проводов как в верхнем ряду контактов, так и в нижнем
- Категорию патч-панели



Шаг первый

Зачищаем изоляцию витой пары. Согласно международным стандартам по СКС, длинна снятой внешней изоляции не должна превышать 75 мм а развитие пар должно быть в пределах 13 мм и не более.

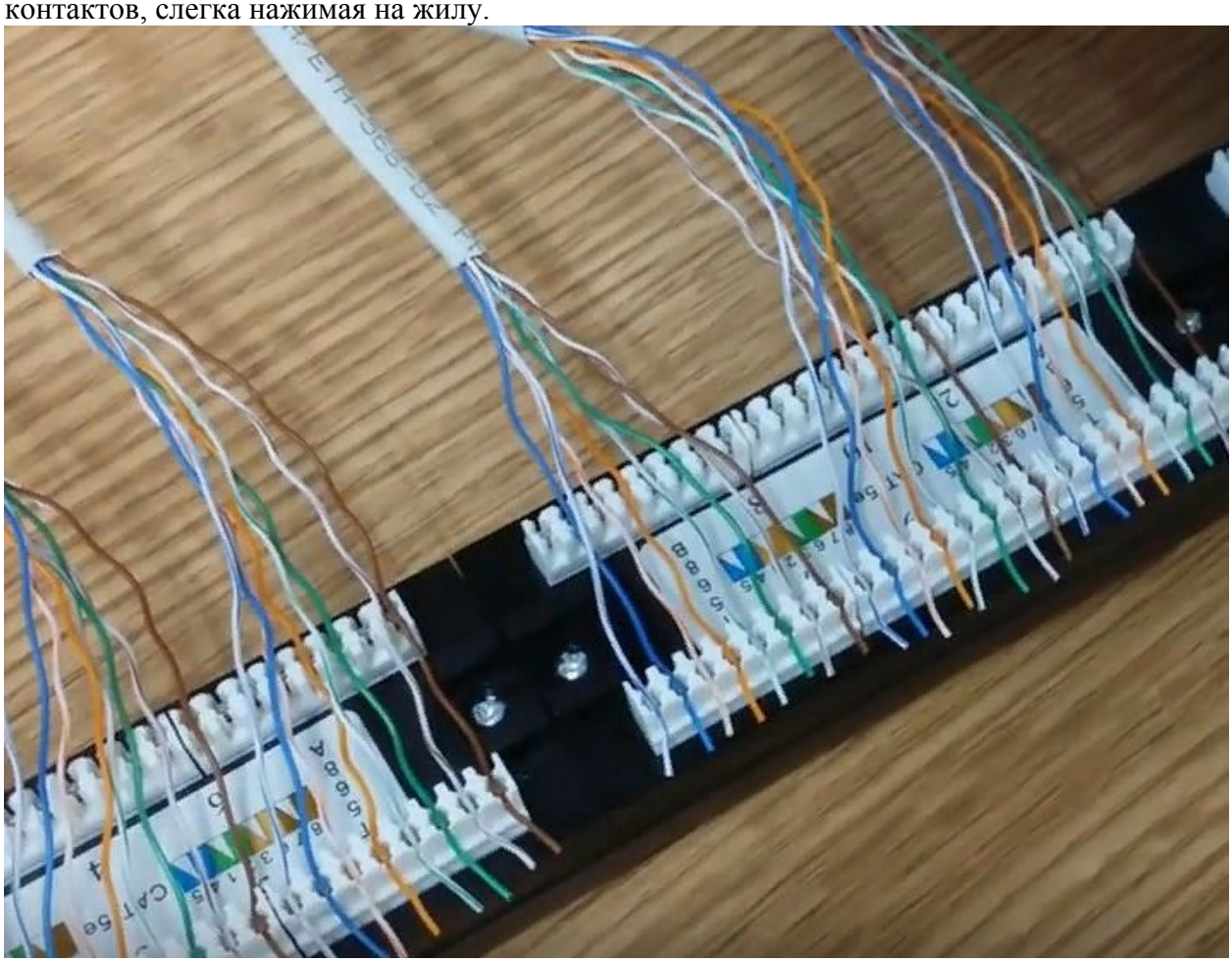


Шаг второй

Удобно разместите патч-панель перед собой ~~на коленке~~ на столе или другой неподвижной и желательно ровной поверхности. Можно заделывать патч-панель прямо в коммутационном шкафу или на стойке, когда она уже прикреплена к 19" направляющим.

Руководствуясь цветовой схемой поочередно разведите пары соответствующим образом.

Зафиксируйте развитые жилы кабеля в соответствующие им по цветам ячейкам контактов, слегка нажимая на жилу.



На фото изображена тренировочная раскладка, пары чрезмерно развиты в демонстрационных целях. Помните, чем меньше размотка пар, тем лучше. При желании можно разложить проводники сразу на несколько портов.

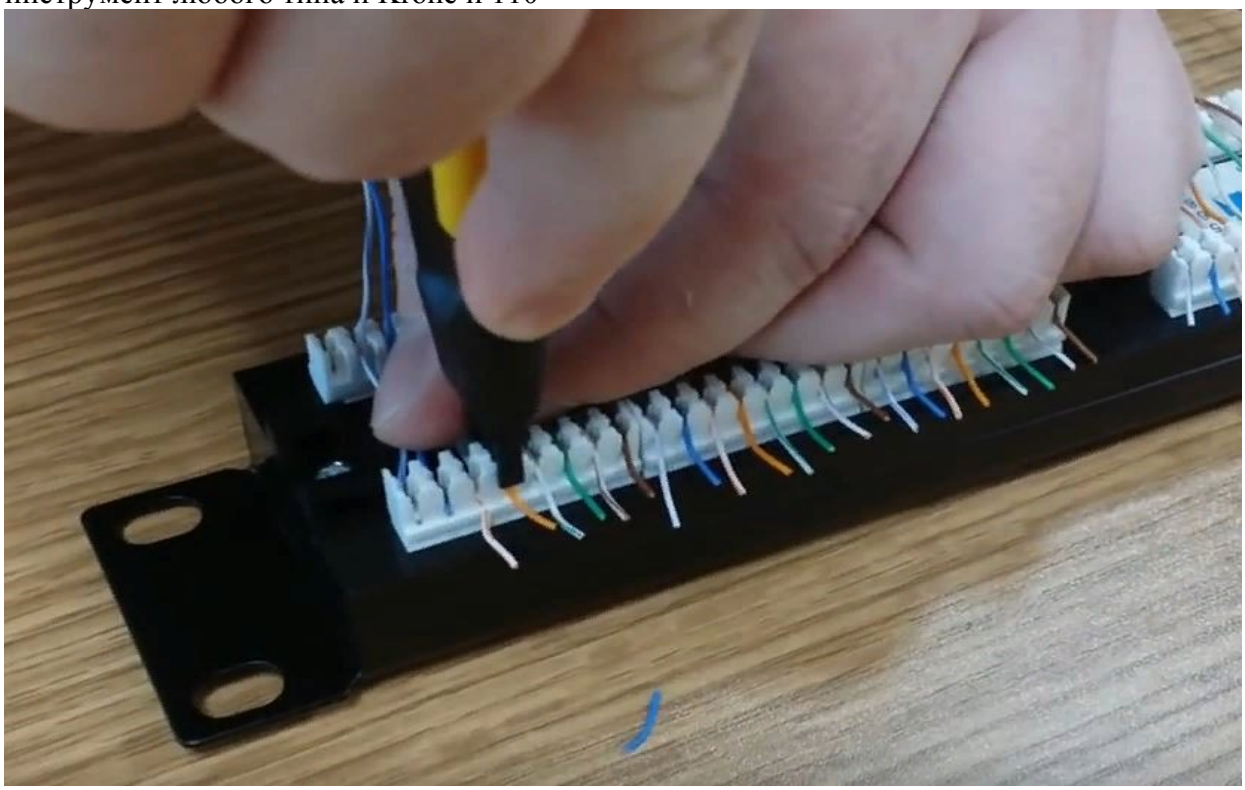
Шаг третий

Финишными действиями в подключении патч-панели можно считать заделку жил кабеля с помощью специального заделочного ключа, например HT-344KR

Нужно отдельно сказать о моменте соответствия типа лезвия на инструменте и типа контактов на патч-панели.

Вкратце картина такова:

- Лезвие типа Krone, может заделывать контакты типа Krone, типа 110, Dual IDC.
- Лезвие типа 110, может заделывать контакты типа 110 и Dual IDC
- Если на патч-панели имеются контакты типа Dual IDC, значит к ним подойдет инструмент любого типа и Krone и 110



Поместите лезвие инструмента в ячейку контакта, где предварительно установлен проводник. Обрезающую сторону заделочного лезвия или специальные ножницы для обрезки остатков жил, в зависимости от модели, нужно размещать строго со стороны концов проводников. На фото излишки жил обрезаются бокорезом установленным с внешней стороны патч-панели.

При выполнении заделки инструмент должен размещаться строго перпендикулярно к патч-панели.

Прижимным движением надавливайте на рукоятку заделочного ключа до характерного ударного щелчка. Ура, вы заделали жилу в контакт!

Стоит отметить, приспособление для заделки вполне может быть и без функции удара, в этом случае нужно просто надавливать до конца хода лезвия. Некоторые умельцы для этих целей пользуются отверткой, но качество подобных соединений может вызывать большие вопросы.

Конечно, как и в любом деле качество оборудования и инструмента способно влиять как на работу по монтажу и подключению патч-панели, так и на окончательный результат. Выбирайте качественного сетевое оборудование.

Практическое задание:*Тестирование кабеля*

Часть 1. Петлевая заглушка

Этап 1. Проверка кабеля Ethernet с помощью петлевой заглушки

a. Подключите петлевую заглушку к одному концу соединителя.

b. Вставьте один конец кабеля Ethernet в другой конец соединителя.

c. Включите концентратор или коммутатор.

d. 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.
Часть 1 лабораторной работы закончена.
Часть 2. Кабельный тестер Проверка кабелей UTP

Этап 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.
Этап 2. Процедура проверки кабелей
Порядок проверки с использованием кабельного тестера Fluke для локальной сети.
a. Вставьте один конец кабеля в разъем RJ-45 тестера с маркировкой «UTP/FTP».
b. Вставьте другой конец кабеля в розетку RJ-45 соединителя (с маркировкой «LAN Use»).
c. Вставьте идентификатор кабеля (с маркировкой «Net Tool») в другой конец соединителя. Ко многим кабельным тестерам прилагаются соединитель и идентификатор кабеля.

Этап 3. Использование функции Wire Map (Схема разводки проводов)
Функцию Wire Map (Схема разводки проводов) и идентификатор кабеля можно использовать дляопределения прокладки ближнего и дальнего концов кабеля. Один набор номеров, отображаемых наЖК-экране, соответствует ближнему концу, а другой ряд — дальнему концу.
a. 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 описаниепроблемы.

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:	

Этап 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)

Практическое задание:*Поддержка пользователей сети*

Вопросы для проверки знаний

1.Вы работаете в IT-аутсорсинговой компании. Ваша работа - решать вопросы, которые не смогли решить менее опытные сотрудники (или решение вопроса находится не в их компетенции). На какой линии поддержки вы работаете?
2.Для выхода в Интернет Вы используете механизм трансляции сетевых адресов NAT. Все пользователи получают IP-адреса из DHCP-зоны, располагающейся на DHCP-сервере. К вам подходит пользователь и говорит, что для его работы (а конкретно, для работы специальной программы) ему необходим внешний статический IP-адрес. Сможет ли эта программа преодолеть NAT - неизвестно. В вашем распоряжении всего 1 белый IP адрес и он задействован. Можете ли Вы помочь пользователю?
3. Вам необходимо распространять видео по локальной сети. Какой групповой IP-адрес (или диапазон IP-адресов) Вы выберете для потокового вещания?
4. Вы устанавливаете беспроводную сеть у пользователя. Точка доступа работает на 802.11n. Вы установили на ней режим "Native". У пользователя ноутбук, беспроводная

сетевая карта которого работает на 802.11g. Будет ли установлено соединение и на какой скорости?
5. Пользователь зашифровал системный диск своего компьютера при помощи технологии Microsoft Bitlocker. Но в виду неаккуратного обращения с флэш-накопителем, ключ для восстановления был утерян. Компьютер без флэш-накопителя не загружается. Бумажной копии ключа у пользователя также нет. Что можно сделать, чтобы получить доступ к данным на диске?
6. Вам звонит абонент и жалуется на постоянные потери соединения. Также он сообщает, что при подъеме телефонной трубки он слышит шипение. В чем из перечисленного может быть проблема?
7. Вам необходимо обеспечить защиту компьютера от DoS (или DDoS) атак. Какой класс программного обеспечения необходимо использовать?
8. Компьютер пользователя стал вести себя ненормально. Иногда мышка "ездит" сама, открывается лоток CD-ROM, мигают индикаторы на клавиатуре. Какой тип заражения характерен для этого поведения?
9. Вам требуется произвести аудит сайтов, на которые заходят Ваши пользователи. Какой тип аудита Вы будете использовать?
10. Пользователь жалуется, что некоторые приложения, которые на Windows XP у него работали, сейчас не работают. ОС установленная на его компьютере - Windows 7 Enterprise. Что Вы можете предложить Вашему пользователю, чтобы его приложения работали?

Практическое задание:*Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)*

Вопросы для проверки знаний

1. Как часто нужно проводить чистку системного блока
2. Как правильно нужно присоединять кабель к порт ПК? Почему?
3. Функции ИБП.
4. Зачем нужно знать, где находится аварийный рубильник выключения питания?
5. Правила подключения принтеров к сети.
6. Особенности эксплуатации струйных принтеров.
7. Особенности эксплуатации лазерных принтеров.
8. Какой тип кабеля должен использоваться для горизонтальной подсистемы?
9. Какие меры нужно принять для повышения надежности ЛВС?
10. Какое коммутационное оборудование вы знаете?
11. Какие правила технической эксплуатации коммутационного оборудования?

Теоретические сведения

Правила технической эксплуатации ПК

1. Необходимо обеспечить защиту ПК от воздействия пыли. Не желательно устанавливаться системный блок на пол, потому что именно так пыль быстрее всего проникает внутрь. Но, не смотря на все меры защиты, пыль, так или иначе, попадает в системный блок, и необходимо своевременно проводить техническое обслуживание ПК. Для чего оно проводится? Из-за воздействия пыли, происходит перегрев компонентов системного блока, помимо этого забиваются контакты, что приводит к выходу из строя того или иного устройства. Чистку системного блока необходимо проводить 2-3 раза в год. Не рекомендуется делать это самостоятельно, так как данная процедура имеет множество нюансов и сложностей.
2. Необходимо поддерживать температурный баланс в системном блоке, так как при высоких температурах компоненты ПК очень быстро изнашиваются, либо не корректно

работают. Температура каждого комплектующего должна быть в пределах нормы, все кулера (вентиляторы) должны быть в хорошем рабочем состоянии.
3. ПК не должен располагаться под прямыми солнечными лучами, желательно обеспечить возможность для хорошей циркуляции воздуха.
4. На вашем ПК обязательно должен быть установлена антивирусная программа, а так же программа для защиты от вирусов, проникающих с флеш-карт. Перед использованием, любой внешний носитель информации (флеш-карта/диск), а так же информацию, скачанную с интернета необходимо просканировать антивирусной программой. Необходимо проследить, что бы при подключении к Internet ежедневно обновлялись антивирусные базы, если подключение отсутствует, делать это вручную.
5. Рекомендуется не посещать сомнительные сайты, не устанавливать пиратские программы. Так же не рекомендуется “перегружать” операционную систему большим количеством не используемых программ, свои документы, личные файлы держать в порядке, не используемую информацию удалять.
6. Все шнуры, используемые для соединения ПК с другими устройствами вставлять и вынимать можно только при выключенном компьютере, иначе можно сжечь порт, куда вставляется кабель. Исключение:USB-порты.
7. Необходимо ВСЕГДА производить правильное отключение компьютера (Пуск—»Завершение работы—»Выключение)
8. Рекомендуется использовать источник бесперебойного питания (ИБП). В случае отключения электропитания, ИБП обеспечит подачу питания для работы ПК, что позволяет сохранить необходимую информацию и произвести корректное отключение. Так же он стабилизирует напряжение, что не мало важно, потому что скачки напряжений/молнии, наносят большой ущерб любой техники, а особенно компьютеру, вплоть до выхода из строя.

Правила технической эксплуатации серверов

- Предохраняйте устройство от пыли и грязи до и после установки
- Убирайте снятый кожух устройства в безопасное место
- Не кладите инструменты в места, где кто-нибудь может на них наступить
- Не носите одежду со свисающими частями во время работы с устройством. Застегните рукава и снимите шарфы и т.д.
- Наденьте защитные очки при работах, могущих быть опасными для глаз.
- Не выполняйте действий, могущих быть опасными для персонала и оборудования

При работе с устройствами, подключенными к линиям электропитания, снимайте металлические ювелирные изделия и наручные часы, могущие причинить серьезные ожоги при контакте с линиями питания и заземления, а также при электростатических наводках.
Используйте следующие правила при работе на подключенном к линиям питания оборудовании

- Перед началом работы определите, где находится аварийный рубильник выключения питания в помещении. При инциденте на линиях питания вы сможете быстро обесточить оборудование.
- Перед работой на оборудовании отсоедините кабель питания.
- Отсоедините все кабеля питания перед:
    - Установкой/ удалением шасси
    - Работой около источников питания

Никогда не делайте предположения о том, что питание выключено. Всегда проверяйте. Тщательно обследуйте рабочее место на предмет обнаружения неисправных и незаземленных кабелей питания, влажных поверхностей

Правила технической эксплуатации принтеров

Подключение принтеров к сети

Сначала принтер подсоединяется к компьютеру, а потом включается в электрическую сеть, иначе у обоих устройств могут сгореть порты ввода-вывода. Данная ситуация обычно расценивается как нарушение инструкции, при этом гарантия аннулируется.

Струйные принтеры

В любой инструкции к таким принтерам есть предупреждение о необходимости использования только одобренных производителем расходных материалов, кроме того, в большинстве моделей всегда должны быть установлены картриджи. При замене картриджа в головку неизбежно попадает воздух, но если замена произведена по правилам, принтер тотчас начинает выполнять процедуру прокачки.

Лазерные принтеры

Нужно использовать бумагу плотностью не ниже 60 г/кв.м, гладкую, хорошего качества, а чтобы бумага не впитывала влагу, хранить ее при небольшой влажности воздуха. Если эти требования не будут выполнены, бумага может намотаться на валики печки, таким образом, могут быть выведены из строя некоторые детали принтера. Использование типографских бланков, бумаги, на которой уже что-то напечатано/написано, также сокращает срок службы офисной техники. А попытка печати на бумажном листе с канцелярской скрепкой обычно приводит к необходимости замены фотобарабана.

Также весьма опасна и самостоятельная заправка картриджа - производитель подбирает состав тонера с учетом технических особенностей моделей. При заправке тонер-картриджа порошком другого состава возможны серьезные проблемы.

Профилактическое обслуживание оргтехники

Профилактическое обслуживание подразумевает очистку, смазку, регулировку функциональных узлов, механизмов офисной техники. Это регламентная процедура, предусмотренная производителем аппарата для его нормальной работоспособности, периодичность которой устанавливается фирмой производителем. Для разных моделей техники периодичность профилактики различна: зависит от месячной нагрузки на аппарат, от условий эксплуатации.

Месячная нагрузка на аппарат

Производительность аппарата, допустимая месячная нагрузка указывается в техпаспорте аппарата, там же указана периодичность обслуживания, если аппарат за месяц перерабатывает максимальную месячную нагрузку, то происходит усиленный износ всех узлов/деталей аппарата, что сокращает их ресурс. Поэтому профилактика должна выполняться чаще, а ремонт придется провести быстрее.

Условия эксплуатации

В помещениях с повышенной влажностью сильно загрязняется оптический узел, в пыльных помещениях сильнее загрязняются высоковольтные узлы, образуется нагар в узле фиксации. Но даже при нормальных условиях тонер из блока проявки понемножку просыпается даже в совершенно исправных аппаратах. Кроме того, любая бумага имеет ворсинки на поверхности, из-за чего при протяжке образуется бумажная пыль, оседающая на всех узлах аппарата.

Правила технической эксплуатации коммутационного оборудования

В комплексе зданий должна быть установлена слаботочная кабельная система EuroLAN. ЛВС, являясь слаботочной структурированной кабельной системой 5е категорий и в соответствии с международным стандартом на кабельные системы ISO/IEC 11801 должна состоять из следующих подсистем:

- подсистемы внешних магистралей, содержащей внешние магистральные кабели между кроссовыми зданий, коммутационное оборудование в кроссовых зданий, к которому они подключаются, и коммутационные шнуры и перемычки в кроссовых зданий;
- подсистемы внутренних магистралей, содержащей внутренние магистральные кабели между кроссовой здания и кроссовыми помещений, коммутационное оборудование в

кроссовой здания и кроссовых помещений, к которому они подключаются, и коммутационные шнуры и перемычки в кроссовой здания,
- горизонтальной подсистемы, состоящей из внутренних горизонтальных кабелей между кроссовыми этажей и информационными розетками рабочих мест, самих информационных розеток, коммутационного оборудования в кроссовых этажей, к которому подключаются горизонтальные кабели, и коммутационных шнуров и перемычек в кроссовых этажей.

1. Рабочие места

На рабочих местах должны быть установлены розетки типового рабочего места, содержащие один информационный разъем, используемый для подключения компьютера. К информационной розетке подходит один кабель горизонтальной подсистемы ЛВС.

2. Горизонтальная подсистема.

Для горизонтальной подсистемы должен использоваться 4-х парный медный кабель неэкранированная витая пара категории 5е типа «19С-115-03-В305».
Кабель должен прокладываться, используя топологию «звезда», от распределительного узла в этажном техническом помещении к каждому отдельно взятому информационному разъему на рабочем месте СКС. В технических помещениях приходящие с рабочих мест горизонтальные кабели разделываются на секции рабочих мест коммутационного поля в соответствии с таблицами соединений и подключений.
При разработке трасс прокладки кабелей должно быть учтено, что длина каждого отдельного сегмента кабеля от кроссового поля до информационного разъема не должна превышать 90 м.
Начиная от кроссового поля, кабель должен прокладывается в кабель - каналах. Трассы прокладки кабелей ЛВС по коридорам и рабочим помещениям должны быть приведены на рабочих чертежах основного комплекта документации.
В помещениях имеющих подвесные потолки кабель прокладывается за панелями. Монтаж коробов должен осуществляться на высоте 10 см ниже уровня потолка, а в помещениях - на высоте не менее 30 см от уровня чистого пола (информационные розетки должны быть расположены ниже уровня рабочей поверхности столов), в помещениях имеющих подвесные потолки или сегмент рабочей локальной сети, схема монтажа коробов может быть изменена.
При прокладке кабеля должен оставляться технологический запас для разделки кабеля - на рабочем месте не менее 30 см от точки размещения информационной розетки, в кроссовой - не менее 2 м от точки размещения 19-дюймового монтажного шкафа. В соответствии с международным стандартом E1A/T1A-606, концы кабелей при прокладке маркируются на обоих концах липкой маркировочной лентой, на которой указывается идентификатор кабельной трассы в соответствии с нумерацией рабочих мест в комнате и информационных розеток на рабочем месте.

3. Подсистема внутренних магистралей

Для прокладки кабельных трасс подсистемы внутренних магистралей должен использоваться одномодовый оптоволоконный кабель.
Подсистема внутренних магистралей ЛВС должна быть реализована на основе одномодового 4 и 8-волоконного кабеля. Он содержит 4 и 8 одномодовых волокна 9/125 мкм соответственно.
Кабели подсистемы внутренних магистралей прокладываются по кабель -каналам, размещение которых показано на рабочих чертежах основного комплекта. Концы кабелей вводятся в технические помещения. В технических помещениях оставляется технологический запас кабеля (не менее 5 м). Оставляемый запас кабеля формируется в бухту, размещаемую в коммуникационном шкафу вдоль задней или боковой стенки.

Концы кабелей в процессе прокладки маркируются на обоих концах липкой маркировочной лентой, на которой указывается идентичный для обоих концов уникальный идентификационный код.

4. Подсистема внешних магистралей

Для прокладки кабельных трасс подсистемы внешних магистралей должен использоваться одномодовый оптоволоконный кабель.

Подсистема внешних магистралей ЛВС должна быть реализована на основе одномодового 4 и 8-волоконного кабеля. Он содержит 4 и 8 одномодовых волокна 9/125 мкм соответственно.

Кабели подсистемы внешних магистралей должны прокладываться по опорам линий электропередач и непосредственно с здания на здание. Концы кабелей вводятся в технические помещения. В технических помещениях должен оставляться технологический запас кабеля (не менее 10 м). Оставляемый запас кабеля формируется в бухту, размещаемую в коммуникационном шкафу вдоль задней или боковой стенки.

Концы кабелей в процессе прокладки должны маркироваться на обоих концах липкой маркировочной лентой, на которой должен указываться идентичный для обоих концов уникальный идентификационный код.

5. Коммутационное оборудование для медных кабелей

В качестве коммутационного оборудования для медных кабелей должны быть использованы 24- или 48- парные коммутационные панели типа «27B-U5-24 (48)» категории 5e для разделки кабелей горизонтальной подсистемы. Также допускается использование соединительных шнуров с разъемами «RJ45-RJ45».

6. Коммутация и подключение оптоволоконных сетей

В проектируемой ЛВС роль кросса для оптоволоконной части подсистемы внутренних и внешних магистралей должны выполнять оптические одномодовые распределительные полки с 4, 8 и 32 разъемами «SC». В комплекте со шкафами должны поставляться крепёжные наборы для монтажа кроссовых панелей и оптических полок. Для обеспечения возможности укладки избытка соединительных коммутационных шнуров под оптическими полками должны быть смонтированы организаторы кабеля, имеющие форму пластины с держателями кабеля.

Для монтажа оптоволоконной части подсистемы внутренних и внешних магистралей должна использоваться технология сварки. Применение этой технологии обеспечивает минимальные потери в точке сращивания световодов и наибольшую надежность соединения.

Коммутация между центральными коммутаторами и оптическими распределительными полками должна осуществляться коммутационными шнурами с разъемами «SC» на обоих концах.

7. Монтажные шкафы

Коммутационное оборудование ЛВС, а также активное оборудование ЛВС должны быть установлены в 19-дюймовые монтажные шкафы 7С1 и 1211, а в серверной - в монтажную стойку.

8. Решения по размещению комплекса технических средств на объекте

Для размещения коммутационного оборудования СКС и активного оборудования ЛВС в каждом здании должно быть предусмотрено не менее 1 технического помещения. В техническом помещении должен быть установлен 19-дюймовый настенный монтажный шкаф, в техническом помещении серверной - монтажная стойка.

В монтажные шкафы должны быть установлены оптические распределительные полки для подключения оптоволоконных кабелей подсистемы внутренних магистралей, а также кроссовые панели для разделки горизонтальных кабелей.

9. Решения по обеспечению надежности

Надежность ЛВС должна определяться составляющими ее компонентами, к которым относятся: кабель, разъёмы и устройства сопряжения, коммутационные панели. Для повышения надежности ЛВС должны быть приняты следующие меры:
- для организации магистральной кабельной разводки должен использоваться оптоволоконный кабель, который является нечувствительным к электромагнитным помехам, а также обеспечивает гальваническую развязку ЛВС;
- кабели должны прокладываться в коробах - т.е. в труднодоступных для пользователей местах;
- для подключения компьютеров и другого оборудования должны использоваться сменные, легкозаменяемые терминальные шнуры.
- перед сдачей ЛВС в эксплуатацию необходимо спланировать проведение комплекса тестовых проверок.

10. Решения по защите информации от несанкционированного доступа

Защита информации должна обеспечиваться техническими мероприятиями, затрудняющими считывание передаваемых данных на всем протяжении физических каналов кабельной системы. Это должно достигаться тем, что кабель прокладывается в физически труднодоступных и скрытых для персонала и клиентов местах.

11. Решения по режимам функционирования системы

ЛВС должна поддерживать круглосуточный режим функционирования.

Практическое задание:*Выполнение действий по устранению неисправностей*

Цель: определение неисправностей персонального компьютера.
Оборудование: ПК, макет системного блока, операционная
система Windows XP, Windows 7.
Базовые сведения.
Любой ремонт ПК тестируется последовательно:

1. Начните с открывания задней крышки и снятия слоя статической пыли с комплектующий частей механизма.
2. Затем включаете компьютер в сеть и проверяете работу механизмов (например, скорость вращения кулера).
3. Если компьютер не включается в сеть, попробуйте сразу проверить исправность блока питания, установив новый блок – это очень частая ошибка. Если он обгорел или искрит – устраните сначала эту проблему!
4. Проверьте исправность клавиатуры и мыши, вычистите их – часто поломки случаются из-за засоренности этих периферийных механизмов.
5. Проверьте все соединения кабелей – выньте и вставьте их обратно.
6. Проверьте все соединения шлейфов с портами внутри ПК.
7. Замените батарейку на материнской плате (если ей больше трех лет).
8. Выньте и вставьте на место планки памяти. Только осторожно.
9. Проверьте состояния портов – все ли они плотно сидят в своих гнездах и не оборваны ли контакты?

Задание №1. Установка оборудования
Если Windows не удалось обнаружить новое оборудование, необходимо воспользоваться Мастером установки оборудования на панели управления, чтобы сообщить Windows о типе устанавливаемого устройства.
Запустите **Мастер установки оборудования.**
Шаг 1. Откройте **Пуск – Панель управления – Установка оборудования**;
Шаг 2. Появилось окно Мастера установки оборудования, щелкните кнопку **Далее**;
Примечание Строго следуйте инструкциям, которые содержит каждое окно.
Шаг 3. Мастер производит поиск нового оборудования;

Шаг 4. На вопрос «Это устройство уже подсоединено к компьютеру?» щелкните **Да** и кликните кнопку **Далее**;
Шаг 5. Посмотрите список установленного оборудования, выделите одно из них и щелкните кн. **Далее**;
Шаг 6. осмотрите текущее состояние оборудования и щелкните кнопку **Готово.**
Задание №2. Настройка системы
Шаг 1. Откройте **Пуск – Панель управления – Система;**
Шаг 2. Ознакомьтесь с информацией на вкладке **Общие**;
Шаг 3. Щелкните на вкладке **Оборудование** кн. **Диспетчер устройств**.
Шаг 4. Просмотрите структуру подключенных драйверов (просмотр осуществляется так же как в проводнике). Если драйвер конфликтует с устройством или неправильно работает, на его значке ставится восклицательный знак в желтом кружке. Если устройство отключено на его значке ставится красный крест.
Шаг 5. В ознакомительном порядке просмотрите остальные вкладки «**Свойства системы**».
Задание № 3. Создание контрольной точки восстановления в Windows 7
Шаг 1. Пуск → Панель Управления → Система и безопасность
Шаг 2. Кликаем по кнопке Система → Защита системы
Шаг 3. Открывается окно, в котором необходимо нажать на кнопку «Создать»
Шаг 4. Вводим какие-нибудь слова, чтобы можно было идентифицировать именно эту точку восстановления, например: «первая точка восстановления», и жмем «Создать».
Все, точка восстановления создана.
Задание № 4. Восстановление системы в Windows 7 с контрольной точки
Шаг 1. Пуск → Все программы → Стандартные → Служебные → Восстановление системы
Шаг 2. Запускается «Восстановление системы». На этот момент у нас уже есть одна контрольная точка. Кликаем кнопку «Далее».
Шаг 3. Ставим галочку левой кнопкой мыши напротив «Показать другие точки восстановления» и жмем «Далее».
Шаг 4. Жмем «Готово» в следующем окне.
Шаг 5. Далее вам система выдаст предупреждение, что восстановление системы невозможно будет прервать. Вы соглашаетесь и жмете «Да».
После нажатия кнопки начнется восстановление на более раннее состояние и произойдет перезагрузка системы и, если был какой-нибудь сбой, то он исчезнет.

Практическое задание:*Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.*
Цель работы: получить навыки использования стандартных сетевых утилит ОС Windows

В процессе занятия решаются следующие задачи:

1. проанализировать конфигурацию сети на платформе ОС Windows;
2. Получить практический опыт применения сетевых утилит для тестирования сети;

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:\Documents and Settings\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 IP-адресов). 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] - используется в сетях Novell NetWare,

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:\Documents and Settings\Администратор>net view \\- /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:\Documents and Settings\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 *Net share*

Управление общими ресурсами. При вызове команды *net share* 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 share ОбщиеДанные=c:\Данные /remark:"Для отдела 123"
Чтобы отменить общий доступ к ресурсу Общие Данные, созданному в предыдущем примере, введите:
net share ОбщиеДанные /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 обладает встроенными 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 её;
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;

Время выполнения работы 45 мин;

Практическое задание:*Оформление технической документации, правила оформления документов*

Цель работы: изучить особенности оформления технической документации.
1.2 В результате выполнения лабораторной работы студент должен знать:
о виды конструкторских документов
опонятие проектно-сметной документации
оособенности изготовления и оформления технической документации
1.3Используемые программно-технические средства:
Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista/7/8/10, MicrosoftOfficeWord.
1.4В процессе выполнения лабораторной работы студент должен:
оОзнакомится с теоретическим материалом.
оПодготовить отчет по лабораторной работе.
оОтчитаться по исполненному заданию.
Перед выполнением лабораторной работы каждый студент обязан изучить правила техники
безопасности при работе в помещении с электронно-вычислительной техникой.
1.5 Указания по оформлению отчета:
Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы;
1.6 Указания по сдаче зачета преподавателю
Для сдачи зачета необходимо:

1) выполнить практическое задание
2) предъявить отчет;
3) ответить на контрольные вопросы.
2 Теоретические сведения
Технические документы – обобщающее название документов (графических итекстовых), в которых зафиксирована техническая мысль.
Техническая документация возникает в процессе проектирования зданий иинженерных сооружений, конструирования машин, проведения научно-технических иэкспериментальных исследований, организации промышленного производства, вовремя осуществления геодезических работ, геологических изысканий. С техническимидокументами все больше стали иметь дело работники делопроизводства, органов научно-
технической информации, ведомственных архивов.Наиболее широко известна конструкторская, проектная, технологическая, научно-исследовательская документация. Основным видом технических документов являетсячертеж – изображение предмета на плоскости, выполненное особыми графическимиприемами. Чертеж, на котором имеются некоторые текстовые указания, даетвозможность представить внешний вид предмета в пространстве, понять его устройство,а также установить, из каких материалов и каким способом предмет следует изготовлять.
Техническая документация служит для решения научно-технических проблем,возведения новых зданий и сооружений, изготовления предметов промышленногопроизводства и т.п. Технические документы сохраняют свое практическое значение ипосле окончания строительства или снятия изделия с серийного производства ивыполнения других работ. Так, технические документы по строительству необходимыдля эксплуатации построенных по этим проектам объектов, различного рода перестроеки т.д. Старые технические документы используются при утверждении новых проектов вкачестве сравнения и для различного рода справок. Для эксплуатации машин и агрегатовтакже оказывается необходимым наличие технической документации.
Технические документы широко используются в качестве источников для
исследований в области истории науки и техники, установления научного приоритета.
Историко-научные и историко-технические выводы являются базой для прогнозирования развития науки и техники, что имеет исключительно большое практическое значение.
2.1. Конструкторская документация
Для изготовления изделия промышленного производства разрабатываетсяконструкторская документация. Стандарты определяют виды и комплектностьконструкторских документов на изделия всех отраслей промышленности.
Устанавливает следующие виды конструкторских документов:
- чертеж – детали, сборочный, общего вида, теоретический, габаритный,
монтажный;
- чертеж-схема;
- спецификация, техническое описание, ведомости, пояснительная записка и др.
Текстовые конструкторские документы могут содержать сплошной текст(технические описания, паспорта, расчеты, пояснительные записки, инструкции и т.п.) итекст, разбитый на графы (спецификации, ведомости, таблицы и др.). Рассмотрикаждый из видов конструкторских документов.
На чертеже детали содержится ее изображение и другие данные, необходимые для
изготовления: размеры, материал, термообработка до заданной прочности (в кг/мм2),
чистота обработки поверхности, класс точности и допуски.На сборочном чертеже – изображение сборочной единицы, которое даетпредставление о расположении и взаимной связи ее составных частей и обеспечиваетвозможность осуществления сборки и контроля. На сборочном чертеже иногдапомещаются схемы соединения или расположения

составных частей изделия, если онине оформлены в виде специальных документов, а также показываются крайниеположения перемещающихся частей конструкций.
На чертеже общего вида содержится изображение изделия с разрезами исечениями, текстовая часть и надписи, необходимые для понимания конструктивногоустройства этого изделия, а также взаимодействия его основных составных частей ипринципа работы, данные о его составе. На чертежах общих видов помещаютсятехнические характеристики.
Теоретический чертеж – документ, определяющий геометрическую форму (обводы) изделия и координаты расположения его составных частей.
Габаритный чертеж – технический документ, содержащий контурное (упрощенное) изображение изделия с указанием габаритных, установочных и присоединительных размеров.
На монтажном чертеже также приводится контурное изображение изделия иданные, необходимые для его установки (монтажа).
Чертеж-схема – это упрощенное изображение машин, механизмов, установок ипр., дающее лишь в общих чертах представление об их устройстве и принципахдействия. На схемах показаны в виде условных изображений или обозначений частиизделий и связи между ними. Электротехнические схемы являются основным видомчертежной документации, составляемой при разработке электротехнических изделий,проектов механизации и автоматизации производственных циклов и процессов. Схемыне дают представления о внешнем виде конструкции и размерах предмета.
Втехническом описаниисодержатся сведения о наиболее характерныхособенностях данного изделия, приводятся его основные показатели, описываетсяназначение конструкции, устройство и работа его отдельных частей.
Спецификация – документ, определяющий состав изделия, сборочной единицы, комплекса или комплекта.
Пояснительная записка – текстовой технический документ, содержащий описание устройства и принципа действия разрабатываемого изделия, а также обоснование принятых технических и технико-экономических решений.
Ведомости – это списки различных документов, сгруппированных поопределенным признакам. Составляются ведомости спецификаций, ссылочныхдокументов, покупных изделий, ведомости технических документов, вошедших в составтехнического предложения, эскизного и технического проектов, ведомости держателейподлинников, т.е. перечень предприятий, которые хранят подлинные документы,разработанные для данного изделия, ведомости согласования применения изделий и др.
Конструкторские документы в зависимости от способа их выполнения и характера использования подразделяются на оригиналы, подлинники, дубликаты, копии.
Оригиналом считается документ, выполненный конструктором на бумаге ипредназначенный для изготовления по нему подлинника (кальки и др.). Подлинник – это технический документ, подписанный ответственными лицами и выполненный на материале, позволяющем многократное снятие с него копий. Дубликаты – копии подлинников. Они также выполняются на материале, который дает возможность снимать с него многократные копии, и подписываются ответственными лицами. Копии – документы, выполненные способом, обеспечивающим их идентичность с подлинником и предназначенные для непосредственного использования при разработке, в производстве, эксплуатации, ремонте изделия.

2.2. Проектно-сметная документация

Проектно-сметная документация создается при решении вопроса о возведении,реконструкции и ремонте объектов капитального строительства. Проектнаядокументация для строительства характеризует вид строительства, внешний

вид итехнико-экономические показатели объекта, архитектурные и технологические решения,стоимость работ. Проектная документация для строительства подразделяется напроектную документацию по планировке и застройке городов, поселков, промышленныхкомплексов, сельских и других населенных пунктов; по жилищно-гражданскому,промышленному и сельскохозяйственному, энергетическому и гидротехническому,транспортному строительству.

В процессе проектирования объектов капитального строительства создаютсяиндивидуальные, экспериментальные, типовые проекты, проекты-эталоны,проекты-привязки и проекты малых архитектурных форм.

Основные виды проектной документации – генеральный план, чертежи фасадов,планов, разрезов здания, паспорта проектов, рисунки, пояснительные записки, эскизы,расчеты, схемы, картографические документы, сметы.

На генеральном плане дается изображение всего участка строительства, накотором в контурах вида сверху представлено размещение существующих ипроектируемых объектов, отражено благоустройство, озеленение, а иногда итопографическое состояние места строительства.

Для строительства какого-либо объекта промышленного или гражданскогоназначения разрабатываются общие чертежи и чертежи деталей. К общим относятсячертежи фасадов, планов по этажам, а также поперечные и продольные разрезы здания.

Фасад – это внешний вид здания с фрагментами его архитектурного оформления. Наобщих чертежах (планах и разрезах) указывается расположение оборудования,инженерных коммуникаций, взаимная их увязка, маркировка, а также габаритныеразмеры. Для проведения особых видов строительно-монтажных работ (отопление и

вентиляция, водопровод и канализация, электроосвещение, телефон, и др.) выполняются чертежи специального оснащения зданий и сооружений с деталировкой сложных узлов и со спецификациями на оборудование и материалы. На деталировочных чертежахуказываются размеры деталей и элементов здания или сооружения, их сопряжения,сечения конструктивных элементов и спецификации.

Для оценки архитектурной стороны проекта создаются в красках рисунки фасадовпроектируемых зданий. Рисунки, так же как и чертежи, представляют собой изображение

предмета на плоскости, но в отличие от чертежа, выполненного в ортогональнойпроекции, рисунки дают рельефное изображение предметов. Различаются рисункихудожественные и технические. Художественные рисунки изображают предмет вперспективе, технические выполняются в аксонометрии: фронтальной, изометрическойи диметрической проекциях.

Эскизами называются чертежи, выполненные от руки, обычно на миллиметровойбумаге. Они являются черновиками, Содержание лекционного материалае которых потом переносится на ватман спомощью чертежных инструментов.

Паспорт проекта – документ, в котором дается схематическое изображениеобъекта, краткое описание и сообщаются основные технические показатели.В пояснительной записке содержится справка о проектировании объекта,сведения о его назначении, внешнем виде, внутреннем устройстве; сообщаются наиболеехарактерные особенности данного объекта, приводятся его основные техническиепоказатели, указывается назначение, описывается внутреннее устройство и работаотдельных частей, особенности конструкции. Кроме того, в пояснительной запискедается объяснение экономических, общественных и других условий и предпосылоксоздания объекта, аргументация выбора данного варианта.Расчеты (гидравлические, тепловые, аэродинамические, на сейсмичность и др.)указывают параметры здания или сооружения и его составных частей в зависимости отустановленных расчетных данных. Расчеты производятся на основании использования

достижений физико-химических, биологических и других отраслей науки.В состав проектов многих сооружений (дорог, электростанций, гидротехническихи др.) входят картографические документы: топографические, специальные и иныекарты, планы городов, населенных пунктов, местности.К проектной документации всегда прикладываются сметы, которые хотя и неявляются техническими документами в собственном смысле слова, но необходимы, таккак ни одна стройка невозможна без предварительного установления финансовых затрат.Сметная документация (генеральная, рабочая смета, калькуляция) составляется на основеединичных расценок строительных работ и других нормативных материалов,установленных соответствующими ведомствами.
Технологическая документация – совокупность графических и текстовыхтехнических документов, которые отдельно или в комплексе определяют процессизготовления изделий промышленного производства или процесс сооружения объектовкапитального строительства.В технологической документации отражены способы изготовления деталей, сборкипромышленных изделий, строительства, эксплуатации и ремонта сооружений, способы
организации производственного процесса. К этой документации относятсятехнологические карты, заводские регламенты, чертежи приспособлений, оборудованияи инструмента, графики работы цехов и бригад, технические условия, схемытехнологического процесса и другие нормативные материалы по составлениютехнологии.
Основным технологическим документом является технологическая карта, накоторой дается подробное описание и приводятся расчеты всех производственныхопераций, необходимых для изготовления изделия.
Технологические карты бывают следующих видов:

1) операционная, на которой зафиксирована отдельная производственная операция (просверлить отверстие, отшлифовать поверхность и т.п.);
2) общая, или маршрутная, на которой показаны в определенной последовательности все операции по изготовлению изделия или детали;
3) цикловая, на которой перечисляются группы операций, выполняемых одним рабочим или производимых, в одном цехе;
4) карта типового технологического процесса, содержащая сведения о средствах

технологического оснащения и материальных нормативах для изготовления группыдеталей и сборочных единиц.Общая, или маршрутная, технологическая карта составляется на каждоеизделие. На основании ее выполняются операционные и другие технологическиедокументы, а также проектируются приспособления, специальный инструмент,подбирается оборудование, схематично указанные на общей карте. В технологическихкартах подробно и последовательно записаны все производственные операции поизготовлению каждой детали, сборочной единицы, изделия.В технологических картах указываются: название операций, схема установки иобработки изделия, применяемые станки, инструмент и приспособления, режим работы(скорость, тепловой режим и т.д.), время обработки (машинное и вспомогательное),специальность и разряд рабочего, стоимость каждой операции.К технологическим документам относятся также заводские регламенты. По нимидет промышленное производство на химических, металлургических, целлюлозно-бумажных, нефтеперерабатывающих и других предприятиях. В заводских регламентахописываются, нормируются и в отдельных случаях схематично изображаются те физико-химические процессы (реакции, компоненты, аппаратура и др.), которые должны
протекать для получения изготовляемого продукта.Научно-исследовательская документация создается в процессе проведениянаучных исследований в различных отраслях техники и выполнения теоретических иприкладных научно-технических разработок, отображает теоретическое и практическоерешение научно-технических

проблем, внедрение их результатов в производство.Основными видами научно-исследовательской документации являются:
1.итоговые и этапные отчеты по научно-исследовательским (НИР), опытно-конструкторским (ОКР), опытно-технологическим (ОТР) и экспериментально-проектным (ЭПР) работам;
2.технические отчеты о НИР, ОКР, ОТР, ЭПР с приложениями; заключения,отзывы и рецензии о НИР, ОКР, ОТР, ЭПР;
3.аннотации на научно-исследовательские работы; паспорта, регламенты нанаучно-исследовательские работы;
4.монографии, диссертации и отзывы на них;
5.технические задания на НИР;
6.программы научно-исследовательских работ;
7.отчеты, доклады о работе научных экспедиций; отчеты, доклады о научных итехнических командировках специалистов;
8.технико-экономические обоснования, обзоры, доклады, записки и др.;
9.первичная документация, образующаяся в процессе проведения НИР, ОКР, ОТР ЭПР (журналы записей экспериментов, результаты анализов, дневники записей показателей приборов);
10.документы на электронных носителях (дисках), фотографии, связанные с процессом исследования.

2.5. Особенности технической документации поизобретательству и стандартизации

Научно обоснованные стандарты способствуют техническому успеху, являютсяэталоном качества продукции.

Стандарты – это особые технические документы юридического значения. Чертежстандартного изделия представляет собой изображение предмета с проставленнымиразмерами и другими показателями, которые важны не для изготовления предмета, а для его применения. Конструктор, проектировщик, технолог выбирает для воплощения своей технической идеи соответствующие детали, арматуру, изделия, конструкции,изображенные на этих стандартах. Применение стандартных деталей и изделий приразработке проектов новых машин или объектов, новой технологии являетсяобязательным. Стандартные детали и изделия изготовляются на специализированныхзаводах по обычным детальным и сборочным чертежам. С целью замены устаревшихпоказателей все действующие стандарты периодически пересматриваются иустанавливаются новые с учетом достижений науки и техники.Наиболее распространенными видами изобретательской документации являются заявки на технические предложения и изобретения, авторские свидетельства (патенты)на изобретения, удостоверения на рационализаторские предложения, свидетельства (илипатенты), выдаваемые на промышленные образцы и др.

Заявка включает в себя заявление, о выдаче соответствующего документа наизобретение, техническое описание, расчет и чертеж общего вида конструкции. Взаявлении содержатся: просьба о выдаче авторского свидетельства на изобретение, егократкое название, фамилия, имя, отчество автора (или авторов) предполагаемогоизобретения, место работы, занимаемая должность, образование, ученая степень идомашний адрес. В заявлении должно отмечаться, публиковалось ли и рассматривалосьли Содержание лекционного материалае предполагаемого изобретения и если рассматривалось, то где, когда икем, каковы результаты; приводятся сведения о наличии разработанной техническойдокументации, об изготовлении опытного образца, его испытаниях и результатах этихиспытаний. В конце заявления даются сведения о приложениях, указывается число ихэкземпляров и на скольких листах выполнен каждый документ. Кроме этого, в заявлениимогут сообщаться и другие данные в зависимости от характера изобретения.Информация о технической стороне предполагаемого изобретения

содержится вописании изобретения, которое представляет собой технико-правовой документ,иллюстрируемый чертежами.Патент – это документ, удостоверяющий авторство определенного лица илигруппы лиц на данное изобретение, дающий этим лицам исключительное правоизготовлять и продавать изобретенные ими предметы.

2.6. Изготовление и оформление технической документацииПервыми техническими документами, которые возникают в процессе техническоготворчества, являются наброски, схемы, эскизы и предварительные расчеты. Этидокументы обычно являются черновиками для создания чертежа или других техническихдокументов. Производственные чертежи выполняются на бумаге стандартного формата.Государственными стандартами установлены форматы листов, применяемых длявыполнения чертежей во всех отраслях промышленности и строительства (таблица 1).

Таблица 1. – Размеры форматов.

Обозначение формата	Размер формата
A0	841×1189
A1	594×841
A2	420×594
A3	297×420
A4	210×297

Допускается при необходимости применять формат А5 (148х210), а также дополнительные форматы, образуемые увеличением коротких сторон основныхформатов на величину, кратную их размерам (таблица 2). Обозначение производногоформата состоит изобозначения основного формата и его кратности, согласно таблице 2,например: А0×2 (1189×1682).

Чертежи выполняются на ватмане, иногда используется пергаментная калька, накоторой можно работать карандашом, а также эмульсированная калька. Калька,покрытая эмульсионным слоем, приобретает ценные свойства: обычный карандаш даетна ней четкие линии.

Таблица 2. – Дополнительные форматы

Кратность	A0	A1	A2	A3	A4
2	1189×1682				
3	1189×2523	841×1782	594×1261	420×891	297×630
4		841×2378	594×1682	420×1189	297×842
5			594×2102	420×1486	297×1051
6				420×1783	297×1261
7				420×2080	297×1471
8					297×1682
9					297×1892

На каждом листе чертежа вычерчивается рамка, отстоящая от краев бумаги с трехсторон на 5 мм, а с левой стороны, если чертежи подлежат брошюровке, – на 20 мм.Чертежи большого формата складываются до размера формата А4. При этом листыскладывают изображением наружу так, чтобы основная надпись (угловой штамп)оказывалась на верхней лицевой стороне сложенного листа в его правом нижнем углу.Все надписи на чертежах сосредоточены в одном месте в специальноразграфленных трафаретках или угловых штампах, расположенных в правом нижнемуглу листа. В угловом штампе указываются все основные сведения о чертеже, чтопозволяет найти нужный документ среди массы других, установить технические данные, необходимые для изготовления изображенного на чертеже изделия (материал, масштаб,режим термообработки и др.). С

помощью углового штампа можно определитьразновидность чертежа (общий вид, чертеж сборочной единицы, детальный чертеж),узнать, к какому изделию относится этот чертеж, какие чертежи в свою очередь с нимсвязаны. Из Содержание лекционного материалая углового штампа выясняют, кто является автором даннойконструкций, дату утверждения чертежа, некоторые элементы техническойхарактеристики изделия. В угловом штампе помещаются также подписи лиц,
ответственных за правильность разработки и оформления технических документов, дата выпуска.

Основная надпись сборочных, детальных, габаритных, монтажных и другихчертежей имеет одни и те же графы и постоянный порядок их расположения.Стандарт устанавливает также дополнительные графы к основной надписи,которые должны быть на всех чертежах, схемах и текстовых документах.Дополнительные графы содержат сведения об инвентарных номерах подлинника (илидубликата) данного документа, полученных в архиве конструкторской организации, обобозначении документа, взамен или на основании которого выпущен данный документ, иподписи лиц, принявших подлинники в архив. Дополнительные графы располагаютсявдоль левого поля чертежа.Выше основной надписи или на отдельном листе в виде приложения к чертежу,если это чертеж общего вида или сборочный, вычерчивается спецификация, в которойопределяется состав сборочных единиц, комплекса и комплекта. В спецификацииуказываются: формат чертежа, зона, порядковый номер позиции сборочной единицы идеталей, производственный номер сборочной единицы и деталей, их наименования,количество сборочных единиц и деталей, необходимых для изготовления одногоэкземпляра изделия, примечание, в котором указываются замены сборочных единиц идеталей, наличие вариантов, заимствования из других проектов, аннулирование чертежейИмеются некоторые особенности в Содержание лекционного материалаи и оформлении основных надписейи чертежей, применяемых в области строительства, в электротехнике ирадиопромышленности, дорожном строительстве, горном деле.Основные сведения, которые обычно указываются в угловых штампахстроительных чертежей: наименования проектной организации и вышестоящего органа,название комплекса, объекта, чертежа, производственный номер комплекса, стадияпроектирования, часть проекта, номер листа, формат чертежа.

Текстовые технические документы могут быть выполнены машинописным,рукописным и типографским способами. Схема получения текстового техническогодокумента выглядит следующим образом: составление проекта документа автором,перепечатка его на пишущей машине или компьютере, согласование и корректирование,подписание руководящими лицами.

Для размещения утверждающих и согласовывающих подписей к текстовымдокументам составляется титульный лист.

На нем указываются:

- наименование министерства или ведомства, в ведении которого находится
организация, разработавшая данный документ;
- название самой организации;
- наименование изделия или его составной части;
- должности и подписи исполнителей и ответственных лиц;
- дата разработки документа.

В научно-исследовательских, конструкторско-технологических, проектныхорганизациях, научно-исследовательских лабораториях вузов, промышленныхпредприятий составляются технические документы научно-исследовательскогохарактера. Основным из них, в котором излагаются исчерпывающие сведения овыполненных экспериментах и этапах научного исследования, является отчет о теме.

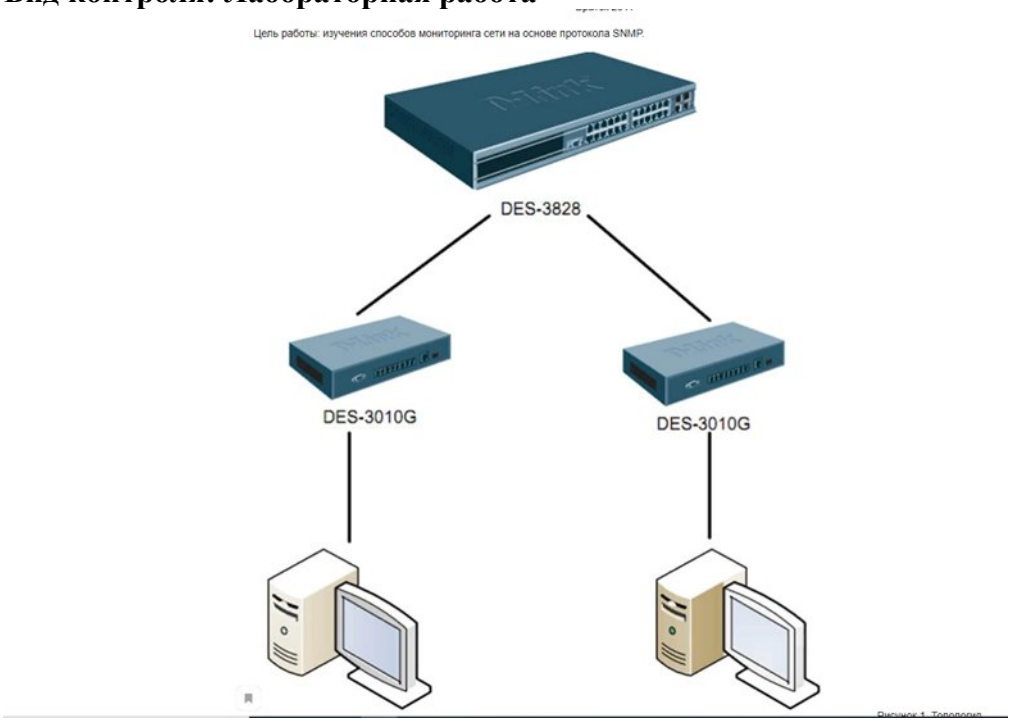
Структуру отчета о НИР:

- титульный лист,

- список исполнителей,
- реферат,
- Содержание лекционного материалае (оглавление),
- перечень сокращений,
- символов и специальных терминов с их определениями,
- условных обозначений;
- введение,
- основная часть,
- заключение,
- список использованных источников и литературы,
- приложения.

На титульном листе отчета о НИР указывается:
-официальное название организации-исполнителя, Министерства (ведомства), которому подчиняется организация;
-номер государственной регистрации, инвентарный номер отчета о НИР;
надписи о согласовании и утверждении отчета, в которых, кроме должностей, фамилий и инициалов, указываются ученые степени и звания лиц, утвердивших и подписавших документ;
-наименование темы, отчета (если последнее не совпадает с наименованием темы) и – в скобках – тип отчета (промежуточный, заключительный, этапный отчет и
-номер (шифр) темы, присвоенный ей в организации (ведомстве);
-должности, ученые степени и звания, фамилии и инициалы руководителей подразделений организации, руководителей НИР и ответственных исполнителей;
-место и год выпуска отчета.

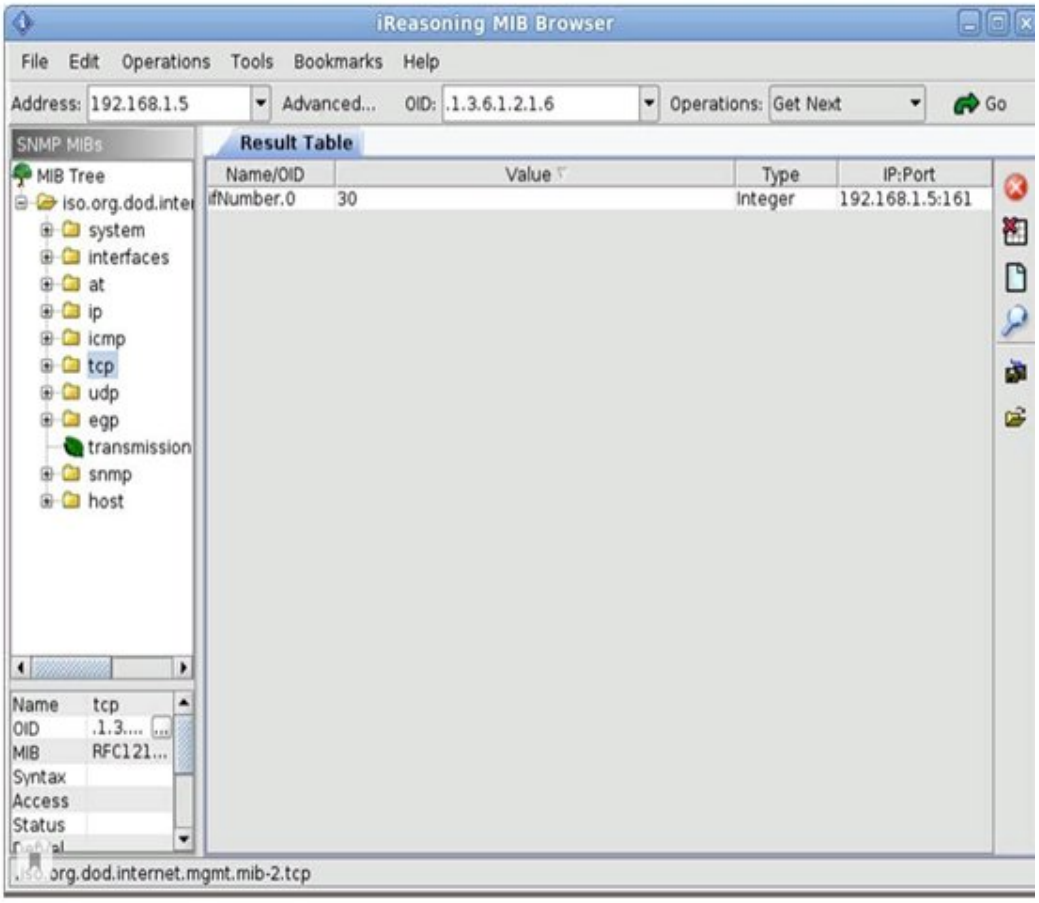
Практическая работа*Протокол управления SNMP*
Вид контроля: Лабораторная работа



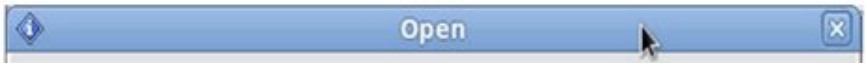
SNMP-протокол включен постоянно. На DES-3828 включается, после изменения парам

Serial Port Baud Rate	9600
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled detail setting
Multicast Router Only	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
Telnet TCP Port Number (1-65535)	23
Web Status	Enabled (TCP 80)
SNMP Status	Enabled
RMON Status	Disabled
Link Aggregation Algorithm	IP Source
Switch 802.1x	Disabled
Auth Protocol	RADIUS Eap
Jumbo Frame	Disabled
Syslog State	Disabled
DVMRP State	Disabled
PIM State	Disabled
RIP State	Disabled
OSPF State	Disabled
ARP Aging Time (0-65535)	40
CPU Interface Filtering	Disabled

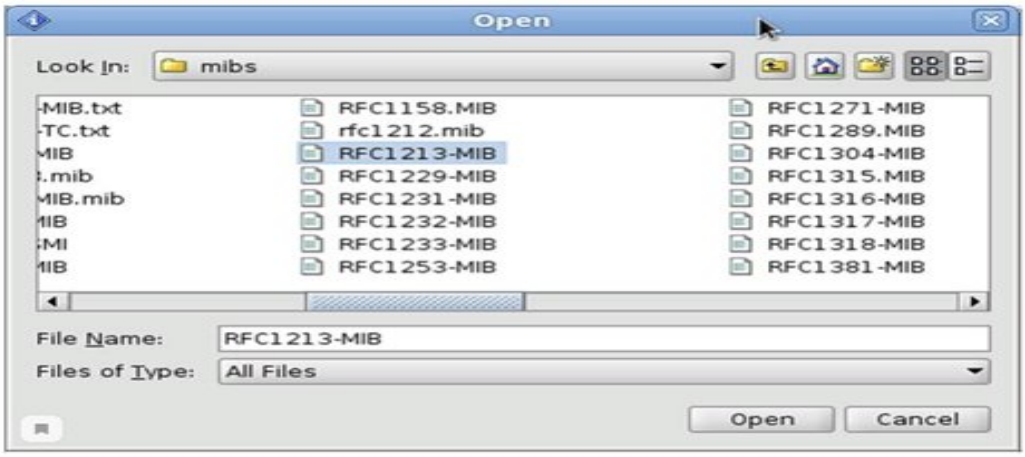
Запустите утилиту iReasoning MIB Browser.



Загрузите базу MIB RFC-1213.



Загрузите базу MIB RFC-1213.



На обоих коммутаторах (DES-3010 и DES-3828) выясните следующие параметры:

Коммутатор DES-3010

звание устройства, время работы устройства, службы, запущенные на

устройстве (ветвь system);

устройстве (ветвь system);

Result Table

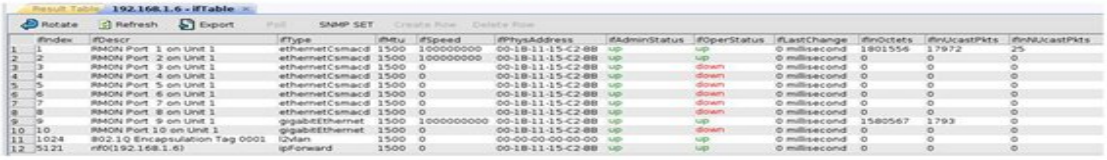
Name/OID	Value	Type	IP:Port
sysDescr.0	Dlink DES-3010G Fast Ethernet Switch	OctetSt...	192.168.1...
sysUpTime.0	28 minutes 55 seconds (173589)	TimeTicks	192.168.1...
sysServices.0	3	Integer	192.168.1...

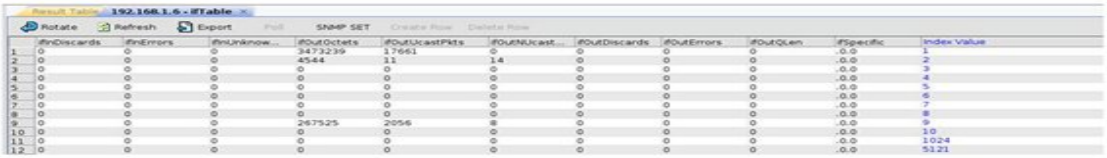
личество интерфейсов на устройстве

Result Table 192.168.1.6 - ifTable

Name/OID	Value	Type	IP:Port
ifNumber.0	12	Integer	192.168.1.6:161

держимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);





-адрес устройства

Result Table | 192.168.1.6 - ifTable | **192.168.1.6 - ipAddrTable**

Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

	ipAdEntAddr	ipAdEntIfInd...	ipAdEntNet...	ipAdEntBca...	ipAdEntRea...	Index Value
1	192.168.1.6	5121	255.255.255.0	1	15000	192.168.1.6

содержимое таблицы маршрутизации (ветвь ip)

Result Table | 192.168.1.6 - ifTable | 192.168.1.6 - ipAddrTable | **192.168.1.6 - ipRouteTable**

Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

	ipRouteDest	ipRouteIfIndex	ipRouteMetric1	ipRouteMetric2	ipRouteMetric3	ipRouteMetric4	ipRouteNex...	ipRouteType	ipRouteProto	ipRouteAge	ipRouteMask
1	192.168.1.0	5121	1	-1	-1	-1	192.168.1.6	direct	local	0	255.255.255.0

ipRouteMetric5	ipRouteInfo	Index Value
-1	.0.0	192.168.1.0

CP-соединения, установленные устройством (ветвь tcp)

Result Table | 192.168.1.6 - ifTable | 192.168.1.6 - ipAddrTable | 192.168.1.6 - ipRouteTable | **192.168.1.6 - tcpConnTable**

Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

	tcpConnState	tcpConnLoc...	tcpConnLoc...	tcpConnRe...	tcpConnRe...	Index Value
1	listen	0.0.0.0	23	0.0.0.0	0	0.0.0.0.23.0.0.0.0
2	listen	0.0.0.0	80	0.0.0.0	0	0.0.0.0.80.0.0.0.0
3	timeWait	192.168.1.6	80	192.168.1.2	47289	192.168.1.6.80.192.168.1.2.47289
4	timeWait	192.168.1.6	80	192.168.1.2	47290	192.168.1.6.80.192.168.1.2.47290

Коммутатор DES-3828

азвание устройства, время работы устройства, службы, запущенные на

устройстве (ветвь system);

Result Table

Name/OID	Value	Type	IP:Port
sysDescr.0	DES-3828 Fast-Ethernet Switch	OctetString	192.168.1.5:161
sysUpTime.0	58 minutes 45 seconds (352588)	TimeTicks	192.168.1.5:161
sysDescr.0	DES-3828 Fast-Ethernet Switch	OctetString	192.168.1.5:161

личество интерфейсов на устройстве

Result Table

Name/OID	Value	Type	IP:Port
ifNumber.0	30	Integer	192.168.1.5:161

держимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);

Result Table | 192.168.1.5 - ifTable

Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

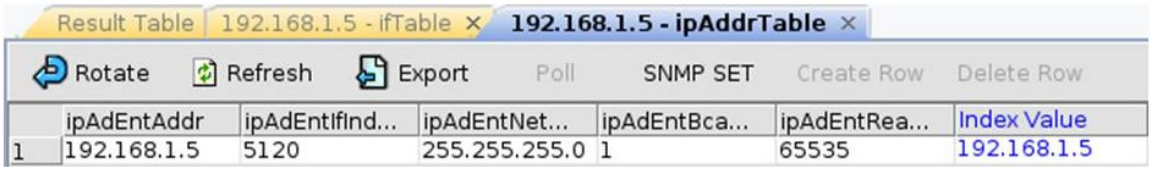
	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts	ifInNUcastPkts
1	1	RMON Port 1 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
2	2	RMON Port 2 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
3	3	RMON Port 3 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
4	4	RMON Port 4 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
5	5	RMON Port 5 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
6	6	RMON Port 6 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
7	7	RMON Port 7 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
8	8	RMON Port 8 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
9	9	RMON Port 9 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
10	10	RMON Port 10 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
11	11	RMON Port 11 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
12	12	RMON Port 12 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
13	13	RMON Port 13 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
14	14	RMON Port 14 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
15	15	RMON Port 15 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
16	16	RMON Port 16 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
17	17	RMON Port 17 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
18	18	RMON Port 18 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
19	19	RMON Port 19 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
20	20	RMON Port 20 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
21	21	RMON Port 21 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
22	22	RMON Port 22 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
23	23	RMON Port 23 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
24	24	RMON Port 24 on Unit 1	ethernetCsmacd	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
25	25	RMON Port 25 on Unit 1	gigabitEthernet	1500	1000000000	00-19-5B-F0-F1-00	up	up	0 millisecond	1312919	9432	3
26	26	RMON Port 26 on Unit 1	gigabitEthernet	1500	1000000000	00-19-5B-F0-F1-00	up	up	0 millisecond	88661	776	1
27	27	RMON Port 27 on Unit 1	gigabitEthernet	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
28	28	RMON Port 28 on Unit 1	gigabitEthernet	1500	0	00-19-5B-F0-F1-00	up	down	0 millisecond	0	0	0
29	1024	802.1Q Encapsulation...	l2vlan	1500	0	00-00-00-00-00-00	up	up	0 millisecond	0	0	0
30	5120	rif0(192.168.1.5)	ipForward	1500	0	00-19-5B-F0-F1-00	up	up	0 millisecond	0	0	0

Result Table | 192.168.1.5 - ifTable

Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

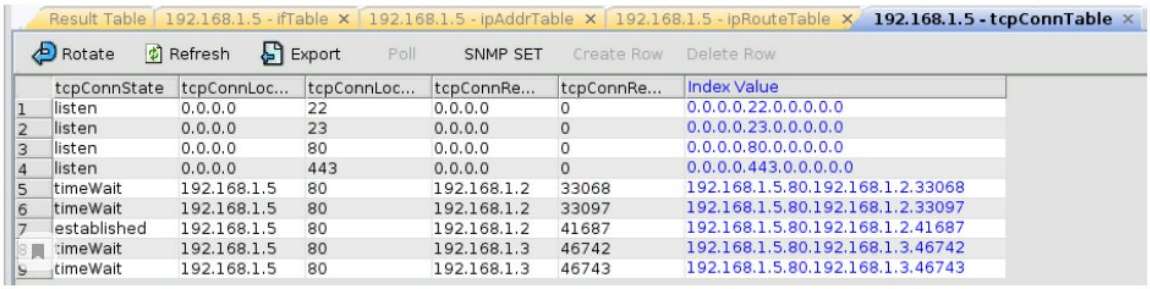
	ifInDiscards	ifInErrors	ifInUnknow...	ifOutOctets	ifOutUcastP...	ifOutNUcast...	ifOutDiscards	ifOutErrors	ifOutQLen	ifSpecific	Index Value
1	0	0	0	0	0	0	0	0	0	.0.0	1
2	0	0	0	0	0	0	0	0	0	.0.0	2
3	0	0	0	0	0	0	0	0	0	.0.0	3
4	0	0	0	0	0	0	0	0	0	.0.0	4
5	0	0	0	0	0	0	0	0	0	.0.0	5
6	0	0	0	0	0	0	0	0	0	.0.0	6
7	0	0	0	0	0	0	0	0	0	.0.0	7
8	0	0	0	0	0	0	0	0	0	.0.0	8
9	0	0	0	0	0	0	0	0	0	.0.0	9
10	0	0	0	0	0	0	0	0	0	.0.0	10
11	0	0	0	0	0	0	0	0	0	.0.0	11
12	0	0	0	0	0	0	0	0	0	.0.0	12
13	0	0	0	0	0	0	0	0	0	.0.0	13
14	0	0	0	0	0	0	0	0	0	.0.0	14
15	0	0	0	0	0	0	0	0	0	.0.0	15
16	0	0	0	0	0	0	0	0	0	.0.0	16
17	0	0	0	0	0	0	0	0	0	.0.0	17
18	0	0	0	0	0	0	0	0	0	.0.0	18
19	0	0	0	0	0	0	0	0	0	.0.0	19
20	0	0	0	0	0	0	0	0	0	.0.0	20
21	0	0	0	0	0	0	0	0	0	.0.0	21
22	0	0	0	0	0	0	0	0	0	.0.0	22
23	0	0	0	0	0	0	0	0	0	.0.0	23
24	0	0	0	0	0	0	0	0	0	.0.0	24
25	0	0	0	4110072	7861	1	0	0	0	.0.0	25
26	0	0	0	955338	853	3	0	0	0	.0.0	26

-адрес устройства



содержимое таблицы маршрутизации (ветвь ip)

CP-соединения, установленные устройством (ветвь tcp)



Выводы по работе: настроили SNMP-протокол на коммутаторах, научились работать с утилитой iReasoning MIB Browser и с её помощью выя различные параметры коммутаторов.

Практическое задание:*Основные характеристики протокола SNMP*

Цель работы: Ознакомление с протоколом SNMP и программными утилитами (net-snmp) для работы с ним.

Введение.

SNMP (англ. Simple Network Management Protocol — простой протокол управлениясетями) — это протокол управления сетями связи на основе архитектуры UDP. Устройства, которые обычно поддерживают SNMP это маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемы и т. д. SNMP является компонентом стека протоколов TCP/IP, как это определено Инженерным советом Интернет (Internet Engineering Task Force, IETF). Он состоит из набора стандартов сетевого управления, включая протокол передачи данных прикладного уровня, схему базы данных и набора объектов.

Обычно при использовании SNMP присутствуют управляемые и управляющие системы. В состав управляемой системы входит компонент, называемый агентом, который отправляет отчёты управляющей системе. По существу SNMP агенты передают управленческую информацию на управляющие системы как переменные (такие как «свободная память», «имя системы», «количество работающих процессов»).

Управляющая система может получить информацию через операции протокола GET, GETNEXT и GETBULK. Агент может самостоятельно без запроса отправить данные, используя операцию протокола TRAP или INFORM. Управляющие системы могут также отправлять конфигурационные обновления или контролирующие запросы, используя операцию SET для непосредственного управления системой. Операции конфигурирования и управления используются только тогда, когда нужны изменения в сетевой инфраструктуре. Операции мониторинга обычно выполняются на регулярной основе.

Управляющая система может получить информацию через операции протокола GET, GETNEXT и GETBULK. Агент может самостоятельно без запроса отправить данные, используя операцию протокола TRAP или INFORM. Управляющие системы могут также

отправлять конфигурационные обновления или контролирующие запросы, используя операцию SET для непосредственного управления системой. Операции конфигурирования и управления используются только тогда, когда нужны изменения в сетевой инфраструктуре. Операции мониторинга обычно выполняются на регулярной основе.
Переменные, доступные через SNMP, организованы в иерархии. Эти иерархии и другие метаданные (такие, как тип и описание переменной) описываются Базами Управляющей Информации.

Management Information Bases (MIBs)

SNMP не определяет, какую информацию (какие переменные) управляемая система должна предоставлять. Наоборот, SNMP использует расширяемую модель, в которой доступная информация определяется Базами Управляющей Информации (MIB — Management Information Base). Базы Управляющей Информации описывают структуру управляющей информации устройств. Они используют иерархическое пространство имён, содержащее уникальный идентификатор объекта (англ. object identifier (OID)). Грубо говоря, каждый уникальный идентификатор объекта идентифицирует переменную, которая может быть прочитана или установлена через SNMP. MIBы используют нотацию, определённую в ASN.1.
Иерархия MIB может быть изображена как дерево с безымянным корнем, уровни которого присвоены разными организациями. На самом высоком уровне MIB OIDы принадлежат различным организациям, занимающимся стандартизацией, в то время как на более низком уровне OIDы выделяются ассоциированными организациями. Эта модель обеспечивает управление на всех слоях сетевой модели OSI, так как MIBы могут быть определены для любых типов данных и операций.
Управляемый объект — это одна из любого числа характеристик, специфических для управляемого устройства. Управляемый объект включает в себя один или более экземпляров объекта (идентифицируемых по OID), которые на самом деле переменные.
Существует два типа управляемых объектов:
Скалярные объекты определяют единственный экземпляр объекта.
Табличные объекты определяют множественные, связанные экземпляры объектов, которые группируются в таблицах MIB.
Идентификатор объекта (OID) уникально идентифицирует управляемый объект в иерархии MIB.

Управляющая база данных MIB

Категории объектов MIB
Системные переменные
Переменные интерфейсов
IP-группа
TCP-группа
ICMP-группа
AT-группа (преобразование адресов)
SNMP-группа
UDP-группа

Расширения MIB, специфические для компаний производителей оборудования
Префиксы фирм-производителей оборудования
Формат записи маршрутной информации
Группа RMON

Вся управляющая информация для контроля ЭВМ и маршрутизаторами Интернет концентрируется в базе данных MIB (Management Information Base, RFC-1213 или STD0017). Именно эти данные используются протоколом SNMP. Система SNMP состоит из трех частей: менеджера SNMP, агента SNMP и базы данных MIB. Агент SNMP должен находиться резидентно в памяти объекта управления. SNMP-менеджер может быть частью системы управления сетью NMS (Network Management System), что реализуется, например, в маршрутизаторах компании CISCO (CiscoWorks).

MIB определяет, например, что IP программное обеспечение должно хранить число всех октетов, которые приняты любым из сетевых интерфейсов, управляющие программы могут только читать эту информацию.

Согласно нормативам MIB управляющая информация делится на восемь категорий.

Категории объектов MIB

MIB-категория включает в себя информацию о (префикс=1.3.6.1.2.1)

MIB-категория	Описание	Код
system	Операционная система ЭВМ или маршрутизатора.	1
Interfaces	Сетевой интерфейс.	2
addr. trans	Преобразование адреса (напр., с помощью ARP).	3
IP	Программная поддержка протоколов Интернет.	4
ICMP	Программное обеспечение ICMP-протокола.	5
TCP	Программное обеспечение TCP-протокола.	6
UDP	Программное обеспечение UDP-протокола.	7
EGP	Программное обеспечение EGP-протокола.	8
cmot	(группа в настоящее время не используется).	9
Trans	Transmission	10
SNMP	Программное обеспечение SNMP-протокола.	11

Системные переменные

Системные переменные MIB (префикс=1.3.6.1.2.1.1)

Системная переменная	Описание	Код
Sysdescr	Текстовое описание объекта;	1
Sysobjectid	Идентификатор производителя в рамках дерева 1.3.6.1.4.1	2
Sysuptime	Время с момента последней загрузки системы (timeticks);	3
Syscontact	Имя системного менеджера и способы связи с ним;	4
Sysname	Полное имя домена;	5
Syslocation	Физическое местоположение системы;	6
Sysservice	Величина, которая характеризует услуги, предоставляемые узлом (сумма номеров уровней модели OSI);	7

Переменные интерфейсов

Переменные **IFtable** (интерфейсы; префикс=1.3.6.1.2.1.2)

Переменная описания интерфейсов (iftable)	Тип данных	Описание	ifEntry
IFindex	integer	Список интерфейсов от 1 до ifnumber.	1
IfDescr	displaystring	Текстовое описание интерфейса.	2
IfType	integer	Тип интерфейса, например, 6 - ethernet; маркерное кольцо; 23 - PPP; 28 - SLIP.	3
IfNumber	integer	Число сетевых интерфейсов.	
IfMTU	integer	mtu для конкретного интерфейса;	4
IfSpeed	gauge	Скорость в бит/с.	5
IfPhysaddress	physaddress	Физический адрес или строка нулевой длины для интерфейсов без физического адреса (напр. последовательный).	6
IfAdminStatus	[1…3]	Требуемое состояние интерфейса: 1 - включен; 2 - выключен; 3 - тестируется.	7
IfOperStatus	[1…3]	Текущее состояние интерфейса: 1 - включен; 2 - выключен; 3 - тестируется.	8

IfLastchange	timeticks	Sysuptime, когда интерфейс оказался в данном состоянии.	9
IfInOctets	counter	Полное число полученных байтов.	10
IfInUcastpkts	counter	Число пакетов, доставленных на верхний системный уровень (unicast).	11
IfInNUcastpkts	counter	Число пакетов, доставленных на верхний системный уровень (unicast).	12
IfInDiscads	counter	Число полученных но отвергнутых пакетов.	13
IfInErrors	counter	Число пакетов, полученных с ошибкой;	14
IfInUnknownProtos	counter	Число пакетов, полученных с ошибочным кодом протокола;	15
IfOutOctets	counter	Число отправленных байтов;	16
IfOutUcastPkts	counter	Число unicast - пакетов, полученных с верхнего системного уровня;	17
IfOutNucastPkts	counter	Число мультикастинг - и широковещательных пакетов, полученных с верхнего системного уровня;	18
IfOutDiscads	counter	Количество отвергнутых пакетов из числа отправленных;	19
IfOutErrors	counter	Число отправленных пакетов, содержащих ошибки;	20
IfOutQlen	gauge	Число пакетов в очереди на отправку;	21

Ниже представлена таблица цифро-точечного представления переменных, характеризующих состояние интерфейса. Эта таблица может быть полезной для программистов, занятых проблемами сетевой диагностики.

Название объекта	Цифра-точечное представление
org	1.3
dod	1.3.6

internet	1.3.6.1
directory	1.3.6.1.1
mgmt	1.3.6.1.2
experimental	1.3.6.1.3
private	1.3.6.1.4
enterprises	1.3.6.1.4.1
security	1.3.6.1.5
snmpV2	1.3.6.1.6
snmpDomains	1.3.6.1.6.1
snmpProxys	1.3.6.1.6.2
snmpModules	1.3.6.1.6.3
snmpMIB	1.3.6.1.6.3.1
snmpMIBObjects	1.3.6.1.6.3.1.1
snmpTraps	1.3.6.1.6.3.1.1.5
mib-2	1.3.6.1.2.1
ifMIB	1.3.6.1.2.1.31
interfaces	1.3.6.1.2.1.2
ifMIBObjects	1.3.6.1.2.1.31.1
ifConformance	1.3.6.1.2.1.31.2
ifTableLastChange	1.3.6.1.2.1.31.1.5
ifXTable	1.3.6.1.2.1.31.1.1
ifStackTable	1.3.6.1.2.1.31.1.2
ifStackLastChange	1.3.6.1.2.1.31.1.6
ifRcvAddressTable	1.3.6.1.2.1.31.1.4
ifTestTable	1.3.6.1.2.1.31.1.3
ifXEntry	1.3.6.1.2.1.31.1.1.1

ifName	1.3.6.1.2.1.31.1.1.1.1
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5
ifLinkUpDownTrapEnable	1.3.6.1.2.1.31.1.1.1.14
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17
ifAlias	1.3.6.1.2.1.31.1.1.1.18
ifCounterDiscontinuityTime	1.3.6.1.2.1.31.1.1.1.19
ifStackEntry	1.3.6.1.2.1.31.1.2.1
ifStackHigherLayer	1.3.6.1.2.1.31.1.2.1.1
ifStackLowerLayer	1.3.6.1.2.1.31.1.2.1.2
ifStackStatus	1.3.6.1.2.1.31.1.2.1.3
ifRcvAddressEntry	1.3.6.1.2.1.31.1.4.1
ifRcvAddressAddress	1.3.6.1.2.1.31.1.4.1.1
ifRcvAddressStatus	1.3.6.1.2.1.31.1.4.1.2
ifRcvAddressType	1.3.6.1.2.1.31.1.4.1.3
ifTestEntry	1.3.6.1.2.1.31.1.3.1
ifTestId	1.3.6.1.2.1.31.1.3.1.1
ifTestStatus	1.3.6.1.2.1.31.1.3.1.2
ifTestType	1.3.6.1.2.1.31.1.3.1.3
ifTestResult	1.3.6.1.2.1.31.1.3.1.4
ifTestCode	1.3.6.1.2.1.31.1.3.1.5
ifTestOwner	1.3.6.1.2.1.31.1.3.1.6

ifGroups	1.3.6.1.2.1.31.2.1
ifCompliances	1.3.6.1.2.1.31.2.2
ifGeneralInformationGroup	1.3.6.1.2.1.31.2.1.10
ifFixedLengthGroup	1.3.6.1.2.1.31.2.1.2
ifHCFixedLengthGroup	1.3.6.1.2.1.31.2.1.3
ifPacketGroup	1.3.6.1.2.1.31.2.1.4
ifHCPacketGroup	1.3.6.1.2.1.31.2.1.5
ifVHCPacketGroup	1.3.6.1.2.1.31.2.1.6
ifRcvAddressGroup	1.3.6.1.2.1.31.2.1.7
ifStackGroup2	1.3.6.1.2.1.31.2.1.11
ifCounterDiscontinuityGroup	1.3.6.1.2.1.31.2.1.13
ifGeneralGroup	1.3.6.1.2.1.31.2.1.1
ifTestGroup	1.3.6.1.2.1.31.2.1.8
ifStackGroup	1.3.6.1.2.1.31.2.1.9
ifOldObjectsGroup	1.3.6.1.2.1.31.2.1.12
ifCompliance2	1.3.6.1.2.1.31.2.2.2
ifCompliance	1.3.6.1.2.1.31.2.2.1
ifNumber	1.3.6.1.2.1.2.1
ifTable	1.3.6.1.2.1.2.2
ifEntry	1.3.6.1.2.1.2.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6

ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22

IP-группа

Практическое задание:*Набор услуг (PDU) протокола SNMP*

Тестовые задания

1.Какими объектами может управлять Простой протокол управления сетью (SNMP)?

Ответ:

(1) маршрутизаторами фирмы CISCO
(2) любыми устройствами на физическом уровне
(3) устройствами на сети Ethernet
(4) на любой сети Интернет, образованной на локальных и общедоступных сетях

2.Какие задачи может выполнить программа SNMP?

Ответ:

(1) определить состояние устройств сети
(2) определить состояние сетевого трафика
(3) интерпретировать и высылать результат статистики управляемых объектов
(4) все перечисленное выше

3.Какой протокол принимает сообщение станции менеджера (SNMP — клиента) сообщение агенту (SNMP — серверу) запрос о числе полученных пользовательских UDP - дейтаграмм?

Ответ:

(1) SMI
(2) MIB
(3) ANSI
(4) RIP

4.К какому определению простого типа данных в протоколе SMI принадлежат следующие типы INTEGER, OCTET STRING ObjectIndetifer?

Ответ:

(1) MIB
(2) SMI
(3) SNMP
(4) ASN.1

5.Какое значение имеет поле длины в протоколе SMI если значение длины равно 2 байта?

Ответ:

(1) младший бит равен 0
(2) старший бит равен (1)
(3) младший бит равен (1)
(4) старший бит равен (0)

6.Какой пакет PDU посылается от менеджера (клиента) к агенту (серверу) программой SNMP , чтобы извлечь значение переменной?

Ответ:

(1) Get Request
(2) Get BulkRequest
(3) Set Request
(4) Response

7.Какой пакет PDU посылается от одного менеджера(клиента) программой SNMP другому менеджеру (клиенту) , чтобы получить значение некоторых переменных?

Ответ:

(1) Trap
(2) InformRequest
(3) PDU рапорт
(4) Response

8.Какое поле формата PDU SNMP , которое используется для извлечения или установки значений менеджером ?

Ответ:

(1) PDU-тип
(2) запрос ID
(3) состояние ошибки
(4) VarBindList

9.Какую концепцию использует протокол SNMP?

Ответ:
(1) каждый хост может управлять другим
(2) управление возможно только соседями
(3) управление по территориальному списку
(4) несколько станций менеджеров управляют набором агентов

10.Какой протокол использует SNMP для определения правил формального описания объекта (имени, тип объекта)?
Ответ:
(1) SMI
(2) MIB
(3) ANSI
(4) RIP

11.Какой протокол находит тип (целое) и имя объекта при запросе о числе полученных пользовательских UDP - дейтаграмм?
Ответ:
(1) SMI
(2) MIB
(3) ANSI
(4) RIP

12.К какому определению простого типа данных в протоколе SMI принадлежат следующие типы INTEGER, OCTET STRING ObjectIndetifer?
Ответ:
(1) MIB
(2) SMI
(3) SNMP
(4) ASN.1

13.Какой пакет PDU посылается от менеджера (клиента) к агенту (серверу) программой SNMP , чтобы извлечь большое количество данных?
Ответ:
(1) Get Request
(2) Get BulkRequrst
(3) Set Request
(4) Response

14.Какой пакет PDU посылается от одного менеджера(клиента) программой SNMP другому менеджеру (клиенту) , чтобы получить сообщение о некоторых ошибках?
Ответ:
(1) Trap
(2) InformRequest

(3) PDU рапорт
(4) Response

15.Какое поле формата PDU SNMP , которое используется для извлечения или установки значений менеджером ?
Ответ:
(1) PDU-тип
(2) запрос ID

(3) состояние ошибки
(4) VarBindList

Практическое задание:*Формат сообщений SNMP*

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*

Исходные данные
Сообщение 1

0000: 08 00 5a e8 02 8e 00 00 0c 7c 02 f1 08 00 45 80
0010: 01 37 9c bf 00 00 10 11 70 56 c0 b5 95 ca c2 b5
0020: 95 66 00 a1 c0 7a 01 23 7b 84 30 82 01 17 02 01
0030: 00 04 05 61 63 2d 30 32 a2 82 01 09 02 04 35 97
0040: ac 59 02 01 00 02 01 00 30 81 fa 30 0f 06 08 2b
0050: 06 01 02 01 01 03 00 43 03 73 d4 5a 30 11 06 0a
0060: 2b 06 01 02 01 02 02 01 05 03 42 03 00 fa 00 30
0070: 0f 06 0a 2b 06 01 02 01 02 02 01 08 03 02 01 01
0080: 30 0f 06 0a 2b 06 01 02 01 02 02 01 09 03 43 01
0090: 00 30 12 06 0a 2b 06 01 02 01 02 02 01 0a 03 41
00a0: 04 04 12 5a 5d 30 11 06 0a 2b 06 01 02 01 02 02

00b0: 01 0b 03 41 03 08 6f da 30 0f 06 0a 2b 06 01 02
00c0: 01 02 02 01 0c 03 41 01 07 30 0f 06 0a 2b 06 01
00d0: 02 01 02 02 01 0d 03 41 01 00 30 0f 06 0a 2b 06
00e0: 01 02 01 02 02 01 0e 03 41 01 00 30 12 06 0a 2b
00f0: 06 01 02 01 02 02 01 10 03 41 04 13 9c 96 fa 30
0100: 11 06 0a 2b 06 01 02 01 02 02 01 11 03 41 03 08
0110: 0d 32 30 0f 06 0a 2b 06 01 02 01 02 02 01 12 03
0120: 41 01 00 30 0f 06 0a 2b 06 01 02 01 02 02 01 13
0130: 03 41 01 00 30 0f 06 0a 2b 06 01 02 01 02 02 01
0140: 14 03 41 01 02

Практическое задание:*Задачи управления: анализ производительности сети*

Цель работы: Анализ производительности сети Ethernet.

Предложенная нагрузка - это количество данных, которые должна передать сеть, или другими словами, это запрос на пропускную способность, выданный пользователем в настоящее время. Этот показатель контрастирует с производительностью сети, которая показывает, сколько информации действительно прошло через ЛВС в заданное время.

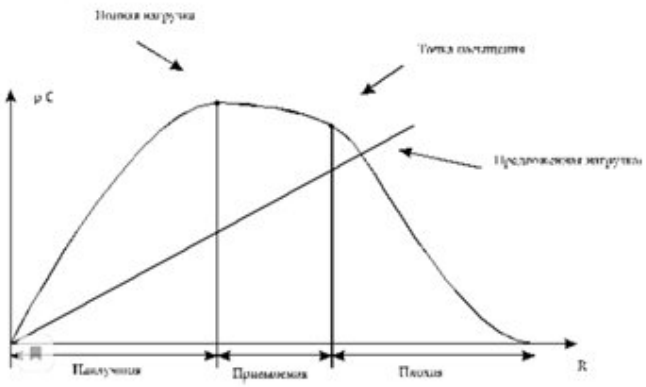
Сравним *нормированную производительность ρ с нормированной нагрузкой R.*

$$R = \lambda \cdot t_k \quad (3.1)$$

$$p = Тзш/<время\ моделирования> \quad (3.2)$$

$$p<C,$$

где λ – суммарная интенсивность потока запросов в сети, кадр/сек;
t_k –время передачи кадра, сек;
Тзш - время занятости шины (время, занятое бесконфликтной передачей запросов);
C – пропускная способность сети;
ρ – нормированная производительность или коэффициент фактической загрузки сети, который является результатом имитационного моделирования сети.
+С возрастанием предложенной нагрузки соответственно увеличивается производительность сети, и в некоторый момент наступит точка полного её "использования. При дальнейшем повышении предложенной нагрузки рост производительности ЛВС прекратится из-за высокой степени конкуренции за среду передачи. Если же нагрузка будет возрастать и дальше, то наступит момент, когда этот показатель начнет резко падать. Это явление называется *крахом Ethernets*.



Если сеть не загружена, то она будет работать быстро, поскольку предложенная нагрузка не превышает её возможностей. Именно в этом режиме работает большинство сетей Ethernet.
Не существует способа прямо измерить предложенную нагрузку, найти точку полного использования сети или определить точку её насыщения. Тем не менее, можно увидеть сеть, понять её, и пронаблюдать за изменением во времени различных её показателей. Лучший способ установить и проанализировать производительность сети - произвести *базирование,* т.е. измерить характеристики производительности, а затем сравнить их с известной базой. *Виза* — это набор соответствующих показателей производительности, измеренных при конкретной работе сетевой системы в условиях нормальной загрузки, желательно поближе к точке полного использования. Для создания базы наиболее употребительны следующие показатели:

- показатель использования сети;
- количество широковещательных кадров в секунду;
- количество кадров в секунду;
- процент коллизий.

Для сбора статистики по перечисленным показателям используются *протокол SNMP* (Simple Network Management Protocol, простой протокол управления сетью) и *стандарт RMON* (Remote Network Monitoring, стандарт дистанционного мониторинга сети). RMON предназначен для дополнения информации, которая может быть получена и использована в рамках протокола SNMP.
Базирование позволяет администратору следить **за** работой сети, своевременно выявлять её перегруженность (до того, как пользователи начнут считать это проблемой). Перегруженность может быть вызвана применением нового приложения или добавлением пользователей в сети.
Эффективным решением проблемы перегруженности является использование *моста* (коммутирующего концентратора: переключателе). Если сеть Ethernet (область коллизий Ethernet) оказывается перегруженной, то с помощью моста её можно разделить на подсети Ethernet (отдельные области коллизий Ethernet). Это значительно снижает конкуренцию пользователей за сеть и приводит к повышению эффективности её работы. Мост предназначен для передачи пакетов данных из одной подсети в другую. С функциональной точки зрения мосты относятся к канальному уровню эталонной модели ВОС. В отличие от повторителей (репитеров), мосты выполняют *фильтрацию* пакетов данных. Это значит, что в подсеть №2 будут попадать только те пакеты, которые предназначены для узлов этой подсети, а пакеты, предназначенные для узлов подсети №1, из которой они поступают, будут возвращаться обратно.

Исходные данные

Исходные данные остаются прежними, как в лабораторной работе №1, за исключением коэффициента загрузки (нормированной нагрузки) *R.* Для проведения серии экспериментов принять *R* равной:

Исходные данные

Первая серия экспериментов	0,1	0,3	0,5	0,7	0,9
Вторая серия экспериментов	0,9	1,1	1,3	1,5	2

Порядок выполнения работы

1. Используя формулу (1.11) лабораторной работы №1, определите суммарные интенсивности X потока запросов для всех точек каждой серии экспериментов. Для облегчения дальнейшего расчета и процесса реконструирования можно принять емкость каждого источника равной 1, т.о. будем полагать, что все источники имеют одинаковую интенсивность. Используя формулу (1.10) лабораторной работы №1, определите интенсивности (нестационарности потока) источников для всех точек каждой серии экспериментов.
2. Используя Реконструктор СИМЛВС, задайте первую серию экспериментов в режиме 1 (интенсивность запросов = var, время передачи = const). В качестве аргумента функции коэффициента фактической загрузки выберите коэффициент предложенной нагрузки в соответствии с исходными данными первой серии экспериментов,
3. Используя Симулятор, проведите первую серию экспериментов.
4. Используя Анализатор результатов, определите зависимость коэффициента фактической загрузки от коэффициента предложенной нагрузки.
5. Повторите пункты 1,2,3 для второй серии экспериментов.
6. Дайте оценку зависимости коэффициента фактической загрузки от коэффициента предложенной нагрузки.

Практическое задание: *Задачи управления: анализ надежности сети*

Тестовые задания

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением Содержание лекционного материалая информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Практическое задание:*Управление безопасностью в сети*

Лабораторная работа

Политику безопасности можно сравнить с пограничником, охраняющим границу страны. Ниже мы рассмотрим два способа улучшения безопасности работы нашей виртуальной сети за два приема.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем — это уязвимость)

Часто при установке Windows пароль администратора пустой и этим может воспользоваться злоумышленник. Иначе говоря, при установке Windows XP в автоматическом режиме с настройками по умолчанию мы имеем пользователя **Администратор** с пустым паролем и любой **User** может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду **Мой компьютер-Панель управления-Администрирование-Управление компьютером-Локальные пользователи-Пользователи** (рис. 1).

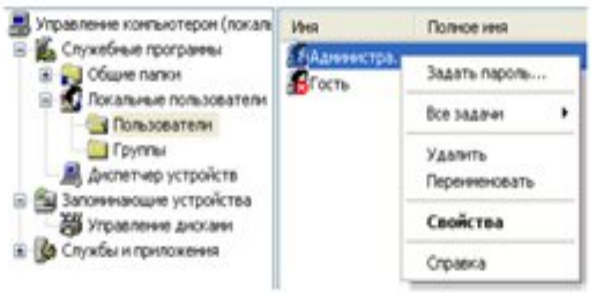


Рис. 1. Окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на **Администраторы** зададим администратору пароль, например, 12345. Это плохой пароль, но лучше, чем ничего. Теперь в окне **Администрирование** зайдем в **Локальную политику безопасности**. Далее идем по веткам дерева: **Локальные политики-Параметры безопасности-Учетные записи: Переименование учетной записи Администратор** (рис..2).

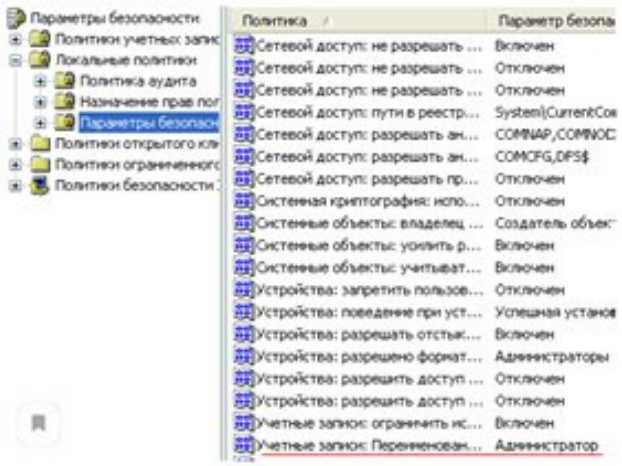


Рис. 2. Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя **Администратор** заменим на **Admin** (рис. 3).

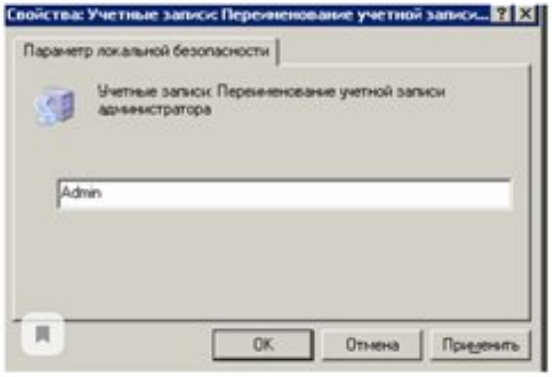


Рис. 3. Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная запись Admin с паролем 12345 и правами администратора (рис. 4).

Рис. 4. Окно входа в ОС Windows XP

Все, теперь мы имеем пользователя **Администратор** с паролем, одна из уязвимостей системы устранена.

Практическое задание: *Учет трафика в сети*

Лабораторная работа

Цель уметь и разрабатывать схему соединения и анализировать трафиклокальной сети на примере протоколов ARP, DNS и HTTPКраткая теоретическая справкаВ этой лаб. работе будем рассматривать два типа трафика: broadcast(широковещательный, на прим. проток ARP) и unicast (на прим. пре-лаhttp).Здесь используетсяанализатор трафика Wireshark свободнораспространяемый (лицензия GNU GPL).Информация о структуре пакета в Wireshark выводится в виде таблицанализа (рис. 1).

Таблица анализа представляет собой три поля, которые заполняютсядинамически по мере поступления пакетов. В основной части представленаинформация о соединении: MAC-адреса источника и получателя, IP-адресаисточника и получателя, протокол, порт отправителя и порт получателя.Обратите внимание – зарезервированные порты часто обозначаются именемпротокола: например, порты 80 и 8080 могут обозначаться как http. Однастрока в этой таблице относится к одному пакету. При выделении строки вдвух других окнах появляется информация о структуре пакета.

Поле со структурой пакета позволяет определить, как заполнены поляпротоколов в соответствии со стандартом. Это позволяет определить адресаотправителя и получателя, номер порта, корректность контрольной суммы ит.п. Поле с представлением пакета в ASCII кодах и 16-ричной системе даетпредставление о реальном виде пакета припередаче по сети. В большинствеанализаторов предусмотрена возможность выделения пункта в поле соструктурой пакета и одновременное выделение соответствующих знаков вполе с представлением пакета в 16-ричной системе.

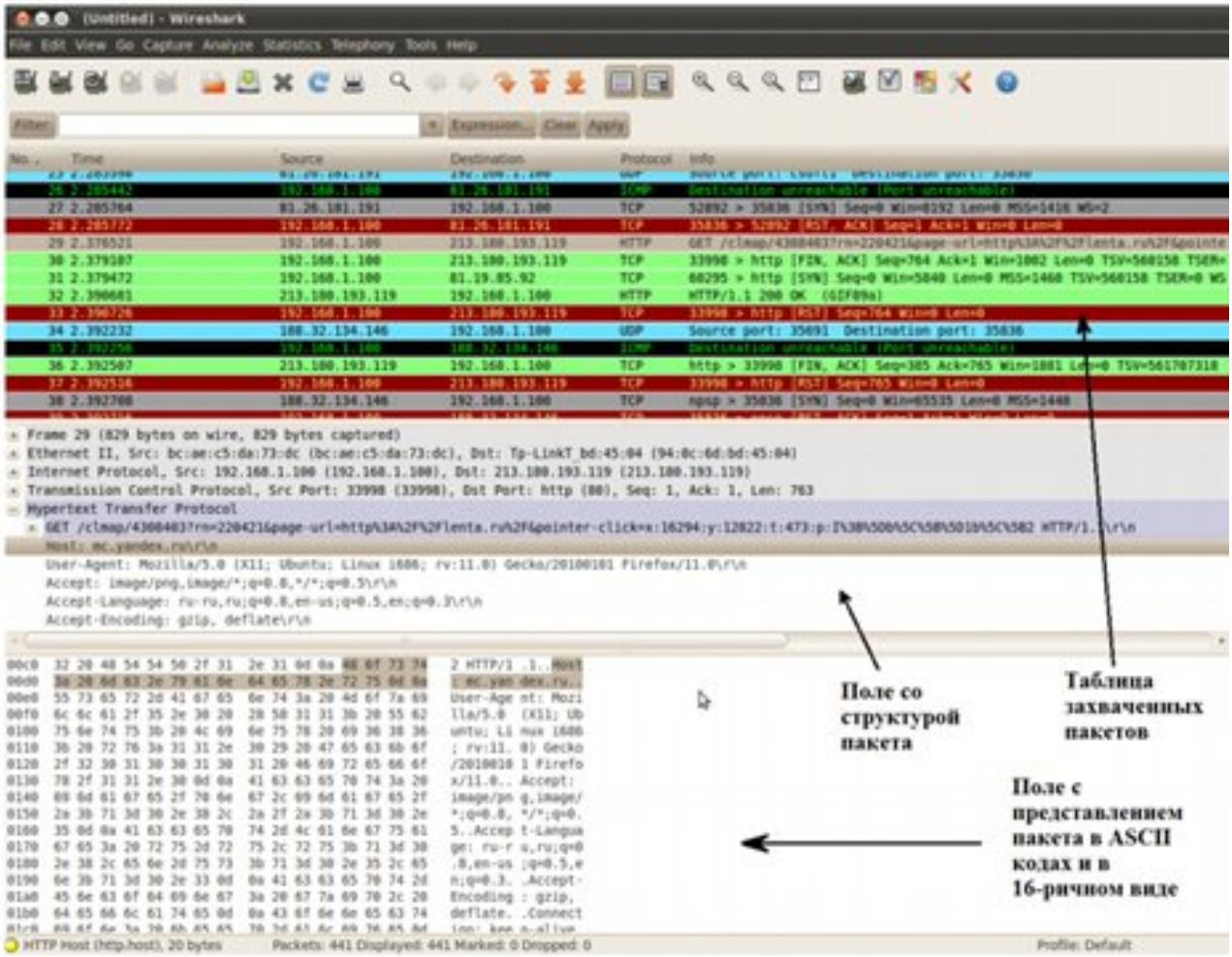


Рис. 1 – Пример таблицы анализа: пакет http, запрос к серверу

Также анализатор трафика позволяет собрать статистику о пакетах, проходящих по сети на различных уровнях модели TCP/IP. В качестве примера на рисунке 2 представлена статистика по размерам пакетов (Statistics®PacketLengths), а на рисунке 3 – по типам протоколов и видам данных, встречающихся в захваченном трафике (Statistics®ProtocolHierarchy).

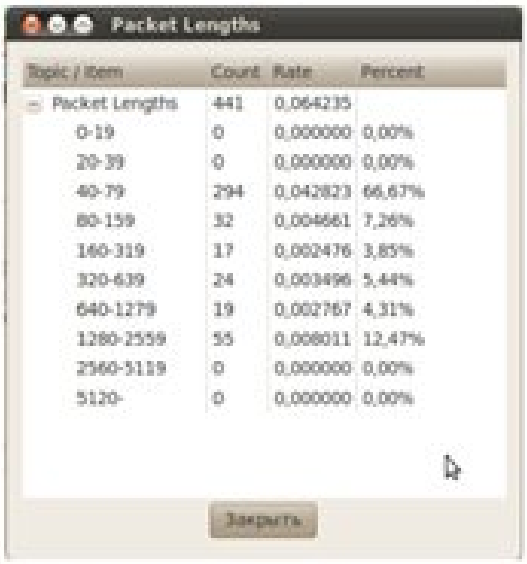


Рис. 2 – Пример статистики по размерам пакетов

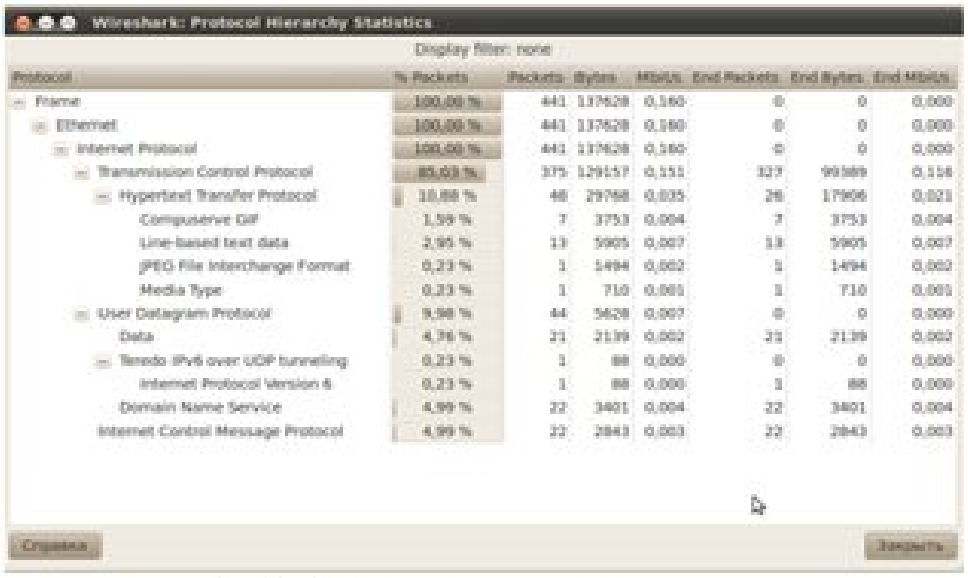


Рис. 3 – Пример статистики по типам протоколов.

При необходимости можно визуально оценить на общем графике интенсивность интересующих видов трафика по протоколам (до пяти протоколов одновременно), настроив соответствующим образом фильтры в окне IOGraphs(как показано на рисунке 4). Данный инструмент находится в меню Statistics®IOGraphs.

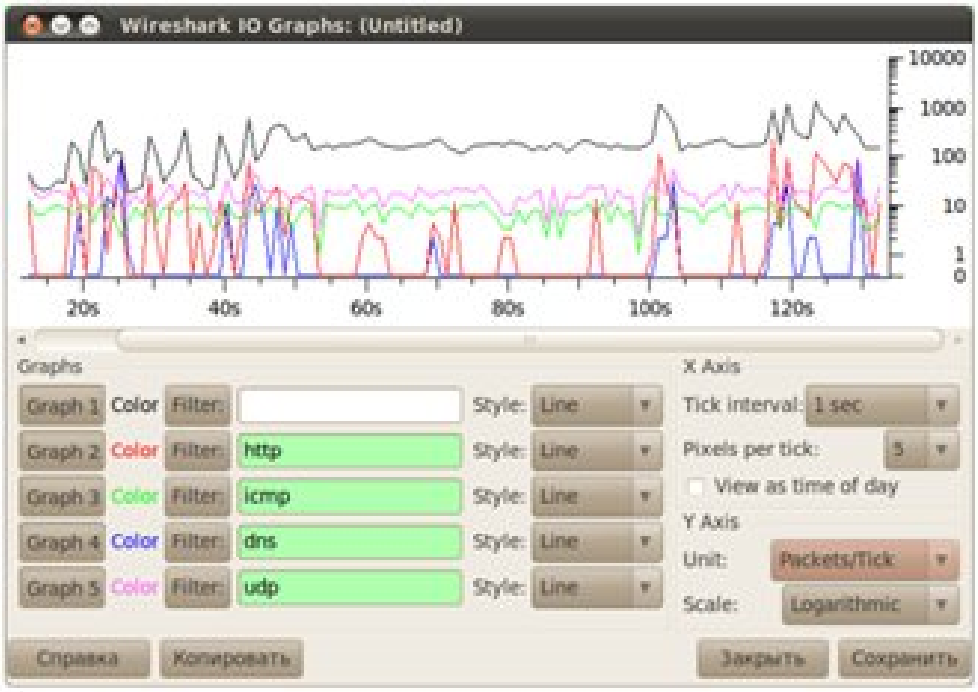


Рис. 4 – Графики интенсивности захваченного трафика.

Кроме того, в большинстве анализаторов можно увидеть статистику по хостам. На сетевом уровне такая статистика (Statistics®IPDestinations) позволяет оценить долю трафика, соответствующую конкретным IP-адресам и используемым ими протоколам (см. рис. 5). Инструмент GraphAnalysis из меню Statistics, окно которого показано на рисунке 6,позволяет в графическом виде представлять процедуры обмена данными на основании захваченного трафика.

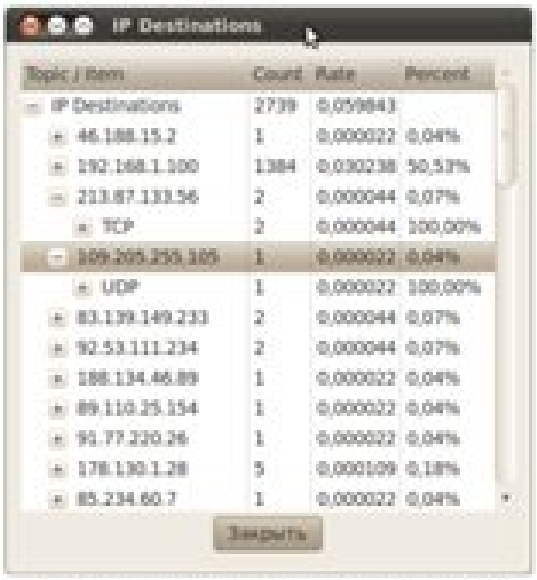


Рис. 5 – Статистика IP-адресов в захваченном трафике

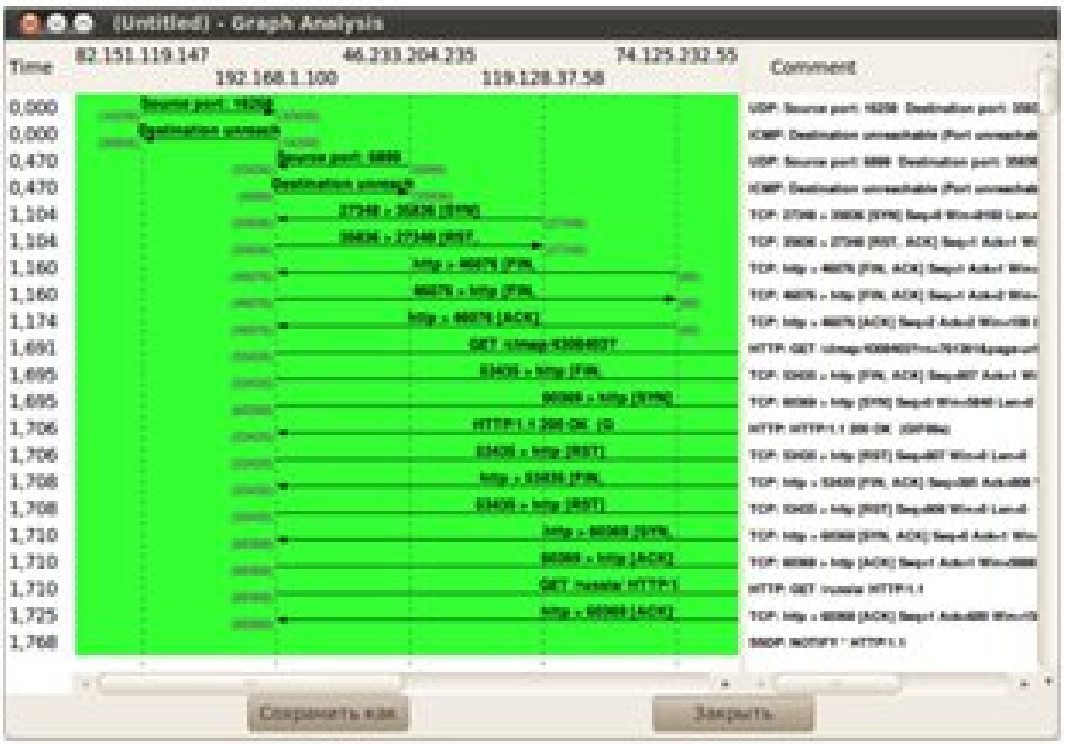


Рис. 6 – Диаграммы соединений.

Задание на лабораторную работу: 1. Запустить анализатор трафика Wireshark. После выбора требуемого сетевого интерфейса кнопкой Startначать сбор трафика (см. рис. 7).

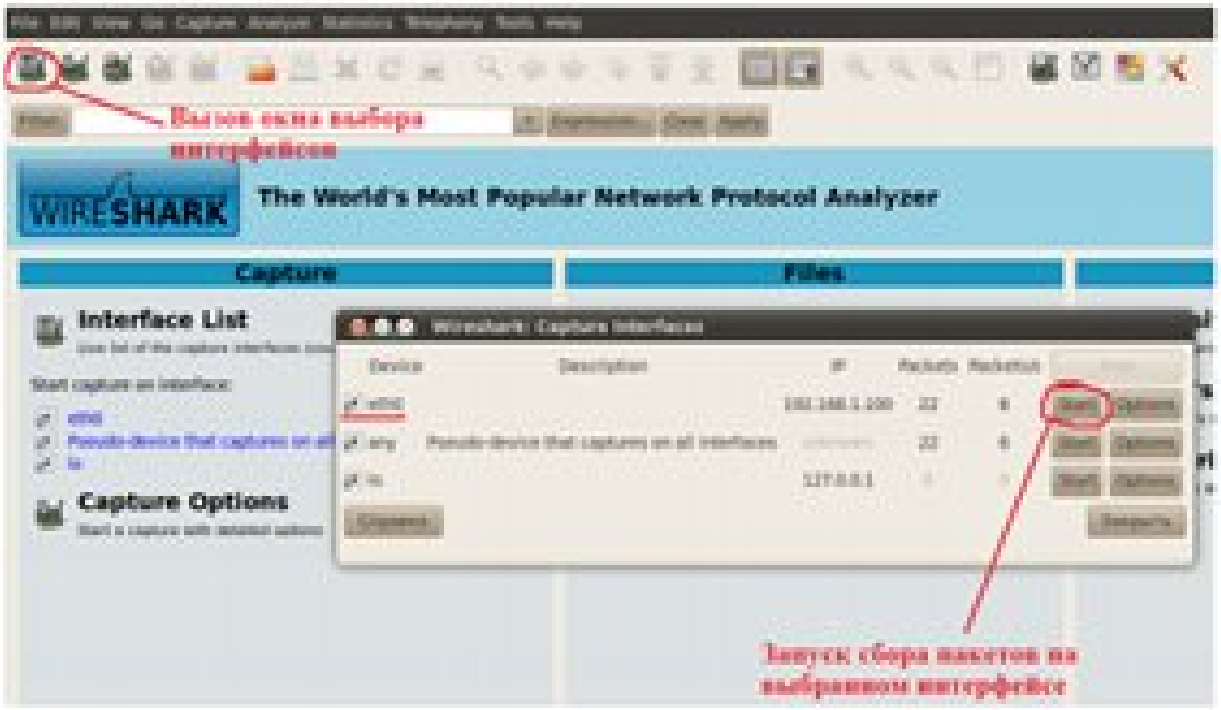


Рис. 7 – Запуск процедуры сбора пакетов

2. Настроить фильтр на широковещательный трафик (см. рис. 8): нажатием на кнопку Filterв панели инструментов Wiresharkзапустить окно выбора/создания фильтра, ввести любое имя для нового фильтра в поле FilterName, ав качестве фильтрующего выражения (FilterString) выставить название протокола «arp». Для применения фильтра нажмите кнопку «Apply»на панели инструментов.
3. 

Рис. 8 – Настройка фильтра для анализа ARP-пакетов

3. Разобрать пакет ARP: запрос и ответ. Снять скриншоты экранов с таблицами анализа протокола ARP
4. Убрать настройку фильтров. Запустить браузер, набрать URL какого- либо веб-ресурса (по желанию студента или заданию преподавателя). Отследить и разобрать пакеты DNS (запрос и ответ). 5. Разобрать пакеты http двух типов: запрос (GET) и ответ сервера. Снять скриншоты экранов: таблицы анализа, график интенсивности трафика HTTP в общем трафике, диаграмму соединений. 6. На основании данных об IP-адресах в полученном трэйсе и инструмента GraphAnalysis, построить карту сети (см. рис. 9), указав с помощью соединительных линий логические связи (т.е. наличие соединений) между хостами.

Практическое задание: *Средства мониторинга компьютерных сетей*
Лабораторная работа

- Изучить принципы работы простейших средств мониторинга сети.
- Получить навыки решения задач, связанных с мониторингом сети.

Теоретические основы

1. Протокол ICMP

Протокол ICMP (Интернет-протокол контрольных сообщений) стека протоколов TCP/IP предназначен для передачи между сетевыми устройствами сообщений об ошибках и контрольных сообщений при помощи IP-пакетов.

В протоколе ICMP определены несколько типов сообщений, в том числе:

Destination Unreachable	Time to Live Exceeded	Parameter Problem
Source Quench	Redirect	Echo
Echo Reply	Timestamp	Timestamp Reply
Information Request	Information Reply	Address Request
Address Reply		

Например, если маршрутизатор получает пакет, который он не может доставить по указанному в нем адресу, отправителю передается ICMP-сообщение о недостижимости адреса (Destination Unreachable).
2. PING: Проверка соединения с определенным интерфейсом.
Программа ping использует протокол ICMP.
Эта команда посылает пакет эхо-запроса на другой IP-адрес и ожидает ответа. Она чаще всего используется для того, чтобы посмотреть, «жив ли» другой компьютер. Ответ на запрос содержит также данные о том, как долго пакет путешествовал до адресата. Можно использовать команду ping с различными опциями: число посланных пакетов (от 1 до 10), время жизни пакета (time to live –TTL, от 1 до 255ms), размер пакета (от 16 до 8192 байт), время ожидания (timeout, до 9999 ms) и разрешать или нет фрагментацию каждого пакета.
Формат команды в ОС Windows:
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list
Options:
-t Выполнение команды до прерывания (Ctrl+C)

-a Разрешать адреса в имена
-n count Число отправляемых пакетов.
-l size Размер буфера отправки
-f Установить флаг "Не фрагментировать".
-i TTL Установить время жизни.
-w timeout Время ожидания ответа в мс.
-v TOS Задание типа службы (поле "Type Of Service").
-r count Запись маршрута для указанного числа переходов.
-s count Штамп времени для указанного числа переходов.
-j host-list Свободный выбор маршрута по списку узлов.
-k host-list Жесткий выбор маршрута по списку узлов.
destination-list Список рассылки.
3. Программа tracert. Определение промежуточных сетевых интерфейсов между хостами.
Трассировка маршрута
Программа трассировки маршрута использует протокол ICMP.
Эта утилита очень похожа на Ping, за исключением того, что она показывает все другие IP-адреса (интерфейсы), которые пакет проходит до своего места назначения. Дополнительно можно изменять различные опции, ассоциированные с Trace Route: максимальное число дозволяемых промежуточных узлов (maximum hops, от 1 до 255) и timeout (до 9999 ms).
Формат команды в ОС Windows:
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
Options:
-d Не разрешать адреса в имена.
-h maximum_hops Наибольшее число промежуточных узлов.
-j host-list Трассировка через определенный список хостов
-w timeout Время ожидания каждого ответа в мс.
4. Программа netstat. Сетевая статистика.
Программа netstat используется для просмотра активных соединений каждого протокола, таблиц маршрутизации, а так же детализирует статистику передачи данных.
Формат команды в ОС Windows:
netstat [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]
-a Отображение всех подключений и ожидающих портов.
(Подключения со стороны сервера обычно не отображаются).
-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.
-n Отображение адресов и номеров портов в числовом формате.
+-p имя Отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.
-r Отображение содержимого таблицы маршрутов.
-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных.
ИнтервалПовторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

Средства/Подготовка

В работе будут использоваться сети, соединенные с рабочей станцией линками разных типов. Первая сеть (194.85.33.0) доступна через спутниковый канал связи, проходящий через спутниковый ретранслятор на геостационарной орбите с пропускной способностью 512 кбит/с. Вторая сеть 217.23.64.0 доступна через наземный волоконно-оптический канал

связи с пропускной способностью 2 Мбит/с, третья сеть 212.194.38.0 входит в состав корпоративной сети ВУЗа и доступна в локальной сети с пропускной способностью 10/100 мбит/с.
В качестве альтернативного инструмента анализа сети используется интерфейс Looking Glass на сайте http://noc.runnet.ru(IP-адрес 194.85.35.100).
Ход работы Задание 1. Ping
Выполните команду ping в командной строке с различными значениями параметров -t, -n, -l, -i,-w. Какие наблюдения и выводы вы сделали?
ping www.seun.ru
ping www.sgu.ru
ping www.microsoft.com
ping www.sun.com
ping212.193.38.83

_____

_____

Выполните ping к тем же хостам с параметром –f, увеличивая параметр -l size. При каком значении размера перестают получаться ответы?

_____

_____

Задание 2. Tracert

Выполните команду tracert в командной строке с различными значениями параметров. Какие наблюдения и выводы вы сделали?

Используйте, например,

tracertwww.seun.ru

tracert www.sgu.ru

tracert www.microsoft.com

tracert www.sun.com

tracert 212.193.38.83

Задание 3. Поисковые сервисы Европейского и Российского ip-регистров
Определите, кому принадлежат сети 194.85.33.0, 217.23.64.0, 212.193.38.0. Для этого используйте поисковые аппараты http://www.ripe.net/db/whois/whois.htmlиhttp://www.ripn.net:8080/nic/whois/index.html.
Пользуясь данными этих информационных систем, попробуйте определите географическое расположение сетей. Попробуйте изобразить топологическую схему соединения этих сетей.
Задание 4. Использование программы ping для исследования параметров сети.

1. Приведите сравнительные результаты выполнения команд ping по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10 по параметрам «время отклика», TTL в форме таблицы. Объясните полученные различия.
2. Соберите средние времена прохождения 10 пакетов на указанные адреса. Сравните с р4езультатами, полученными при использовании сервиса ping в интерфейсе Looking Glass на сайте http://noc.runnet.ru. Объясните полученные различия.
+3. Соберите усредненные времена прохождения 10 пакетов увеличивающегося размера по указанным адресам. Начните с 64 байт и каждый раз удваивайте размер пакета. При каком размере пакета потери превышают 50 %. Как влияет время ожидания отклика на процент прохождения пакетов этого размера. При каком времени ожидания отклика потери для пакетов зафиксированного размера не возникают?
Представьте результаты измерений в форме таблиц, наилучшим образом проявляющим, по вашему мнению, обнаруженные зависимости.
4. Используя программу ping, оцените вклад разных сетевых участков, по которым проходит эхо-пакет между вашей рабочей станцией и интерфейсом 194.85.33.29.
Задание 5. Использование программы tracert для анализа соединений в сети.
1. Приведите сравнительные результаты выполнения команд tracert по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10. Объясните полученные различия.
2. Выполните трассировку к адресу 212.193.38.248 и к адресу 217.23.64.2 со стороны сайта http://noc.runnet.ru. Приведите полученные результаты.
3. Используя данные, полученные в результате выполнения трассировки и отправки эхо-пакетов между интерфейсами 212.193.38.248 и 194.85.35.100, оцените вклад разных участков сетей, соединяющих эти интерфейсы, в среднее время прохождения пакетов между ними.
4. Используя полученную в ходе выполнения всех заданий информацию, уточните схему задания 1, изобразите на ней обнаруженные вами промежуточные интерфейсы и линки сети, объединяющей подсети 194.85.33.0, 217.23.64.0, 212.193.38.0.

Практическое задание:*Средства анализа сети с помощью команд сетевой операционной системы*

Вопросы для проверки знаний

1. К какой из пяти стандартных функциональных групп системы управления относится функция концентратора Ethernet по обнулению поля данных в кадрах, поступающих на порты, к которым не подключен узел назначения?
2. К какому уровню модели TMN относится большинство выпускаемых сегодня систем управления?
3. Какая функция в системах управления системами соответствует функции построения карты сети в системах управления сетями?
4. Какое свойство агента, поддерживающего RMON MIB, послужило поводом назвать данную MIB базой управляющих данных для *удаленного* мониторинга?
5. Какие действия предпринимает агент SNMP, если его сообщение о сбое управляемого устройства, посланное с помощью команды trap, потеряется?
6. Можно ли построить систему управления, работающую без платформы управления?

7. Относится ли средство, называемое community string, к средствам аутентификации?
8. Какую базу данных использует протокол CMIP для воздействия сразу на группу агентов?
9. У вас есть подозрение, что часть коллизий в вашей сети вызвана электромагнитными наводками. Сможет ли анализатор протоколов прояснить ситуацию?

Упражнение

Как объяснить, что наличие в одном сегменте сети NetWare сравнительно небольшого числа (3 %) ошибочных кадров Ethernet резко снижает пропускную способность сети. Рассчитайте коэффициент снижения полезной пропускной способности сети, если при передаче файлов используется метод квитирования с простоями, причем тайм-аут ожидания квитанции составляет 0,5 с, сервер тратит на подготовку очередного кадра данных 20 мкс после получения квитанции от клиентской станции, а клиентская станция отсылает квитанции через 30 мкс после получения очередного кадра данных от сервера. Служебная информация протоколов верхних уровней занимает в кадре Ethernet 58 байт, причем данные передаются в кадрах Ethernet с полем данных максимального размера в 1500 байт, а квитанции помещаются в заголовке протокола прикладного уровня.

Практическое задание:*Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры*

Вопросы для проверки знаний

1. Архитектура вычислительных систем.
2. Состав системного блока.
3. Назначение, основные характеристики, интерфейс устройств персонального компьютера (по каждому устройству), входящих в состав системного блока.
4. Устройство жесткого диска
5. Базовая аппаратная конфигурация;
6. Основные характеристики монитора;
7. Характеристики (тип разъема, количество контактов, скорость передачи данных) разъемов: видеоадаптера; последовательных портов; параллельного порта; шины USB; сетевой карты; питания системного блока; питания монитора.
8. Типы периферийных устройств.

Цель работы: изучить основные блоки и периферийные устройства персонального компьютера, способы их соединения, конструктивы (разъемы), основные характеристики (название, тип разъема, количество контактов, скорость передачи данных, дополнительные свойства);
Краткие теоретические и справочно-информационные материалы по теме занятия.

Периферийное устройство — аппаратура, которая позволяет вводить информацию в компьютер или выводить ее из него.
Периферийные устройства являются опциональными, и, технически, могут быть отключены от компьютера без потери его работоспособности. Однако абсолютное большинство компьютеров используются вместе с теми или иными периферийными устройствами. Выделяют три основных типа периферийных устройств: • Устройства ввода, использующиеся для ввода информации в компьютер: мышь, клавиатура, сенсорный экран, сканер, веб-камера и видеозахват • Устройства вывода, например мониторы, принтеры • Устройства хранения, служащие для накопления информации,

обрабатываемой компьютером: НЖМД, НГМД, ленточные и дисковые устройства,накопители "флеш" Иногда периферийное устройство относится к нескольким типам, например Устройство ввода-вывода. Отдельно взятое устройство из класса периферийных устройств компьютера. Класс периферийных устройств появился в связи с разделением вычислительной машины на внутренние и внешние устройства. Внутренние — это вычислительные (логические) блоки (то есть процессоры) и память хранения выполняемой программы. Внешние устройства — это и есть периферийные устройства, вместе с подключающими их интерфейсами. Таким образом, периферийные устройства, расширяя возможности ЭВМ, не изменяют её архитектуру. Периферийными устройствами также можно считать внешние по отношению к системному блоку компьютера устройства.

Порядок работы внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

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. Мышь может подключаться к разъему последовательного порта или к специальному порту PS/2, имеющему разъем круглой формы. Последний способ является более современным и удобным. В этом случае мышь имеет собственный выделенный порт, что исключает возможность ее конфликта с другими устройствами, подключаемыми к последовательным портам. Последние модели могут подключаться к клавиатуре через разъем интерфейса USB.

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. Для материнских плат в форм-факторе AT подключение питания выполняется двумя разъемами. Обратите внимание на расположение проводников черного цвета - оно важно для правильной стыковки разъемов.
12. Установите местоположение жесткого диска. Установите местоположение его разъема питания. Проследите направление шлейфа проводников, связывающего жесткий диск с материнской платой. Обратите внимание на местоположение проводника, окрашенного в красный цвет (на жестком диске он должен быть расположен рядом с разъемом питания).

13. Установите местоположения привода CD-ROM (DVD-ROM). Проследите направление их шлейфов проводников и обратите внимание на положение проводника, окрашенного в красный цвет, относительно разъема питания.
14. Установите местоположение платы видеоадаптера. Определите тип интерфейса платы видеоадаптера.
15. При наличии прочих дополнительных устройств выявите их назначение, опишите характерные особенности данных устройств (типы разъемов, тип интерфейса и др.).
16. Заполните таблицу:

Устройство	Характерные особенности	Куда и при помощи чего подключается

Тема 1.2 Эксплуатация систем IP телефония

Практическое задание:*Настройка аппаратных IP-телефонов*

Лабораторная работа

Цель: научиться настраивать аппаратные IP-телефоны

Рассмотрим типовые случаи **настройки IP телефона** на примере телефонного аппарата Addpac. Настройку IP телефона произведем для его подключения: к аппаратной IP-АТС AddPac IPNext

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:

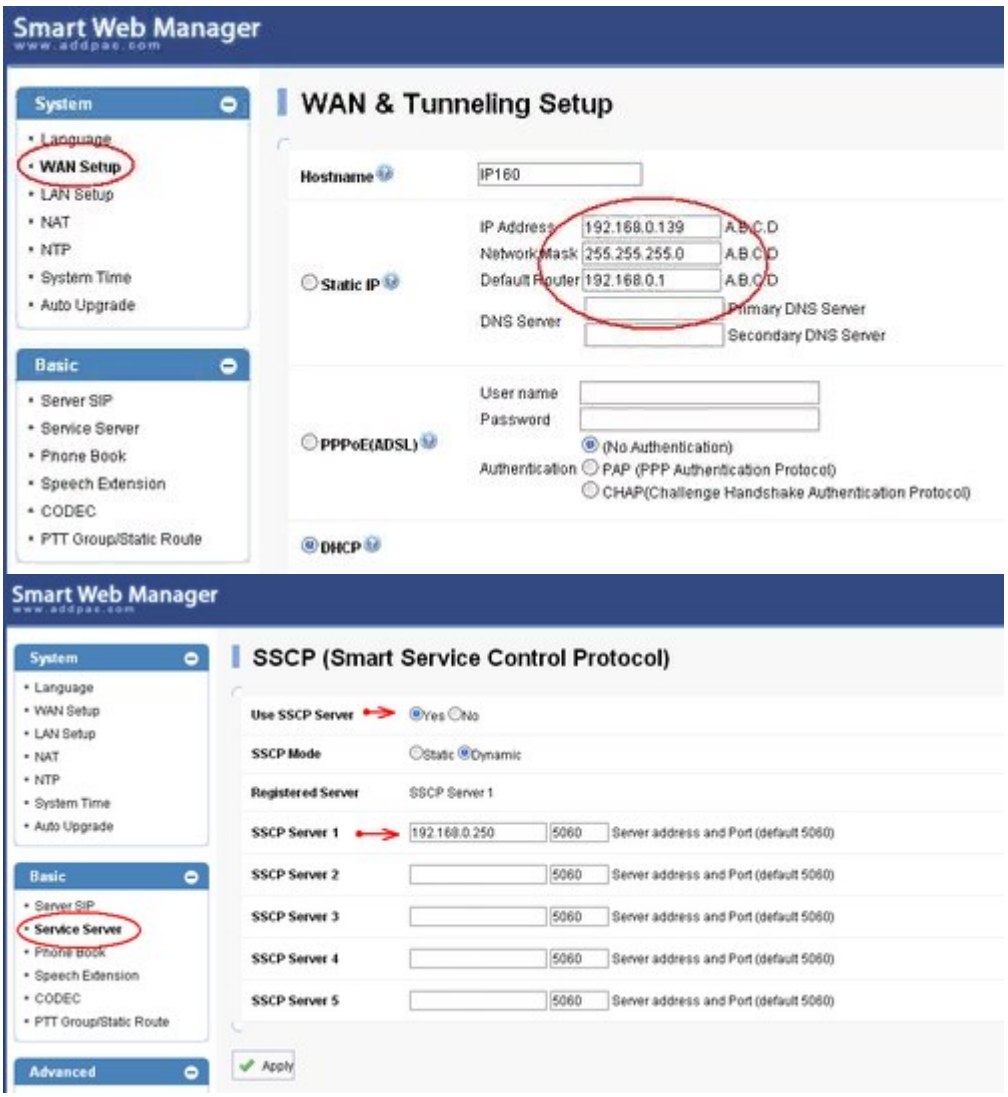
Menu => Network Setup => Internet Setup (далее выбираем тип: DHCP или статический IP)

Теперь необходимо указать адрес SSCP (адрес IPNext)

Menu => Network Setup => SSCP Setup => Use SSCP => Enable

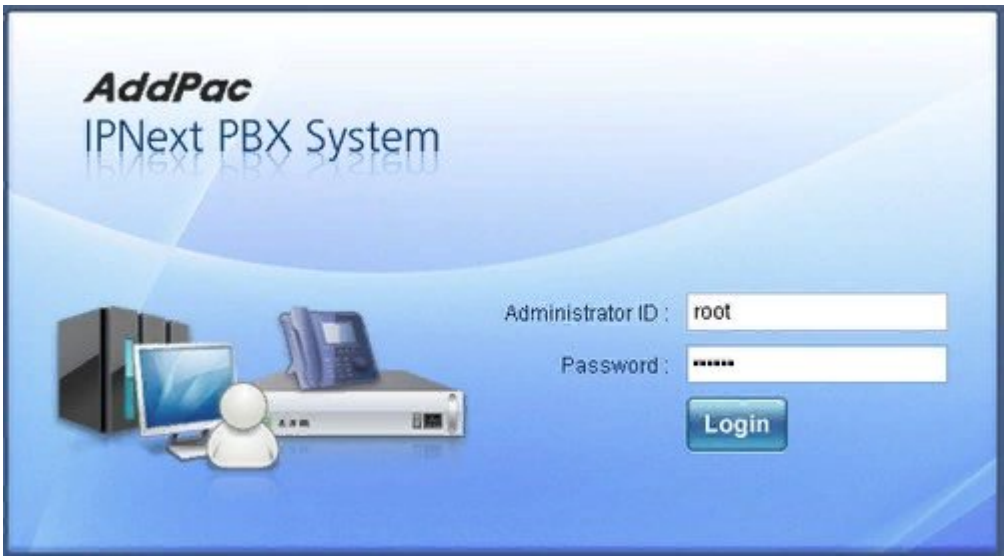
Menu => Network Setup => SSCP Setup => CM Setup => Call Manager1 (вводим IP адресАТС IPNext)

б) Те же самые настройки можно произвести через WEB-интерфейс телефона.

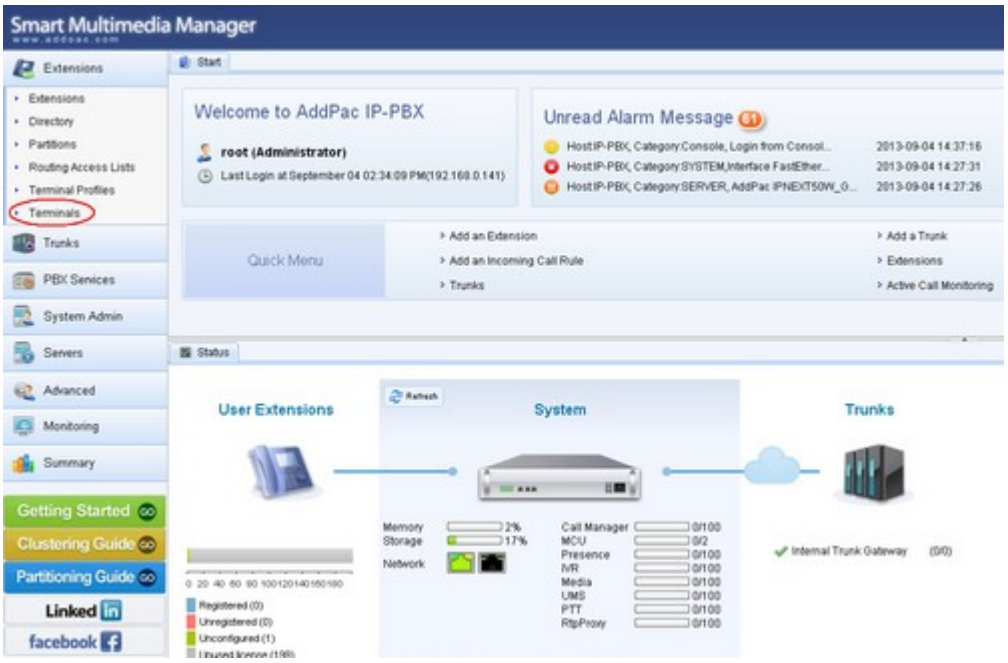


На этом настройка IP телефона закончена. Теперь телефон сообщается с IPNext по фирменному протоколу AddPac SSCP. Далее все настройки производим на IP-АТС через web-интерфейс.

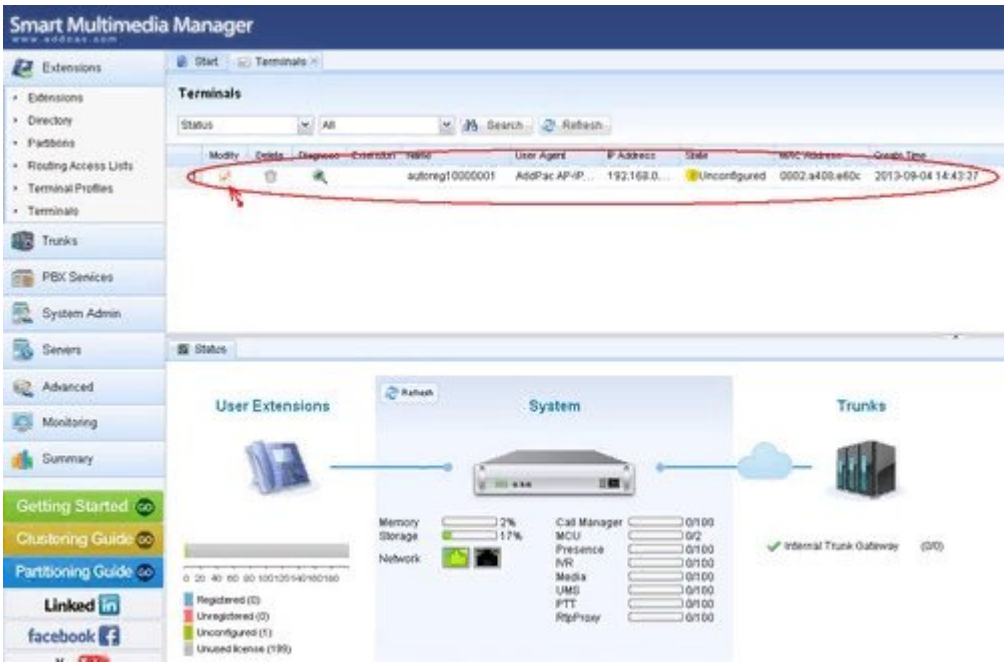
Заходимна Smart Multimedia Manager IPNext



Выбираем меню Extensions, и подменю Terminals.



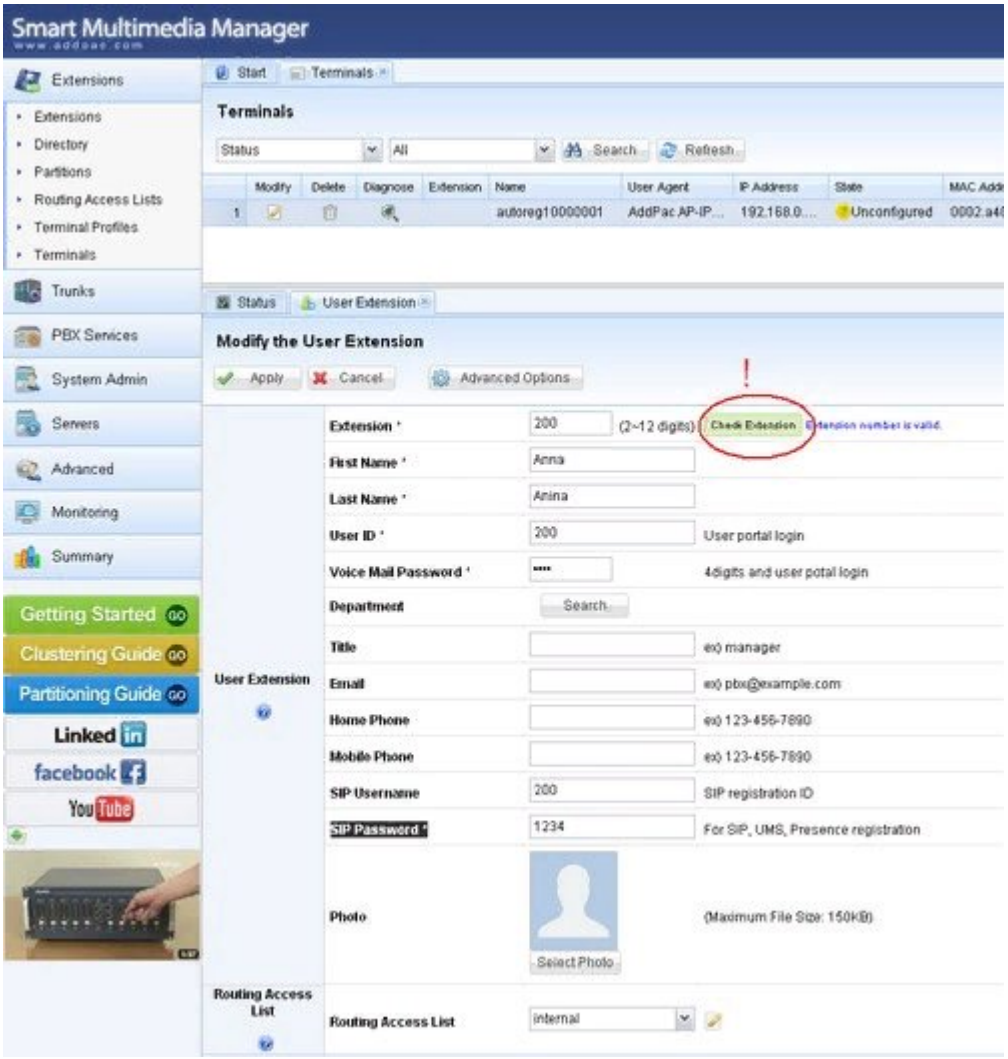
Здесь мы видим наш телефон, запросивший авторегистрацию (его модель, IP адрес, MAC адрес). Теперь нам нужно назначить ему номер. Нажимаем Modify.



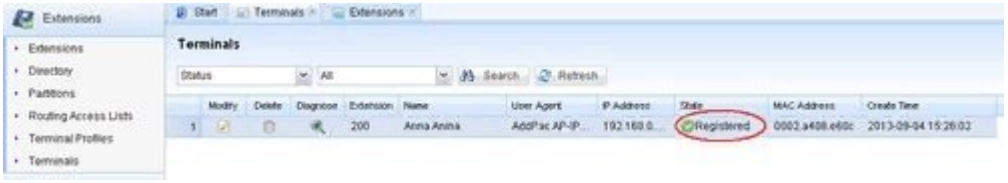
Заполняем поля отмеченные звездочкой:

- 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.



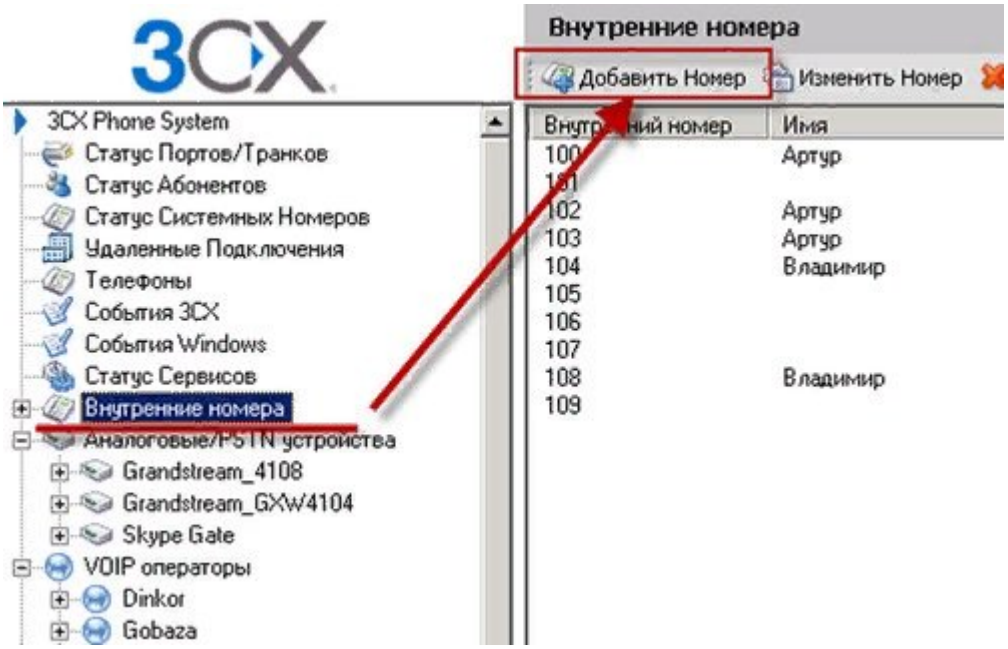
Теперь в меню Extensions мы можем наблюдать новый номер.
А в меню Terminals видим наш зарегистрированный IP телефон.



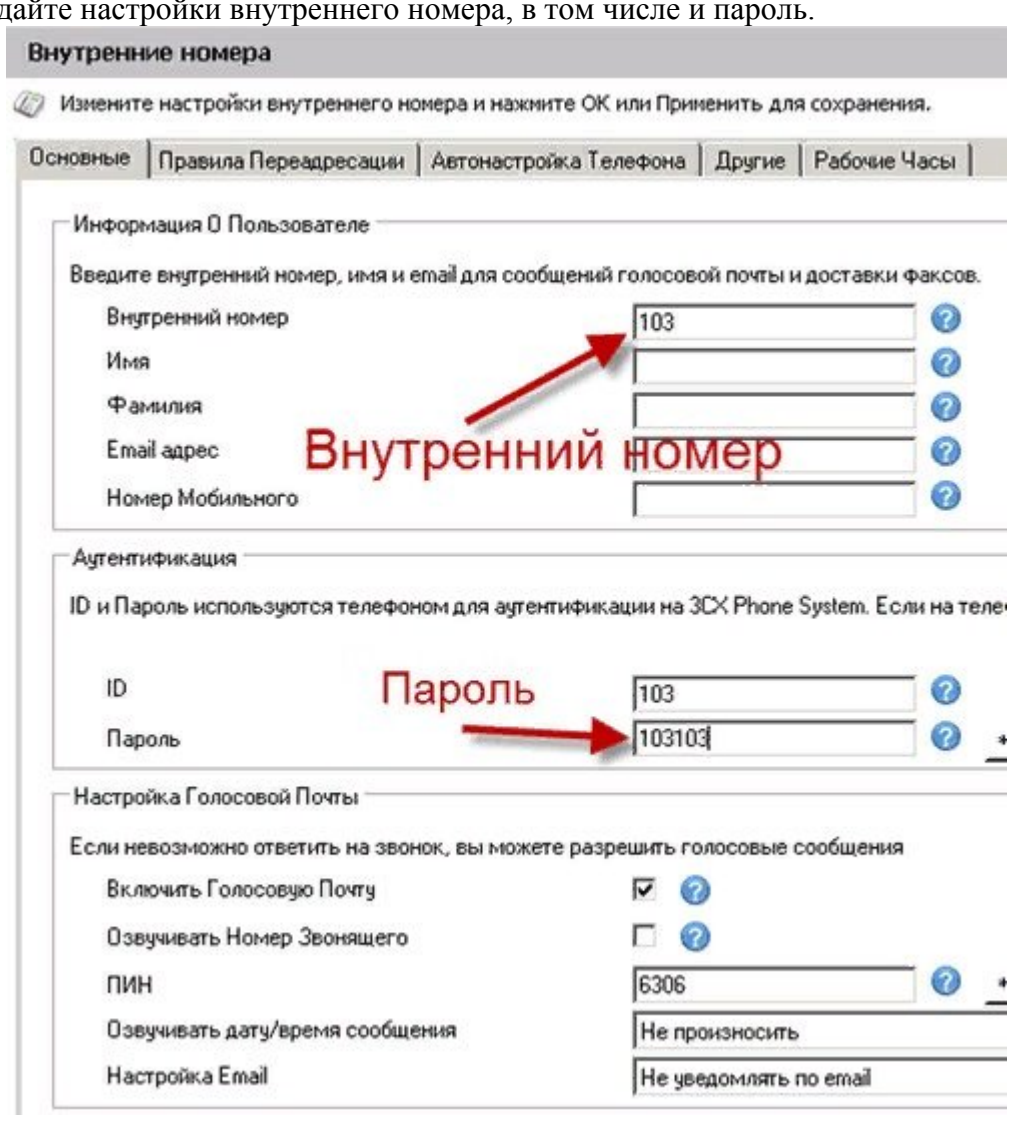
На самом аппарате должен высветится значок подключения ?и номер внутреннего абонента.
На этом настройка IP телефона для работы с IP-АТС AddPac IPNext успешно завершена.

Практическое задание:*Настройка программных IP-телефонов, факсов*
Лабораторная работа
Цель: научиться настраивать программных IP-телефонов, факсов

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.



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 AP 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 (информацияоконфигурацияхвашегопорта 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 (пользовательскиенастройки)
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 (важныйпараметр)
call-waiting
recording all
!
!
!
! Voip peer configuration.
!
dial-peer voice 1001 voip (настройкавходящихзвонков)
destination-pattern T (важныйпараметр)
session target sip-server (важныйпараметр)
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 (настройкарегистрациителефонав 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 (важныйпараметр)
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
На этом настройка IP телефона AddpacAP-IP90 для работы с 3CXPhoneSystem успешно завершена!
Практическое задание:*Развертывание сети с использованием VLAN для IP-телефонии*
Лабораторная работа

Цель работы: в рамках настоящей лабораторной работы вам предстоит создать виртуальные локальные сети (VLAN) и настроить транковую связь между ними.
Задачи:
1. Построение сети и настройка базовых параметров устройства
2. Настройка коммутаторов с сетями VLAN и транковой связи между ними
Часть 1. Построение сети и настройка базовых параметров устройства
В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов, коммутаторов и маршрутизатора ПК.
1. Подключите кабели в сети в соответствии с топологией.
2. Настройте узлы ПК.
3. Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.
4. Настройте базовые параметры каждого коммутатора.
Отключите поиск DNS.
Настройте имена устройств в соответствии с топологией.
Назначьте class в качестве пароля привилегированного режима EXEC.
Назначьте cisco в качестве паролей консоли и VTY.
Настройте logging synchronous для консольного канала.
Настройте IP-адрес, указанный в таблице адресации для сети VLAN 1, на обоих коммутаторах.
Настройте шлюз по умолчанию на обоих коммутаторах.
Используя права администратора, отключите все неиспользуемые порты на коммутаторе.
Сохраните текущую конфигурацию в загрузочную конфигурацию.
5. Настройте базовые параметры для маршрутизатора.
Отключите поиск DNS.
Настройте имена устройств в соответствии с топологией.
Настройте IP-адрес loopback-интерфейса в соответствии с таблицей адресации. На данном этапе не нужно настраивать подынтерфейсы, поскольку их настройка будет выполняться в третьей части лабораторной работы.
Назначьте cisco в качестве паролей консоли и VTY.
Назначьте class в качестве пароля привилегированного режима EXEC.
Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.
Сохраните текущую конфигурацию в загрузочную конфигурацию.
Часть 2. Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов
Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLAN и транковых каналов.

Примечание . Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении А. Проверьте свои знания — попытайтесь настроить коммутаторы S1 и S2, не обращаясь к информации, приведённой в приложении.

1. Настройте сети VLAN на коммутаторе S1.
На коммутаторе S1 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора.
На коммутаторе S1 настройте интерфейс, подключённый к маршрутизатору R1 в качестве транкового канала. Также настройте интерфейс, подключённый к маршрутизатору R2 в качестве транкового канала.
На коммутаторе S1 назначьте порт доступа для компьютера PC-A сети VLAN 10.
2. Настройка сетей VLAN на коммутаторе S2.
На коммутаторе S2 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора.
Убедитесь, что номера и имена VLAN на коммутаторе S2 совпадают с данными на коммутаторе S1.
На коммутаторе S2 назначьте порт доступа для компьютера PC-B сети VLAN 20.
На коммутаторе S2 настройте интерфейс, подключённый к коммутатору S1 в качестве транкового канала.

Практическое задание:*Настройка шлюза*
Лабораторная работа
Цель работы. Ознакомится с архитектурой стека протоколов TCP/IP с использованием программного сетевого эмулятора Packet Tracer Cisco Systems.
Задание. Построить сеть с использованием маршрутизаторов, коммутаторов и оконечного оборудования с обеспечение шлюза.
Краткие теоретические сведения
Открытая система(OSI) — это стандартизированный набор протоколов и спецификаций, который гарантирует возможность взаимодействия оборудования различных производителей. Она реализуется набором модулей, каждый из которых решает простую задачу внутри элемента сети. Каждый из модулей связан с одним или несколькими другими модулями. Решение сложной задачи подразумевает определенный порядок следования решения простых задач, при котором образуется многоуровневая иерархическая структура на рис. 1. Это позволяет любым двум различным системам связываться независимо от их основной архитектуры.

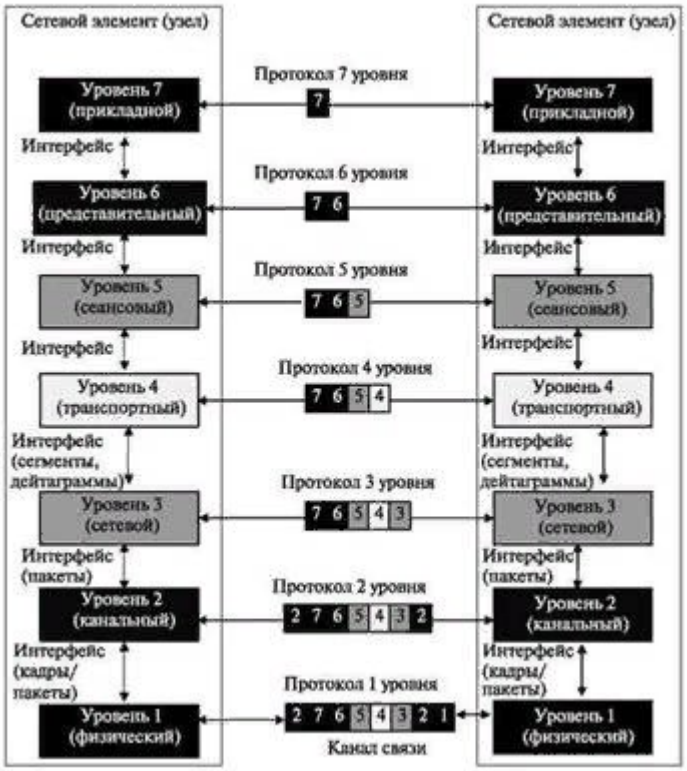


Рис. 1. Модель взаимодействия открытых систем OSI

Модель OSI составлена из семи упорядоченных уровней: физического (уровень 1), звена передачи данных (уровень 2), сетевого (уровень 3), транспортного (уровень 4), сеансового (уровень 5), представления (уровень 6) и прикладного (уровень 7).

Обмен информацией между модулями происходит на основе определенных соглашений, которые называются интерфейсом. При передаче сообщения модуль верхнего уровня решает свою часть задачи, а результат, понятный только ему, оформляет в виде дополнительного поля к исходному сообщению (заголовка) и передает измененное сообщение на дообслуживание в нижележащий уровень. Этот процесс называется инкапсуляцией.

Стек протоколов Интернета

Стек протоколов сети Интернет был разработан до модели OSI. Поэтому уровни в стеке протоколов Интернета не соответствуют аналогичным уровням в модели OSI. Стек протоколов Интернета состоит из пяти уровней: физического, звена передачи данных, сети, транспортного и прикладного. Первые четыре уровня обеспечивают физические стандарты, сетевой интерфейс, межсетевое взаимодействие и транспортные функции, которые соответствуют первым четырем уровням модели OSI. Три самых верхних уровня в модели OSI представлены в стеке протоколов Интернета единственным уровнем, называемым прикладным уровнем рис. 2.

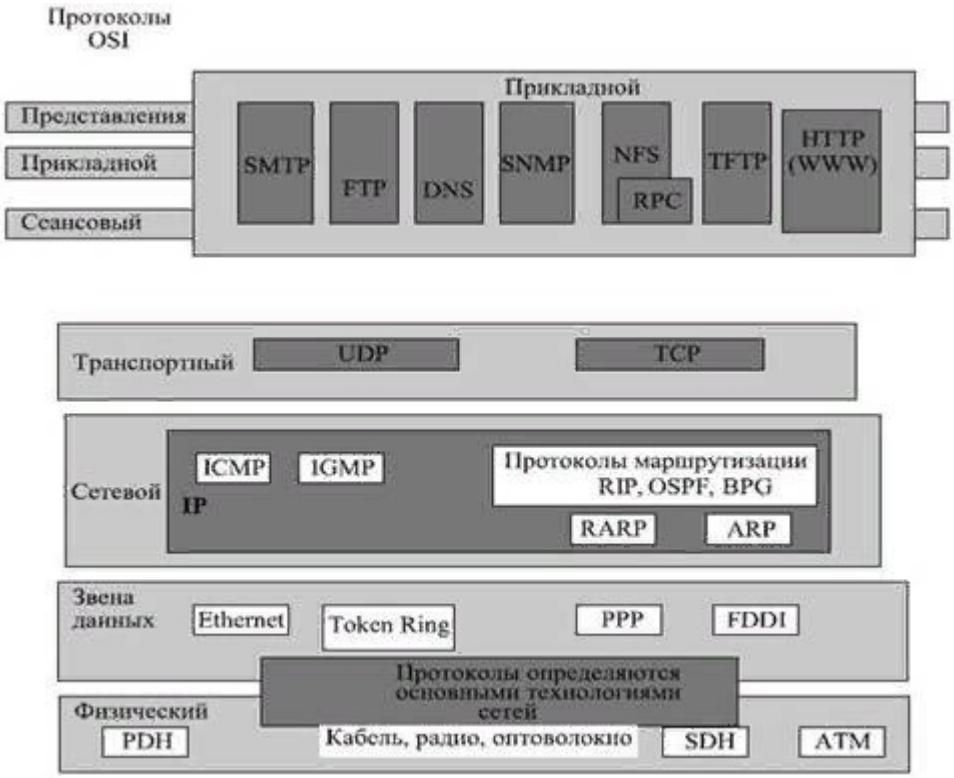


Рис. 2. Стек протоколов Интернета по сравнению с OSI

Стек базовых протоколов Интернета — иерархический, составленный из диалоговых модулей, каждый из которых обеспечивает заданные функциональные возможности; но эти модули не обязательно взаимозависимые. В отличие от модели OSI, где определяется строго, какие функции принадлежат каждому из ее уровней, уровни набора протокола TCP/IP содержат относительно независимые протоколы, которые могут быть смешаны и согласованы в зависимости от потребностей системы. Термин иерархический означает, что каждый верхний протокол уровня поддерживается соответственно одним или более протоколами нижнего уровня.

На транспортном уровне стек определяет два протокола: протокол управления передачей (TCP) и протокол пользовательских дейтаграмм (UDP). На сетевом уровне — главный протокол межсетевого взаимодействия (IP), хотя на этом уровне используются некоторые другие протоколы, о которых будет сказано ниже.

Адресация узлов в IP-сетях

В сетях TCP/IP принято различать адреса сетевых узлов трех уровней

физический (или локальный) адрес узла (MAC-адрес сетевого адаптера или порта маршрутизатора); эти адреса назначаются производителями сетевого оборудования; IP-адрес узла (например, 192.168.0.1), данные адреса назначаются сетевыми администраторами или Интернет-провайдерами; символьное имя (например, www. microsoft. com); эти имена также назначаются сетевыми администраторами компаний или Интернет-провайдерами.

Рассмотрим подробнее IP-адресацию.

Компьютеры или другие сложные сетевые устройства, подсоединенные к нескольким физическим сетям, имеют несколько IP-адресов — по одному на каждый сетевой интерфейс. Схема адресации позволяет проводить единичную, широковещательную и групповую адресацию. Таким образом, выделяют 3 типа IP-адресов.

Unicast-адрес (единичная адресация конкретному узлу) — используется в коммуникациях "один-к-одному". Broadcast-адрес (широковещательный адрес, относящийся ко всем адресам подсети) — используется в коммуникациях "один-ко-всем". В этих адресах поле идентификатора устройства заполнено единицами. IP-адресация допускает широковещательную передачу, но не гарантирует ее — эта возможность зависит от

конкретной физической сети. Например, в сетях Ethernet широковещательная передача выполняется с той же эффективностью, что и обычная передача данных, но есть сети, которые вообще не поддерживают такой тип передачи или поддерживают весьма ограничено. Multicast-адрес (групповой адрес для многоадресной отправки пакетов) — используется в коммуникациях "один-ко-многим". Поддержка групповой адресации используется во многих приложениях, например, приложениях интерактивных конференций. Для групповой передачи рабочие станции и маршрутизаторы используют протокол IGMP, который предоставляет информацию о принадлежности устройств определенным группам.

Класс сети	**Наименьший идентификатор сети**	**Наибольший идентификатор сети**	**Количество сетей**
Класс A	1.0.0.0	126.0.0.0	126
Класс B	128.0.0.0	191.255.0.0	16384
Класс C	192.0.0.0	223.255.255.0	2097152

Сетевое оборудование

Мост (bridge), как и репитер, может соединять сегменты или локальные сети рабочих групп. Однако, в отличие от репитера, мост также служит для разбиения сети, что помогает изолировать трафик или отдельные проблемы. Например, если трафик одного-двух компьютеров или одного отдела “затопляет” сеть пакетами, уменьшая ее производительность в целом, мост изолирует эти компьютеры или этот отдел. Мосты обычно решают следующие задачи. Увеличивают размер сети. Увеличивают максимальное количество компьютеров в сети.

В среде, объединяющей несколько сетевых сегментов с различными протоколами и архитектурами, мосты не всегда гарантируют быструю связь между всеми сегментами. Для такой сложной сети необходимо устройство, которое не только знает адрес каждого сегмента, но и определяет наилучший маршрут для передачи данных и фильтрует широковещательные сообщения. Такое устройство называется **маршрутизатором**.

Маршрутизаторы (routers) работают на Сетевом уровне модели OSI. Это значит, что они могут переадресовывать и маршрутизировать пакеты через множество сетей, обмениваясь информацией (которая зависит от протокола) между раздельными сетями. Маршрутизаторы считывают в пакете адресную информацию сложной сети и, поскольку они функционируют на более высоком по сравнению с мостами уровне модели OSI, имеют доступ к дополнительным данным. Маршрутизаторы могут выполнять следующие функции мостов: фильтровать и изолировать трафик; соединять сегменты сети.

Устройства **Switch** - коммутатор. Это оборудование относится к активному сетевому оборудованию, и служит для обработки пакетов в сети. Свитч (то же самое, что переключатель, мост, switch, bridge) - устройство, служащее для разделения сети на отдельные сегменты, которые могут содержать хабы и сетевые карты. Свитчи являются устройствами 2-го уровня, т. е. содержат в себе порты - устройства 1-го уровня для работы с сигналами, но помимо того, работают с содержимым сетевых пакетов - читают поле физического адреса назначения (MAC) пакета, пришедшего на один из портов, и в зависимости от его значения и таблицы MAC-адрес - порт "ретранслируют" пакет на другой порт (или не ретранслируют).

Практическое задание

Ниже на рис.1 приведена спроектированная сеть, которая включает в себя следующее оборудование:

Маршрутизаторы; Коммутаторы; ПК; IP-телефоны; Сервер.

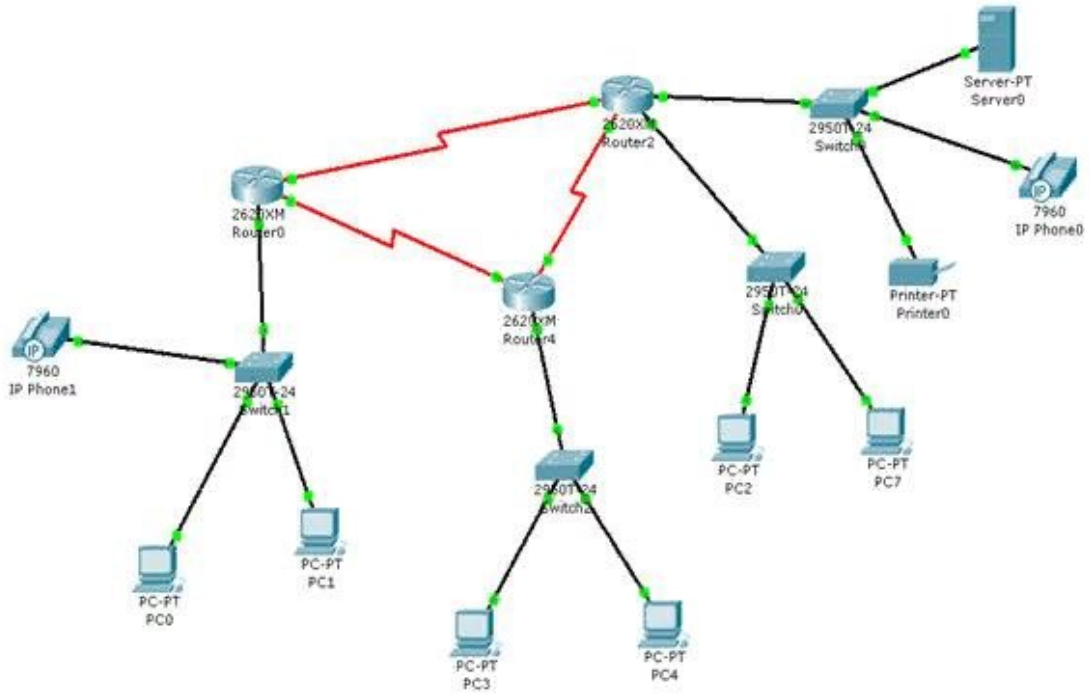


Рис. 1. Результат построения сети

Маршрутизаторы соединяются между собой при помощи DCE – кабеля. В данной сети маршрутизаторы используют RIP – протокол для осуществления передачи данных между различными подсетями(рис. 2).

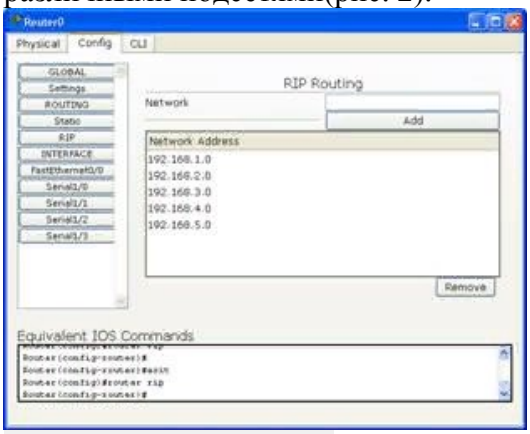


Рис. 2. Список подсетей

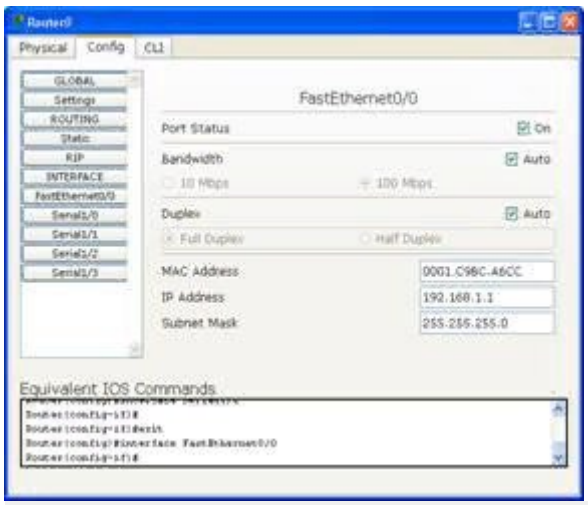


Рис. 3. Назначение IP-адреса маршрутизатору

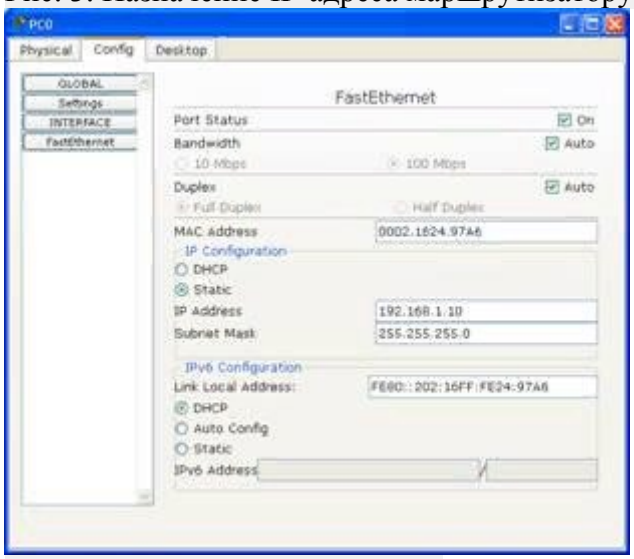
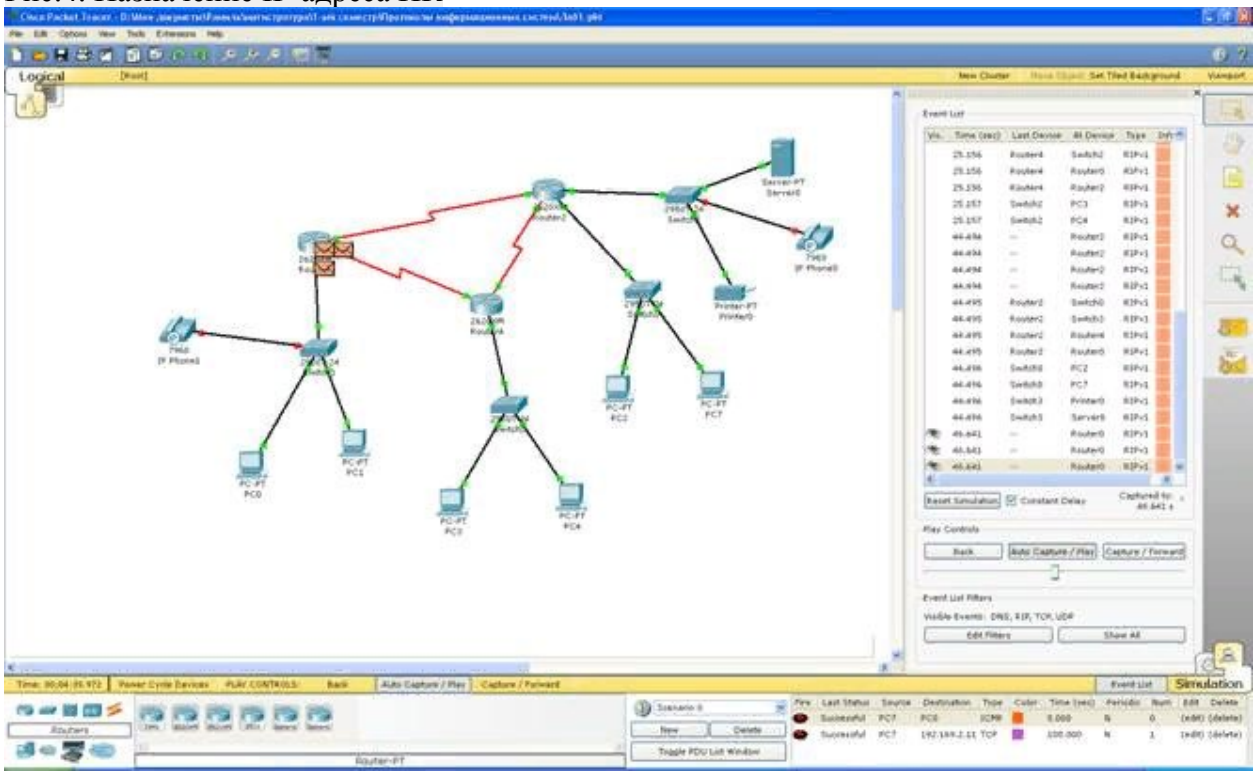


Рис.4. Назначение IP-адреса ПК



При этом, IP-адреса назначаются статически для маршрутизаторов и оконечного оборудования (рис. 3, 4).
Задание:
1. Построить аналогичную сеть. Сеть должна быть работоспособной на 100%;
2. В отчет необходимо включить таблицу следующего характера:

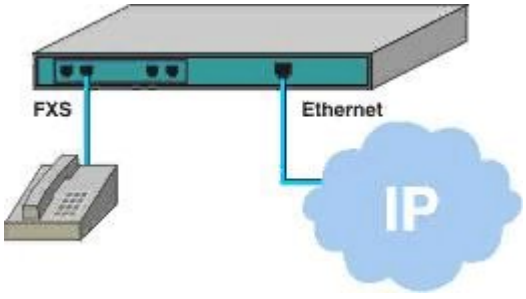
№ п. п.	Наименование оборудования	IP – адрес	MAC - адрес

3. Отправить пакеты по маршрутам представленным в таблице через команду ping результат записать в таблицу.

п. п.	Маршрут отправки	Команда	Полученный результат
1	**S1 => PC-PT PC4**		
2	**S3 => PC-PT PC2**		
3	**S1 => PC-PT PC4=> PC-PT PC1**		
4	**S1 => S3**		
5	**S3 => PC-PT PC3**		
6	**S2 => 7960 IP Phone0**		

Практическое задание:*Установка, подключение и первоначальные настройки голосового маршрутизатора*
Лабораторная работа
Цель:изучение установки, подключение и первоначальные настройки голосового маршрутизатора

Конфигурирование голосового модуля.
FXS (Foreign Exchange Station) порт - предназначен для подключения телефонного аппарата и эмулирует для последнего PBX (АТС).
FXO – (Foreign Exchange Office) порт – в противоположность FXS подключается в телефонную линию.
Таким образом, простейший шлюз H323 может выглядеть как cisco маршрутизатор (2600 или 3600) с голосовым модулем и интерфейсной картой FXS в нем, к которой подключен обычный телефонный аппарат. Ну и конечно какой-нибудь интерфейс для связи с IP сетью, например Ethernet.



После подключения голосового модуля необходимо проверить голосовые порты:

#sh voice port summary
1/0/0 -- fxo-ls up dorm idle on-hook y
1/0/1 -- fxo-ls up dorm idle on-hook y
1/1/0 -- fxs-ls up dorm on-hook idle y
1/1/1 -- fxs-ls up dorm on-hook idle y

Как видим, у нас два порта FXO (1/0/0 и 1/0/1) и два порта FXS (1/1/0 и 1/1/1), где цифры расшифровываются как slot-number/sub unit-number/port .
Подключим телефонный аппарат к FXS порту и посмотрим состояние:

 # sh voice port summary...1/1/1 -- fxs-ls up dorm on-hook idle y...

А теперь при поднятой трубке телефона:

 # sh voice port summary
1/1/1 -- fxs-ls up up off-hook idle y...

Описание dial peer.

После того, как мы определились с голосовыми портами необходимо обозначить соответствие набираемого (принимаемого) телефонного (E164) номера и пункта назначения (порт, ip адрес, gatekeeper) – описать так называемый dial peer. Согласно официальной документации dial peer служит для определения атрибутов, направления и участников звонка.
Если рассматривать dial peer как таблицу для ассоциации телефонного номера и пункта назначения звонка, то все dial peerы можно разделить на два вида: те, которые направляют звонок на соответствующий POTS интерфейс (например FXS) и те, которые предполагают приемной стороной определенное VOIP устройство (например VOIP шлюз).
В качестве иллюстрации соберем VOIP полигон с двумя шлюзами cisco.

Конфигурация шлюза A (gate A):

!
dial-peer voice 1 voip
destination-pattern 666
session target ipv4:192.168.0.2
codec g711alaw
!
dial-peer voice 2 pots
destination-pattern 555
port 1/1/1
!

В конфигурации шлюзу сказано, что звонки на номер 666 отправлять на участника IP сети с адресом 192.168.0.2 (предположительно VOIP шлюз) причем для связи использовать определенный звуковой кодек (алгоритм кодирования). А для терминирования звонка по номеру 555 использовать собственный голосовой порт номер 1/1/1. Также следует обратить внимание на задаваемый кодек – он должен быть одинаковым у обоих участников VoIP соединения.

Аналогично выглядит конфигурация шлюза B (gate B):

!
dial-peer voice 1 voip
estination-pattern 555
session target ipv4:192.168.0.1
codec g711alaw
!
dial-peer voice 2 pots
destination-pattern 666
port 1/1/1
!
Только он терминирует звонки на номер 666 (на свой порт 1/1/1) и направляет звонки по номеру 555 на IP адрес 192.168.0.1 .
Можно посмотреть все dial peerы:
sh dial-peer voice summary
В итоге, если поднять на телефонном аппарате A трубку и набрать номер 666, на шлюзе A сработает dial peer (описанный как dial-peer voice 1 voip) и направит звонок по адресу 192.168.0.2, то есть на шлюз B. На шлюзе B данный звонок в соответствии со своим dial peer (описанным как dial-peer voice 2 pots) терминирует звонок на порт 1/1/1 – зазвонит телефон B. Для того, чтобы направлять звонки (например, начинающиеся на 7) не просто в IP сеть, а на GATEKEEPER (маршрутизирующий звонки) необходимо на интерфейсе, подключенном к IP сети описать h323-gateway (указать его адрес и порт):
!interface FastEthernet0/0
p address 192.168.0.1 255.255.255.0
peed 10
f u l l - d u p l e x
h323-gateway voip interface
h323-gateway voip id GATEKEEPER ipaddr 192.168.0.100 1719
h323-gateway voip h323-id cisco
!
И в соответствующем dial peer вписать session target как ras:

!
dial-peer voice 5 voip
destination-pattern 7T
session target ras
codec g711ulaw
!
В данном случае cisco шлюз будет регистрироваться на gatekeepere и направлять звонки на номер, начинающиеся с цифры 7 на него.
Посмотреть работу шлюза H323 можно так:
sh gateway

Практическое задание:*Настройка таблицы пользователей в голосовом маршрутизаторе*

Практическое задание:*Настройка групп в голосовом маршрутизаторе*

Практическое задание:*Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе*

Практическое задание:*Настройка голосовых сообщений в маршрутизаторе*

Лабораторная работа

Цель: изучение 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. Настраиваем своего автосекретаря (IVR) в CUC 11
- Использование централизованного UCCX (см. Настройка UCCX с нуля. Часть 1)
- Использование продукта Third Party. Asterisk как IVR для CUCM
- Использование скриптов IVR (см. Простой IVR или автоответчик на маршрутизаторе)

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

serviceivrrflash:/vxml-ivr/My.vxml

!

global

servicealternatedefault

Настройкафизическогопорта FXO.

Входящийзвонокбудетперенаправленнавнутреннийномер 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

Данныйдиалпирнаправляетзвонкинавнутреннийномер 550 наскрипт.

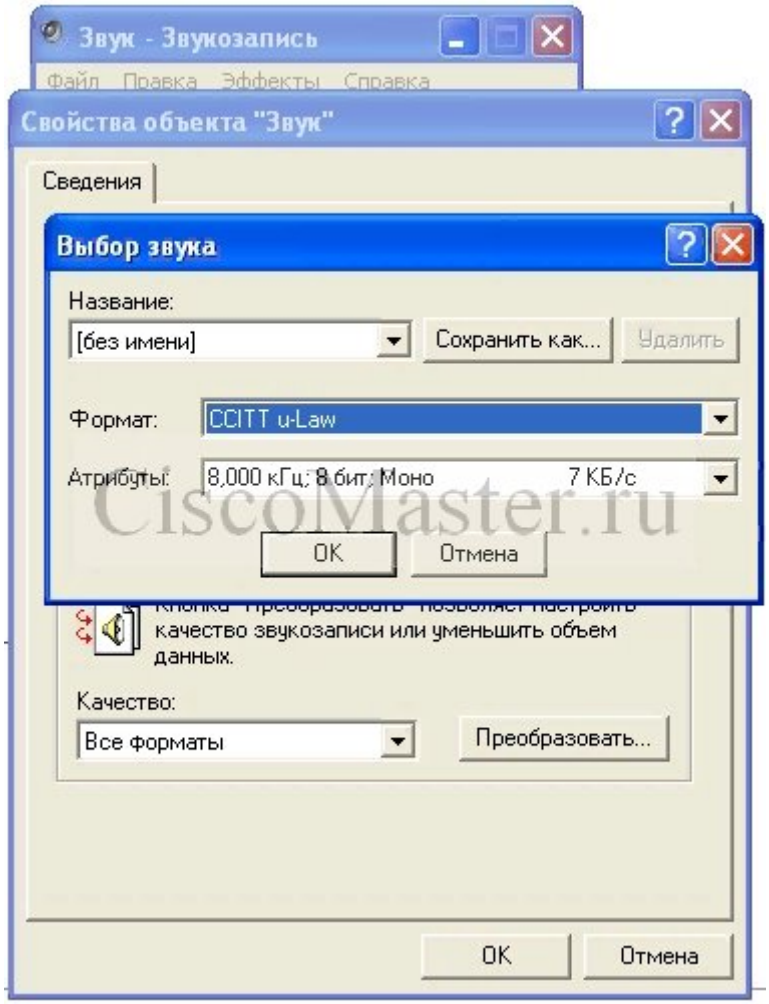
dial-peer voice 1000 pots

service ivrr

incoming called-number 550

port 1/0/8

Скрипт возвращает трехзначный номер абонента. Егоотдаемна 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
Приизменениискриптаилифайловнеобходимоперезапустить:
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
Вариант скрипта самый простой:
My2.vxml
Вариант скрипта посложней
My1.vxml

Также см.
Пример рабочего IVR CME + E1
Возможные проблемы
При настройке данного скрипта для работы с SIP провайдером может не проходить трансфер, решить можно попытаться:

- conf t
- vxml version 2.0
- vxml allow-star-digit
- voice register global
- call-forward system redirecting-expanded
- Настройка MTP.

Практическое задание:*Настройка программно-аппаратной IP-АТС*

Лабораторная работа

Цель: познакомить с устройствами и программными средствами, с помощью которых создается компьютерная сеть.

Для создания и функционирование компьютерных сетей нужны специальные устройства и программные средства. К аппаратной части для создания сети относятся сетевой адаптер, сетевой кабель, модем, маршрутизатор и главный компьютер – именно эти устройства позволяют организовать локальную сеть и возможность выхода в Интернет. Аппаратное обеспечение сети. Основным техническим устройством является специальный компьютер, обеспечивающий информационные функции. Такую машину называют хост – компьютером – он должен всегда находиться во включенном состоянии, так как обеспечивает прием и передачу данных по сети.

IP АТС, входящая в состав программно-аппаратного комплекса Doka базируется на основе свободно распространяемой АТС Asterisk, с соблюдением всех требований GPL.

Основные функции, доступные пользователям Doka "прямо из коробки":

1. Прямой многоканальный московский номер в коде 495/499.
2. Голосовая почта.
3. Установка собственного приветствия.
4. Установка музыки на ожидание.
5. Удержание вызова.
6. Перехват вызова.
7. Перевод вызова на внутренний/мобильный номер сотрудника.
8. Конференц-связь.

Doka дает возможность малому и среднему бизнесу иметь современную телефонию с возможностями которые раньше были доступны только крупным компаниям.

Настройка IP АТС Doka

Этап 1. Настройка провайдера.

Doka поставляется уже с преднастроенным многоканальным городским номером в коде 495/499. Если Вас устраивает предлагаемый нами провайдер - смело переходите к этапу 2. Если, по каким либо причинам, Вы желаете изменить провайдера IP телефонии, выполните следующие действия:

1. Войдите в интерфейс Doka используя учетную запись администратора.
2. Перейдите на страницу настроек (1).
3. Перейдите на вкладку "Параметры" (2).
4. Перейдите на вкладку "Телефон" (3)
5. Выберите вашего провайдера из выпадающего списка (4)
1. Если Вы не нашли вашего провайдера в списке - выберите "Другой"*.
2. Заполните поля "Номер"(Логин) и "Пароль". Данную информацию запросите у вашего провайдера IP телефонии (5),(6).
3. * Если выбран "Другой" заполните также поле "Сервер".

4. Для установки собственного приветствия и музыки на ожидание (замена стандартного гудка) Подготовьте 2 файла и загрузите их через соответствующие формы. Не забудьте установить галочки для включения данных опций.
5. Нажмите "Сохранить" (7) для того, чтобы ваши изменения вступили в силу.

Этап 2. Внутренние номера.

При заведении учетной записи нового сотрудника ему присваивается внутренний телефонный номер.

1. Войдите в интерфейс Doka используя учетную запись администратора.
2. Перейдите на страницу настроек (1).
3. Перейдите на вкладку "Пользователи" (2).
4. Нажмите + для добавления нового пользователя (3).

В окне добавления нового пользователя укажите:

Мобильный телефон сотрудника (1).

1. Внутренний номер сотрудника (2).

В случае заполнения этих полей Вам станет доступны включение опций "Переводить на мобильный" и "Голосовая почта". Нажмите "Сохранить" (3) для применение изменений.

Этап 3. Настройка телефонов

Настройка стационарного IP телефона сводиться к 3 простым шагам:

1. Подключите телефон к Doka.Box
2. В настройках телефона укажите адрес сервера - doka.start
3. В настройках телефона укажите имя пользователя и пароль, которые идентичны внутреннему номеру сотрудника. Например имя 1001, пароль 1001.

Настройка программных IP телефонов.

Обладатели смартфонов на базе iOS и Android могут съэкономить значительные средства на покупке стационарных IP телефонов, установив программный SIP клиент, при помощи которого смартфон (находясь в зоне действия офисной сети) превращается в офисный телефон сотрудника со своим внутренним номером.

Настройка смартфонов на базе Android на примере CSipSimple

1. Установите программу CSipSimple из Google Play.
2. Нажмите "Добавить аккаунт"
3. Выберите из выпадающего списка Basic

Заполните поля "Название" - произвольно, "Пользователь" - внутренний номер абонента, "Сервер" - doka.start, "Пароль" - внутренний номер абонента.

Сохраните настройки и дождитесь регистрации вашего смартфона на АТС Doka.Box

Ваша АТС готова к работе. С этого момента Вы:

- Значительно сократите расходы на местные, мобильные, междугородние и международные звонки.
- Обеспечите полноценную мобильность вашего бизнеса. Звонок может быть принят на телефон, компьютер или на мобильный телефон. Ваши сотрудники теперь всегда на связи.
- Телефонный номер больше не привязан к местоположению вашего бизнеса. В случае смены офиса, ваш номер перезжает вместе с вами.

Практическое задание:*Установка и настройка программной IP-АТС (например, Asterisk)*

Лабораторная работа

Цель работы: научиться устанавливать, запускать и тестировать IP АТС Asterisk в ОС Ubuntu 14.04 LTS на виртуальной машине Oracle VM VirtualBox.

Установка Asterisk из исходников

1. **Сборка и установка необходимых зависимостей и пакетов.**

Вначале нужно установить дополнительные пакеты, которые необходимы для установки и работы Asterisk. Без части из этих пакетов Asterisk вообще откажется устанавливаться (к примеру, если отсутствует gcc). Без некоторых пакетов Asterisk установится и даже будет работать, однако часть функционала будет недоступна. Например, пакет bison необходим для обработки выражений в файле extensions.conf. Еще пример: libnewt необходим для работы интерфейса управления astman. Для сервера Asterisk он не требуется, но без этого пакета у Вас не будет приложения astman, которое является отдельной программой. В нашем приводиться пример установки Asterisk 13 в системе Cent OS 6.9:
yum -y install gcc gcc-c++ make ncurses-devel libxml2-devel sqlite-devel bison kernel-headers kernel-devel openssl openssl-devel newt newt-devel flex curl sox binutils
Для 12-13 версии Asterisk требуется установка пакетов uuid и janson. Для установки библиотеки uuid в RHEL / Centos выполните команду:
yum -y install libuuid-devel
. Для установки библиотеки jansson в RHEL / Centos выполните команду:
yum -y install jansson-devel (предварительно требуется установка репозитория epel: yum install epel-release)
После обновляем систему до последней версии командой yum update –y и перегружаем ее: reboot

2. **Установка и установка их исходников**

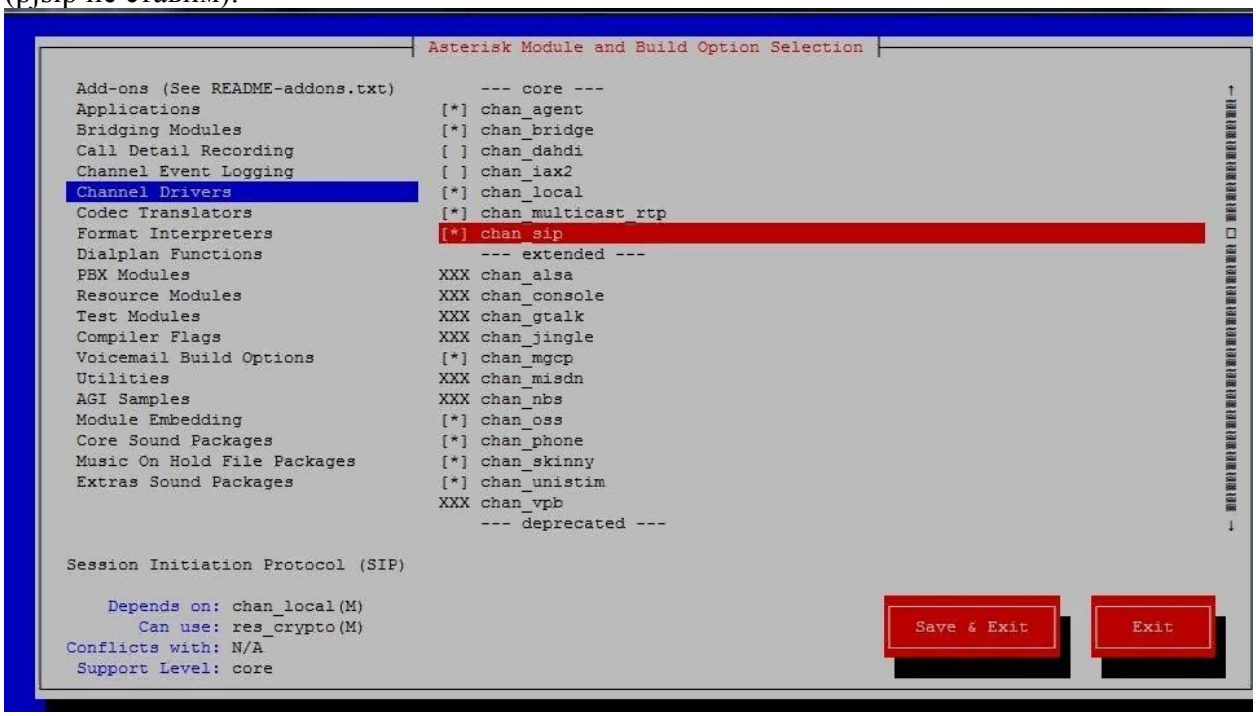
Чтобы получить эффективное и рабочее решение, рекомендуем: выполняйте установку и настройку Asterisk в чистом виде, без дополнительных плат расширения и модемов. Так вы получите программную АТС, которую можно легко переносить с одного сервера на другой. Для этого необходимо установить Asterisk с нуля, инсталлировать pjproject с jansson, обновить систему и отключить SELinux.
Для начала отключим **Selinux**. Для этого заходим /etc/selinux/config и ставим: *SELINUX=DISABLED*.
Также выключаем **FireWall (iptables)**:

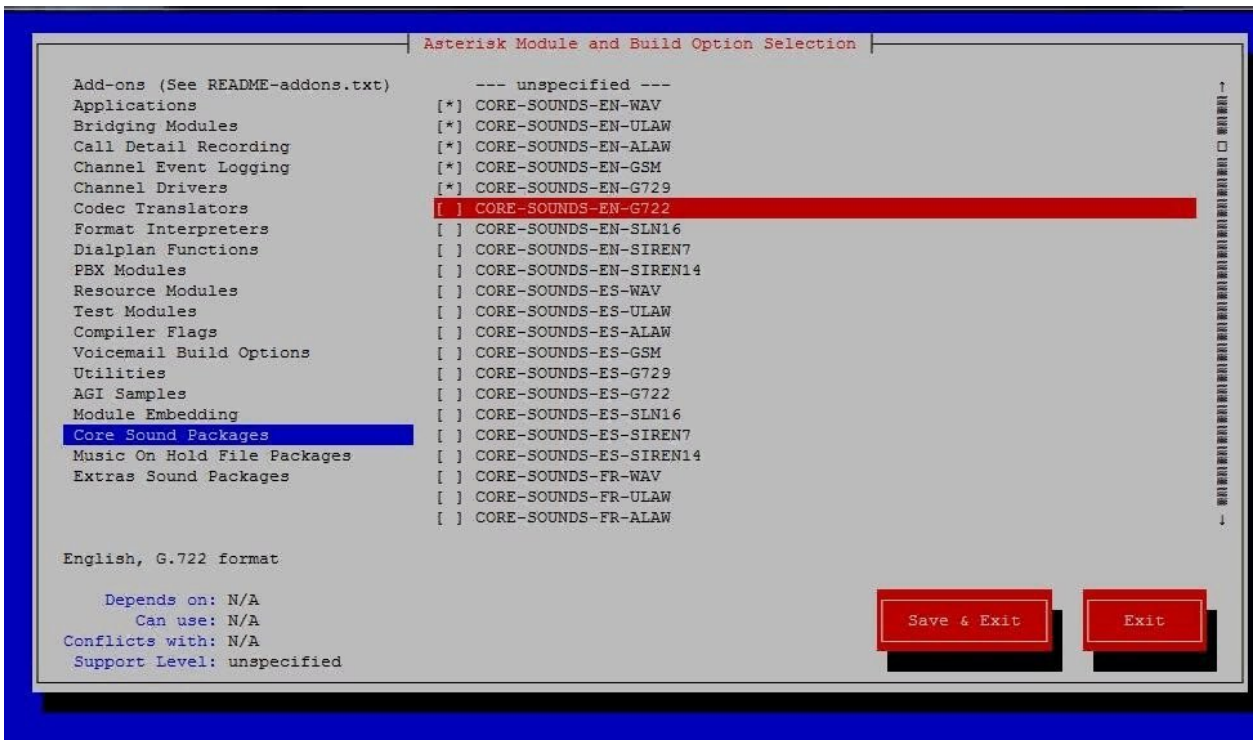
1. Проверкастатуса: service *iptables status*;
2. Отключение: service *iptables stop*
3. Отключение из автозагрузки: *chkconfig iptables off*
4. Перегружаем систему: *reboot*

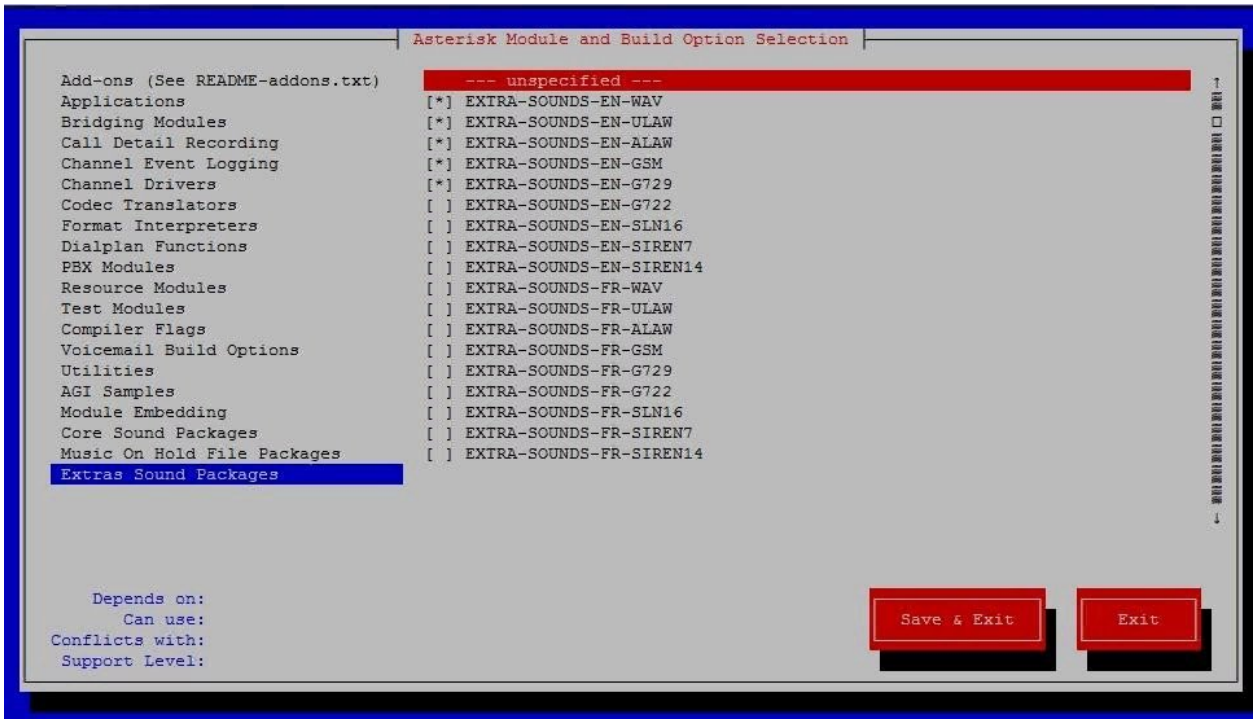
Скачайте и инсталлируйте pjproject:
d /usr/src
git clone git://github.com/asterisk/pjproject pjproject
cd pjproject/
./configure –libdir=/usr/lib64 –prefix=/usr –enable-shared –disable-sound –disable-resample
make dep
make
make install
ldconfig
ldconfig -p | grep pj
Для конвертации mp3 файлов необходим пакет Lame. Установим его из репозитория:
rpm -Uvh http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el6.rf.x86_64.rpm
yum repolist — проверка установленных репозиториев
Далее устанавливаем сам пакет: *yum install lame*
Скачиваем и устанавливаем библиотеку Libpri:
cd /usr/src/
wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz
tar xvfz libpri-1.4-.tar.gz*
*cd /usr/src/libpri-1.4.**
make

make install
Если команды wget – не существует, то устанавливаем ее командой *yum –y install wget*
Далее скачиваем и устанавливаем сам **asterisk 13**:
cd /usr/src/
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
tar xvfz asterisk-13-current.tar.gz
cd asterisk-13.*
contrib/scripts/get_mp3_source.sh
./configure –libdir=/usr/lib64
Если при проверки и подготовки сборки необходимых настроек, моделей никаких ошибок нету, то появиться в консоли иконка **Asterisk**

make menuselect — выбираются все необходимые параметры, но в принципе можно оставить по умолчанию, главное чтобы были включены необходимые драйверы каналов
Выберите модули и звуки (можно оставить по ум-чанию). В модулях выбираем только sip. (pjsip не ставим):







Пользователи, пароли и контекст

Установите любую программную «звонилку» или воспользуйтесь реальным телефоном. В первом варианте вам понадобится настроить софт для работы с АТС. В нашем примере

используем Zoiper 5. Пример настроек указан в нашей вики http://wiki.new-tel.net/doku.php?id=Zoiper-PC:

Настройки софтовой «звонилки» для проверки Asterisk

Все дальнейшие настройки звонилки и принцип работы указан в ссылке выше.

Теперь проверьте подключенные пиры с помощью команды:

Sip show peers

Если все верно, вы увидите такую строку:, в котором видно нашу SIP-линию и статус подключения SIP-линии:

Sip-линия IP-address A 5060 OK Cached RT

После настройки Asterisk протестируйте звонки на двух абонентах. Для этого подключите еще один физический или программный телефон. Позвоните от одного абонента другому (набрав с 101 на 102 и наоборот). Проверьте содержимое файла */var/log/asterisk/full.* – там появится запись о последнем вызове. Также там фиксируется все сообщения и ошибки, возникаемые при работе **Asterisk**.

Записи обо всех последующих вызовах тоже попадут в этот файл. Позже их можно будет перебросить в базу данных.

Настройка транка

Зарегистрируйтесь у SIP-провайдера и получите настройки транков. Необходимую информацию – логин, пароль, адрес сервера, настройки подключения и номера для тестирования – можно найти в личном.
В конец файла *sip.conf* добавьте нового пира, как это рекомендует ваш провайдер:
[test_trunk]
context=trunk_cid
dtmfmode=rfc2833
host=ip-адрес sip-провайдера
type=friend
username=test_trunk
qualify=yes
secret=password ;парольдляподключениятранка
disallow=all
allow=ulaw
allow=alaw
allow=g729
insecure=invite,port
nat=yes
Пусть Asterisk заново перечитает файл:
Sip reload
Если настройка программы в IP АТС Asterisk прошла успешно, в консоли появится такая строка:
Sip-линия IP-address A 5060 Unmonitored Cached RT
Редактирование dialplan
Чтобы настроить входящие и исходящие звонки в IP-телефонии Asterisk, отредактируйте файл *extensions.conf, добавив в конце следующий код (с контекста local)*:
;для исход по транку (пример указан с префиксом 123#).
exten => _123#8XXXXXXXXXX,1,Set(CALLERID(all)=78125000963)
exten => _123#8XXXXXXXXXX,n,Noop((CALLERID(all) + Boris)
exten => _123#8XXXXXXXXXX,n,Dial(SIP/7${EXTEN:5}@Ip-address)
; избавление от префикса 123# и заменой цифры 8 на 7. Далее отправляется звонок на хост IP провайдера (указан в sip.conf)
[trunk_cid]
;для вход. по транку на 101.
exten => _XXXXXXXXXX,1,Dial(SIP/101,30,r)
Перезагрузите Asterisk командой *core restart now* и снова сделайте тестовый звонок. Информация о нем добавится в файле full
Пример лога консоли Asterisk:

На этом базовая настройка IP-телефонии «Астерикс» завершена. Чтобы расширить функционал после того, как Asterisk установлен, настройте приветствие и голосовое меню

(ivr), активируйте голосовую почту, настройте очередь (queue) входящих звонков, сбор и просмотр статистики (cdr viewer), запись (record) разговоров, поставьте музыку на ожидание (on hold), настройте конференции, перевод, перехват и переадресацию звонков.

Практическое задание:*Тестирование кодеков. Исследование параметров качества обслуживания*

Лабораторная работа

Цель работы: провести тестирование существующих кодеков, сравнить различные реализации кодеков. Получить экспериментальные данные загрузки кодеками сетевого канала, объем потребляемого трафика и подверженности кодеков негативным влияниям задержек и потерь пакетов в сети передачи данных.

Задание на лабораторную работу

Для выполнения лабораторной работы необходимо протестировать используемые кодеки на количество потребляемого трафика, занимаемую полосу пропускания, подверженность влиянию негативных воздействий несущей сети.

1. Запустить сервер IP телефонии на основе лабораторной работы №2.
2. В sip.conf установить тестируемый кодек.
3. С помощью trafshow провить используемый кодеком трафик и скорость передачи.
4. В Wireshark выставить фильтр на UDP пакеты и только с нужных нам адресов и посмотреть сколько пакетов передалось за минуту и какой их размер.
5. Оценить качество связи при загруженной сети.

2.Краткие теоретические сведения

1. Кодирование речевой информации

Источником информационных данных является речевой сигнал, возможной моделью которого является нестационарный случайный процесс. В первом приближении можно выделить следующие типы сигнальных фрагментов: вокализированные, невокализированные, переходные и паузы. При передаче речи в цифровой форме каждый тип сигнала при одной и той же длительности и одинаковом качестве требует различного числа бит для кодирования и передачи. Следовательно, скорость передачи разных типов сигнала также может быть различной, что обусловливает применение кодеков с переменной скоростью. В результате передача речевых данных в каждом направлении дуплексного канала рассматривается как передача асинхронных логически самостоятельных фрагментов цифровых последовательностей (транзакций) с датаграммной синхронизацией внутри транзакции, наполненной блоками различной длины. В основе кодека речи с переменной скоростью лежит классификатор входного сигнала, определяющий степень его информативности и, таким образом, задающий метод кодирования и скорость передачи речевых данных. Наиболее простым классификатором речевого сигнала является Voice Activity Detector (VAD), который выделяет во входном речевом сигнале активную речь и паузы. При этом, фрагменты сигнала, классифицируемые как активная речь, кодируются каким-либо из известных алгоритмов (как правило, на базе метода Code Excited Linear Prediction — CELP) с базовой скоростью 4-8 кбит/с. Фрагменты, классифицированные как паузы, кодируются и передаются с низкой скоростью порядка 0.1 — 0.2 Кбит/с, либо не передаются вообще. При этом передача минимальной информации о фрагментах пауз предпочтительна. Данная стратегия позволяет оптимизировать скорость кодирования до 2-4 кбит/с при достаточном качестве синтезируемой речи. При этом для особо критичных фрагментов речевого сигнала выделяется большая скорость передачи, для менее ответственных — меньшая. Вместе с тем необходимо отметить, что вокодер вносит дополнительную задержку порядка 15-45 мс, возникающую по следующим причинам:

• использование буфера для накопления сигнала и учета статистики последующих отсчетов (алгоритмическая задержка);

• математические преобразования, выполняемые над речевым сигналом, требуют процессорного времени (вычислительная задержка).

Данную задержку необходимо учитывать при расчете сквозных задержек. Проведенный в различных исследовательских группах анализ качества передачи речевых данных через сеть Интернет показывает, что основным источником возникновения искажений, снижения качества и разборчивости синтезированной речи является прерывание потока речевых данных, вызванное:

• потерями пакетов при передаче по сети связи;

• превышением допустимого времени доставки пакета с речевыми данными.

Это требует решения задачи оптимизации задержек в сети и создание алгоритмов компрессии речи устойчивых к потерям пакетов (восстановления потерянных пакетов).

Таблица 5.1 – Сравнительные характеристики VoIP кодеков

Кодек	Размер полезной нагрузки пакета (байты)	Информационная скорость (Кбит/с)	Алгоритмическая задержка	Занимаемый поток IP-пакетами (Кбит/с)	Занимаемый поток Ethernet-фреймами (Кбит/с)
G.711	160	64	20	64.8	80
G.723.1 (6.3)	24	6.3	37.5	6.9	17.1
G.723.1 (5.3)	20	5.3	37.5	5.9	16
G.726-32	160	32	20	32.8	42.7
G.726-24	160	24	20	24.8	34.7
G.726-16	160	16	20	16.8	26.7
G.729(8)	20	8	25	8.8	18.7
G.729(6.4)	16	6.4	25	7.2	17.1

Декодирование речевой информации

С учетом возможных потерь пакетов в сети для восстановления речевого потока на приемной стороне используется протокол реального времени — Real Time Protocol (RTP). В заголовке данного протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты. Восстановленная последовательность, с возможными пропусками как одиночных пакетов, так и групп пакетов, поступает на декодер. Декодер должен обеспечить восстановление речевой информации, заполнение пауз фоновым шумом, а также эхо компенсацию кодируемого сигнала, обнаружение и детектирование телефонной сигнализации.

3. Механизмы оптимизации задержек в сети

Задержки пакетов в IP-сетях определяются:

- случайной задержкой пакетов на обработку в транзитных маршрутизаторах;
- датаграммным режимом передачи, приводящим к нарушению порядка следования пакетов и необходимости их сортировки на принимающей стороне.

В соответствии с этим существует несколько подходов к оптимизации задержек с целью обеспечения требуемого качества передачи.

1. Реализация первого подхода предусматривает резервирование части пропускной способности сети для передачи пакетов с речевой информацией. Для того, чтобы более эффективно использовать зарезервированную полосу пропускания, на оконечном или шлюзовом оборудовании должна осуществляться предварительная концентрация речевой информации. При этом IP-пакеты должны формироваться не по мере поступления

речевых сигналов, а с некоторой задержкой, достаточной для сборки информационного блока больших размеров. Передача речи в больших информационных блоках упрощает процедуру управления очередями на транзитных узлах, что очень существенно в связи с неразвитой системой приоритетов существующего протокола IP. Однако реализация этого подхода приводит к появлению дополнительной задержки.

Для резервирования полосы пропускания в сети IP может использоваться метод WFQ (Weighted Fair Queuing) или протокол RSVP.

- Метод WFQ позволяет для каждого вида трафика выделять определенную часть полосы пропускания. Оператор через систему административного управления может задать количество очередей (до 10 очередей для передачи данных и одну очередь для системных сообщений). В случае, если одна очередь не использует полностью выделенную ей полосу пропускания, то свободный резерв полосы пропускания может задействоваться для передачи информации из следующей очереди. Этот метод позволяет гибко использовать ресурсы сети и реализован в оборудовании фирмы Cisco.
- Протокол RSVP предназначен только для резервирования части пропускной способности. Механизм работы данного протокола описан выше. Недостатком протокола RSVP является то, что полоса пропускания, выделяемая источнику информации, при снижении активности источника не может быть использована для передачи другой информации. Как альтернатива этому способу может использоваться алгоритм управления потоками на основе системы приоритетов, однако в существующей версии IP этот механизм развит недостаточно.

2. Также одним из способов оптимизации задержки в сети является использование протокола RTCP (Real-Time Transport Control Protocol), который позволяет приложению реагировать на изменение состояния сети.

+3. Третий подход предусматривает построение магистральной транспортной сети Интернет на основе технологии Frame Relay или ATM. В этом случае пограничные узлы IP взаимодействуют друг с другом через виртуальные соединения сети Frame Relay или ATM, для которых гарантируются параметры качества обслуживания (скорость передачи, время и джиттер задержки). Использование Frame Relay или ATM позволяет отказаться от применения транзитных маршрутизаторов IP. При этом возможно более эффективное использование полосы пропускания за счет установления соединения для каждого телефонного разговора.

3. Порядок выполнения работы

Для выполнения лабораторной работы необходим установленный и настроеный согласно требованиям второй лабораторной работы сервер **Asterisk**. А также утилита**trafshow**– из пакета netdiag для Ubuntu (можно также использовать любое другое ПО, позволяющее считать трафик), и программа**Wireshark**для отлавливания пакетов, содержащих голосовой трафик. Из аппаратного обеспечения нужен IP – телефон (при отсутствии можно использовать любой softphone) в количестве не менее двух экземпляров.

Необходимо протестировать каждый их кодеков по отдельности, но так как все кодеки тестируются по одному плану, то приведем этот план на примере тестрования кодека G.729.

+

1. Настраиваем /etc/asterisk/sip.conf. В строке, где задаётся кодек, ставим нужный нам: allow =g729, также включаем NAT, чтобы трафик шёл через наш сервер: nat=yes. Остальные настройки программы asterisk приведены во второй лабораторной работе. Конфигурируем телефоны, указывая наш сервер и кодек g729.
2. Для проверки используемого кодеком трафика и скорости передачи запускаем trafshow. Звоним с одного телефона на другой, засекаем 1 минуту. Отмечаем исходящий и входящий трафик с адресов, принадлежащих телефонам. Скорость будет отношением трафика и времени опыта.

3. Аналогичный опыт проводим с отключенной трубкой для определения полезного трафика. Этим самым мы определим сжимает ли кодек тишину или пропускает её.
4. Проводим аналогичные опыты со включенной программой Wireshark, в которой выставлен фильтр, чтобы утилита ловила только UDP пакеты и только с нужных нам адресов. Таким образом мы увидим сколько пакетов передалось за минуту и какой их размер.
5. Провести чисто субъективный опыт, который будет заключаться в том, какое качество связи будет при загруженной сети. Для этого нужно просто общаться через телефоны и слушать качество передаваемого звука в то время, как с сервера будет исходить большой трафик (можно просто с сервера качать большой файл, например фильм).

Тестирование нужно провести при величине задержек более 500 мс и потери пакетов около 10%.

Практическое задание: *Мониторинг и анализ соединений по различным протоколам*

Лабораторная работа

Цель: изучить принципы работы простейших средств мониторинга сети.
получить навыки решения задач, связанных с мониторингом сети.
Теоретические основы
1. Протокол ICMP
Протокол ICMP (Интернет-протокол контрольных сообщений) стека протоколов TCP/IP предназначен для передачи между сетевыми устройствами сообщений об ошибках и контрольных сообщений при помощи IP-пакетов.
В протоколе ICMP определены несколько типов сообщений, в том числе:

Destination Unreachable	Time to Live Exceeded	Parameter Problem
Source Quench	Redirect	Echo
Echo Reply	Timestamp	Timestamp Reply
Information Request	Information Reply	Address Request
Address Reply		

Например, если маршрутизатор получает пакет, который он не может доставить по указанному в нем адресу, отправителю передается ICMP-сообщение о недостижимости адреса (Destination Unreachable).
2. PING: Проверка соединения с определенным интерфейсом.
Программа ping использует протокол ICMP.
Эта команда посылает пакет эхо-запроса на другой IP-адрес и ожидает ответа. Она чаще всего используется для того, чтобы посмотреть, «жив ли» другой компьютер. Ответ на запрос содержит также данные о том, как долго пакет путешествовал до адресата. Можно использовать команду ping с различными опциями: число посланных пакетов (от 1 до 10), время жизни пакета (time to live –TTL, от 1 до 255ms), размер пакета (от 16 до 8192 байт), время ожидания (timeout, до 9999 ms) и разрешать или нет фрагментацию каждого пакета.
Формат команды в ОС Windows:
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list
Options:
-t Выполнение команды до прерывания (Ctrl+C)
-a Разрешать адреса в имена
-n count Число отправляемых пакетов.

-l size Размер буфера отправки
-f Установить флаг "Не фрагментировать".
-i TTL Установить время жизни.
-w timeout Время ожидания ответа в мс.
-v TOS Задание типа службы (поле "Type Of Service").
-r count Запись маршрута для указанного числа переходов.
-s count Штамп времени для указанного числа переходов.
-j host-list Свободный выбор маршрута по списку узлов.
-k host-list Жесткий выбор маршрута по списку узлов.
destination-list Список рассылки.
3. Программа tracert. Определение промежуточных сетевых интерфейсов между хостами. Трассировка маршрута
Программа трассировки маршрута использует протокол ICMP.
Эта утилита очень похожа на Ping, за исключением того, что она показывает все другие IP-адреса (интерфейсы), которые пакет проходит до своего места назначения. Дополнительно можно изменять различные опции, ассоциированные с Trace Route: максимальное число дозволяемых промежуточных узлов (maximum hops, от 1 до 255) и timeout (до 9999 ms).
Формат команды в ОС Windows:
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
Options:
-d Не разрешать адреса в имена.
-h maximum_hops Наибольшее число промежуточных узлов.
-j host-list Трассировка через определенный список хостов
-w timeout Время ожидания каждого ответа в мс.
4. Программа netstat. Сетевая статистика.
Программа netstat используется для просмотра активных соединений каждого протокола, таблиц маршрутизации, а так же детализирует статистику передачи данных.
Формат команды в ОС Windows:
netstat [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]
-a Отображение всех подключений и ожидающих портов.
(Подключения со стороны сервера обычно не отображаются).
+-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.
-n Отображение адресов и номеров портов в числовом формате.
-p имя Отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.
-r Отображение содержимого таблицы маршрутов.
-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных.
интервалПовторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.
Средства/Подготовка
В работе будут использоваться сети, соединенные с рабочей станцией линками разных типов. Первая сеть (194.85.33.0) доступна через спутниковый канал связи, проходящий через спутниковый ретранслятор на геостационарной орбите с пропускной способностью 512 кбит/с. Вторая сеть 217.23.64.0 доступна через наземный волоконно-оптический канал связи с пропускной способностью 2 Мбит/с, третья сеть 212.194.38.0 входит в состав корпоративной сети ВУЗа и доступна в локальной сети с пропускной способностью 10/100 мбит/с.

В качестве альтернативного инструмента анализа сети используется интерфейс Looking Glass на сайте http://noc.runnet.ru(IP-адрес 194.85.35.100).
Ход работы Задание 1. Ping
Выполните команду ping в командной строке с различными значениями параметров -t, -n, -l, -i,-w. Какие наблюдения и выводы вы сделали?
ping www.seun.ru
ping www.sgu.ru
ping www.microsoft.com
ping www.sun.com
ping212.193.38.83

_____
_____

Выполните ping к тем же хостам с параметром –f, увеличивая параметр -l size. При каком значении размера перестают получаться ответы?

_____
_____

Задание 2. Tracert
Выполните команду tracert в командной строке с различными значениями параметров. Какие наблюдения и выводы вы сделали?
Используйте, например,
tracertwww.seun.ru
tracert www.sgu.ru
tracert www.microsoft.com
tracert www.sun.com
tracert 212.193.38.83
Задание 3. Поисковые сервисы Европейского и Российского ip-регистров
Определите, кому принадлежат сети 194.85.33.0, 217.23.64.0, 212.193.38.0. Для этого используйте поисковые аппараты http://www.ripe.net/db/whois/whois.htmlиhttp://www.ripn.net:8080/nic/whois/index.html.
Пользуясь данными этих информационных систем, попробуйте определите географическое расположение сетей. Попробуйте изобразить топологическую схему соединения этих сетей.
Задание 4. Использование программы ping для исследования параметров сети.
1. Приведите сравнительные результаты выполнения команд ping по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10 по параметрам «время отклика», TTL в форме таблицы. Объясните полученные различия.
2. Соберите средние времена прохождения 10 пакетов на указанные адреса. Сравните с р4езультатами, полученными при использовании сервиса ping в интерфейсе Looking Glass на сайте http://noc.runnet.ru. Объясните полученные различия.
3. Соберите усредненные времена прохождения 10 пакетов увеличивающегося размера по указанным адресам. Начните с 64 байт и каждый раз удваивайте размер пакета. При каком размере пакета потери превышают 50 %. Как влияет время ожидания отклика на процент прохождения пакетов этого размера. При каком времени ожидания отклика потери для пакетов зафиксированного размера не возникают?
Представьте результаты измерений в форме таблиц, наилучшим образом проявляющим, по вашему мнению, обнаруженные зависимости.
+4. Используя программу ping, оцените вклад разных сетевых участков, по которым проходит эхо-пакет между вашей рабочей станцией и интерфейсом 194.85.33.29.
Задание 5. Использование программы tracert для анализа соединений в сети.

+1. Приведите сравнительные результаты выполнения команд tracert по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10. Объясните полученные различия.

2. Выполните трассировку к адресу 212.193.38.248 и к адресу 217.23.64.2 со стороны сайта http://noc.runnet.ru. Приведите полученные результаты.

3. Используя данные, полученные в результате выполнения трассировки и отправки эхо-пакетов между интерфейсами 212.193.38.248 и 194.85.35.100, оцените вклад разных участков сетей, соединяющих эти интерфейсы, в среднее время прохождения пакетов между ними.

4. Используя полученную в ходе выполнения всех заданий информацию, уточните схему задания 1, изобразите на ней обнаруженные вами промежуточные интерфейсы и линки сети, объединяющей подсети 194.85.33.0, 217.23.64.0, 212.193.38.0.

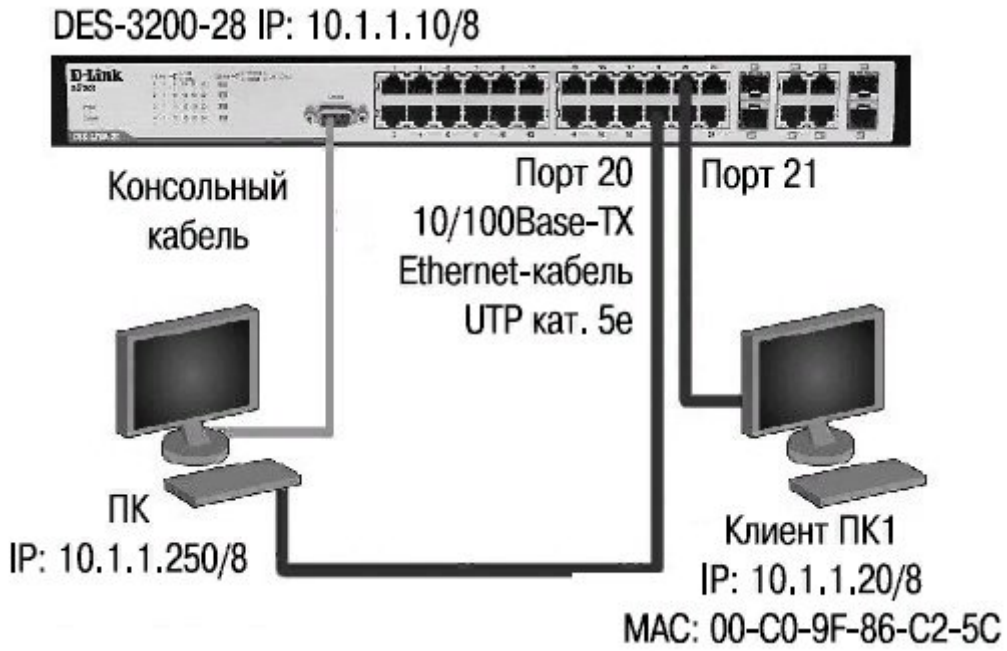
Практическая работа *Мониторинг вызовов в программном коммутаторе*

Вид контроля:Лабораторная работа

Цель: изучить процесс мониторинга состояния коммутатора.

Оборудование:

DES-3200-28	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.



Настройка DES-3200-28

Изучение команд просмотра утилизации (загрузки) портов и CPU коммутатора

Просмотрите загрузку CPU коммутатора

show utilization cpu

Внимание! В случае длительной загрузки CPU более 90-100% необходимо проверить следующие характеристики:

1. возможные атаки на коммутатор, неправильная настройка сети. Данная проблема может быть решена путем включения функции *SafeGuard* Engine;
2. неправильная настройка ACL или других функций коммутатора, влияющих на производительность и работу CPU;
3. некорректная работа ПО коммутатора при выполнении некоторых функций. Данная проблема может быть решена путем замены ПО коммутатора.

Просмотрите загрузку портов коммутатора

show utilization ports 1-24

Примечание. С помощью данной команды можно посмотреть как загрузку (утилизацию) портов коммутатора, так и объем передаваемого трафика.

Изучение команд просмотра статистики/ошибок передаваемых пакетов на порте коммутатора

Просмотрите пакеты, передаваемые станцией ПК1, подключенной к порту 21

show packet ports 21

Примечание. Данная команда позволяет определять количественные характеристики передаваемых пакетов. В случае большого количества широковещательного трафика (более 15% от общего числа передаваемого трафика) необходимо провести анализ на наличие в сети *DOS-атак* или ее неисправности (широковещательный шторм).

Просмотрите статистику об ошибках пакетов, принимаемых и передаваемых через порт 21

show error ports 21

Примечание. Данная команда позволяет определять ошибки передаваемых данных и локализовать проблемы в коммутируемой сети.

Очистите счетчики статистики на порте 21

clear counters ports 21

Примечание. В случае устранения выявленных ошибок или проверки отчета загрузки портов можно обнулить устаревшие данные.

Изучение команд просмотра сессий подключенных к коммутатору пользователей и Log-файла коммутатора.

Проверьте сессии пользователей, подключенных к коммутатору

show session

Просмотрите Log-файл коммутатора

show log

Просмотрите Log-файл коммутатора, начиная с определенного индекса

show log index 25

Очистите Log-файл

clear log

Команда диагностики кабелей

Протестируйте состояние медных кабелей, подключенных к портам коммутатора

cable_diag ports all

Примечание. Данная функция позволяет определить состояние пар подключенного к порту коммутатора медного кабеля, а также его длину. Функция определяет следующие повреждения кабеля: разомкнутая цепь (Open Circuit) и короткое замыкание (Short Circuit).

Практическое задание:*Создание резервных копий баз данных*

Лабораторная работа

Цель работы: ознакомиться с основными конструкциями SQL, технологиями среды MS SQL Server Management, объектами SMO (среды MS Visual Studio) для резервного копирования и восстановления БД.

Задание №1. необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

Ход работы:

1. Запустите SQL Server Management Studio (SSMS), подключитесь к своему экземпляру SQL Server, используя технологию 1.
2. Создайте папку с именем c:\Student\ВашаПапка\test.

3. Откройте окно нового запроса. Измените контекст на базу данных master, используя технологию 6. Наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных:
   BACKUP DATABASE MMM TO DISK = 'C:\.....TEST\AW.BAK’
   Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.
4. Внесите изменение в таблицу «Модель» базы данных MMM. Добавьте одну запись (придумайте сами)/
5. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать резервную копию журнала транзакций и сохранить только что внесенное изменение:
   BACKUP LOG MMM TO DISK = ‘C:\.....TEST\AW1.TRN'
   Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.
6. Внесите еще одно изменение в таблицу«Модель».
7. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать разностную резервную копию базы данных:
   BACKUP DATABASE MMM TO DISK = ‘C:\.....\TEST\AWDIFF1.BAK' WITH DIFFERENTIAL
   Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.
   +
8. Внесите еще одно изменение в таблицу«Модель».
9. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных в указанном месте на диске:
   BACKUP LOG MMM TO DISK = ‘C:\....TEST\AW2.TRN'
   Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.
   Задание №2. необходимо провести восстановление базы данных «MMM» из сделанных в задании №1 резервных копий.
   Ход работы:
   +
1. Если необходимо, запустите SSMS, подключитесь к своему экземпляру SQL Server, используя технологию 1.
2. Выполните восстановление БД из первой полной резервной копии (C:\...TEST\AW.BAK) средствами оболочки SSMS. Для этого выполните:

- В обозревателе объектов вызовите контекстное меню на вашей БД и выберите задачу восстановления базы данных (см. рисунок 6)

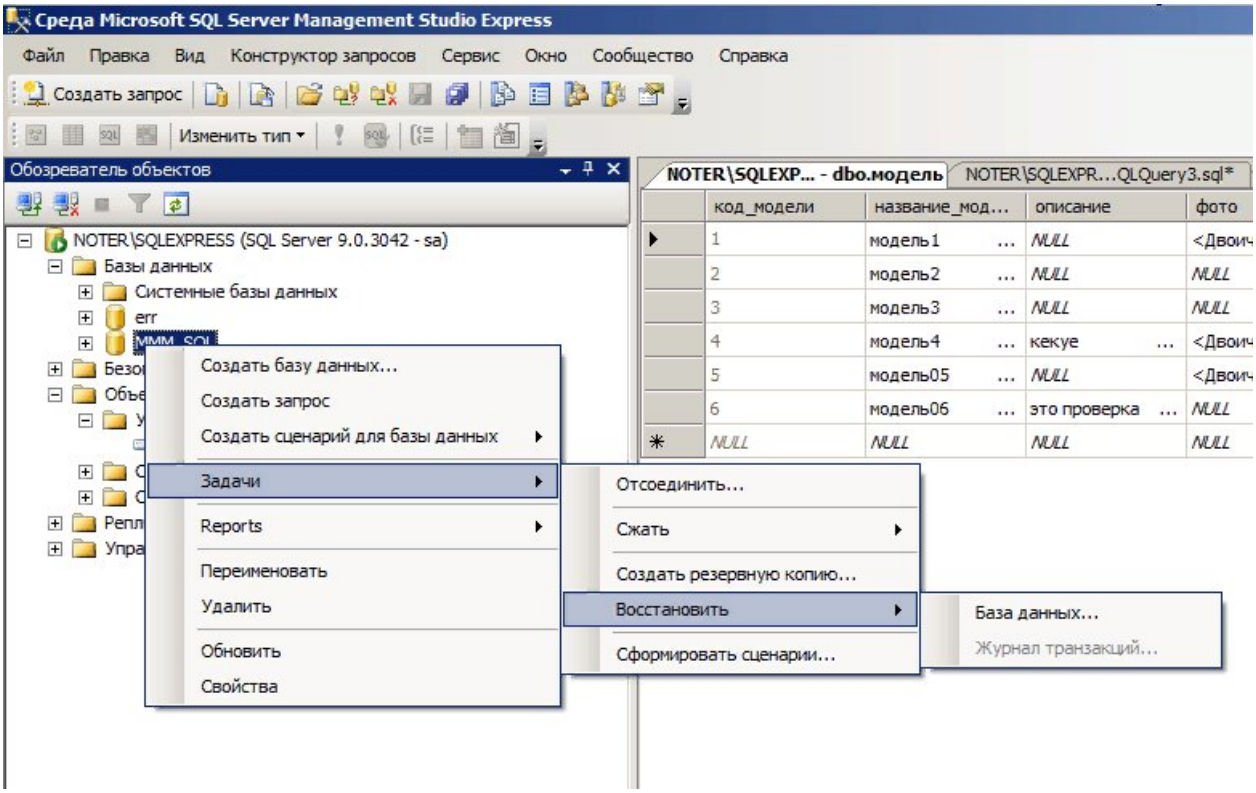
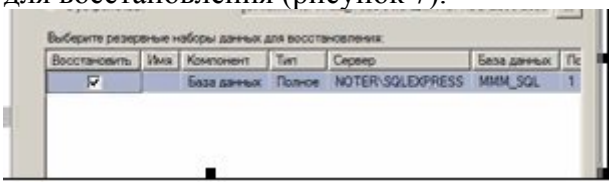


Рисунок 6 – Восстановление БД

- В открывшемся окне необходимо задать следующие параметры восстановления

+На закладке «Общие» необходимо выбрать:

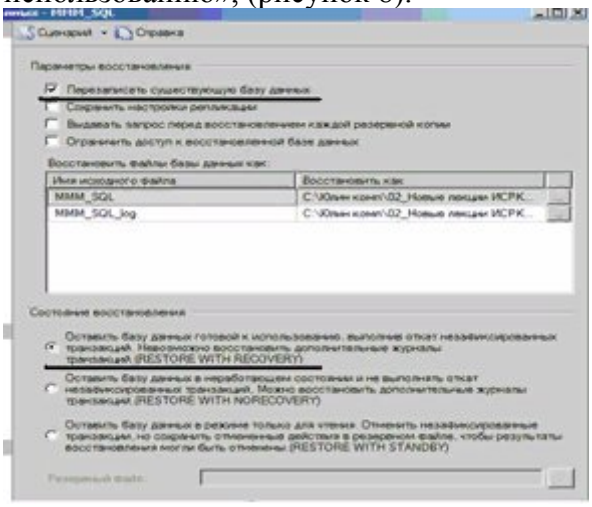
1. Базу данных для восстановления (вашу MMM)
2. Выбрать источник набора данных для восстановления с устройства à файл C:\...TEST\AW.BAK
3. После определения файла-источника данных необходимо флажком выбрать базу данных для восстановления (рисунок 7).



На закладке «Параметры»

+

1. необходимо включить опцию «Перезаписать БД» и «оставить БД готовой к использованию», (рисунок 8).



3. Нажмите ОК
4. После восстановления БД, откройте таблицу «Модель» и убедитесь, что она не содержит всех добавлений, вносимых вами в процессе выполнения упражнения, так как восстановление происходило из первой резервной копии (без изменений).

   Задание №3. необходимо организовывать со стороны клиентского приложения, созданного в Visual Studio удаленное администрирование БД (резервное копирование).

   Ход работы:

   В Visual Studio

   +

1. Создайте новый проект Windows Application и сохраните его в своей папке под именем Лабы_МММ_2 семестр.
2. В главную форму добавьте меню, изображенное на рисунке 9:

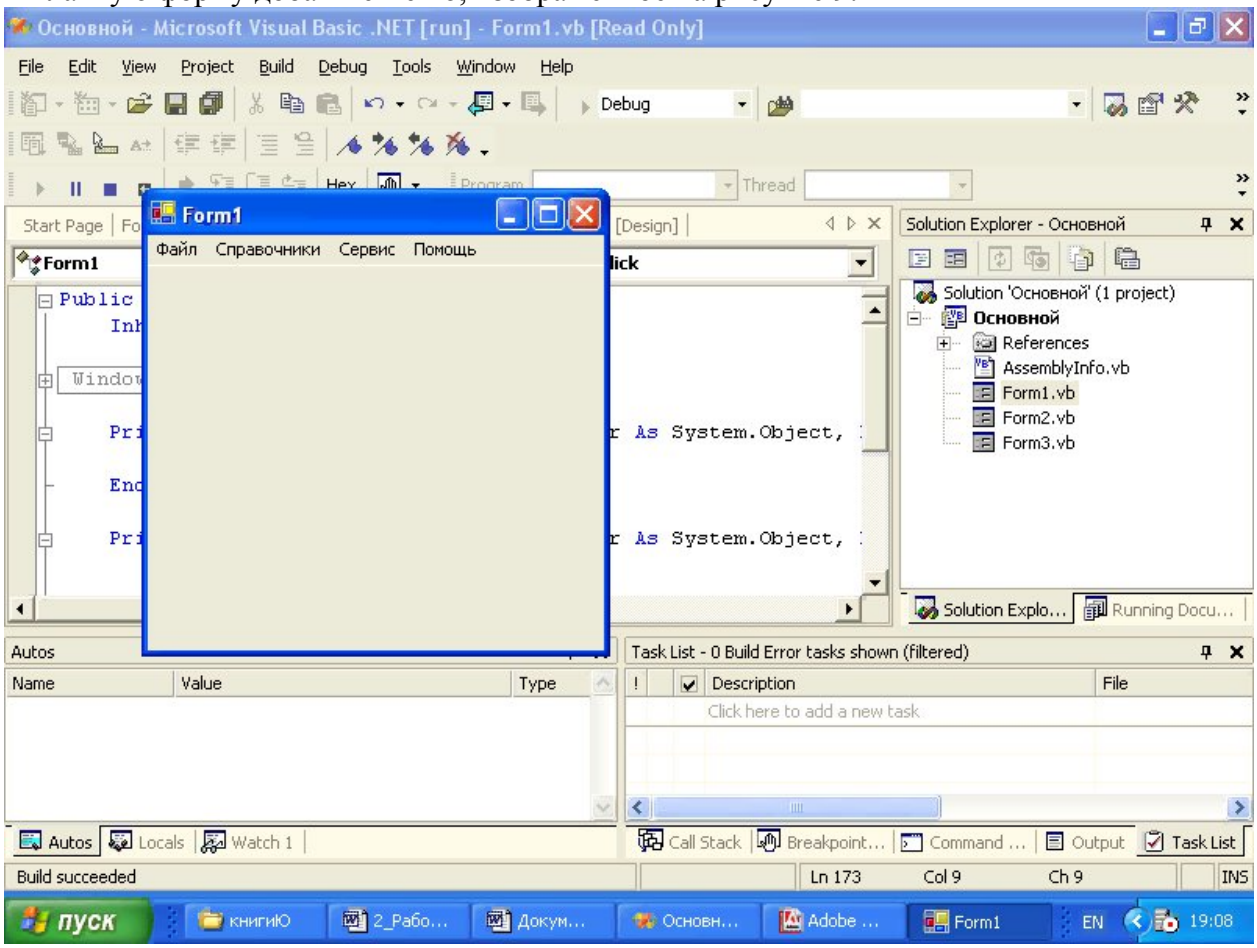


Рисунок 9 – Главное меню проекта

Файл (Открыть, Закрыть, Выход)

Справочники (Модель, Магазин, Дерево моделей)

Заказы (Работа с заказами)

+Отчеты (Прайс-лист, Бланк заказов)

Администрирование БД (Резервное копирование, Безопасность)

Сервис (Калькулятор)

Помощь (Справка, О программе)

3. Добавьте новую форму в проект
4. Добавьте на только что созданную форму компоненты в соответствии с рисунком 10.

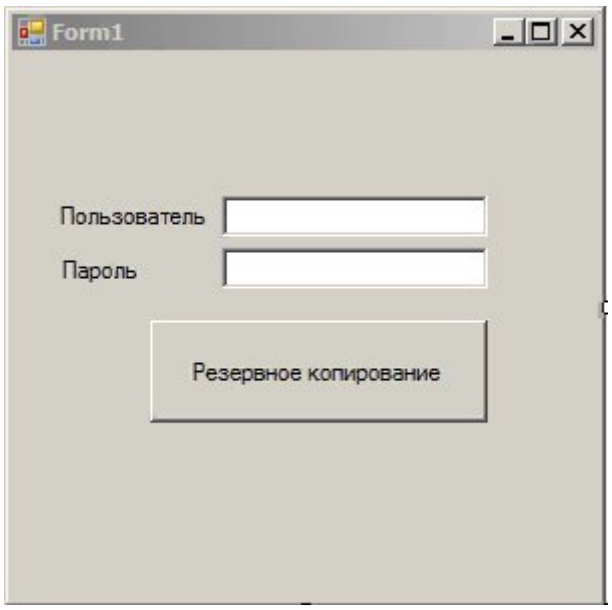


Рисунок 10 – Форма для подключения к серверу

5. Обеспечьте функциональную работу формы (напишите обработчик кнопки «Резервное копирование» с использованием объектов SMO. Описание объектов SMO, их свойств и методов см. в лекционном материале.)
6. Добавьте возможность открытия данной формы при выборе в главной форме пункта меню Администрироване БД à Резервное копирование
7. Запустите проект, проверьте работу формы.
8. Закройте проект
9. Убедитесь в появлении файла резервной копии на диске (файл, который указан в тексте программы).
10. Откройте SSMS. Добавьте в таблицу «Модель» новую строку данных (самостоятельно).
11. Средствами оболочки SSMS, выполните восстановление БД из резервной копии, созданной вашей программой
12. Убедитесь, что после восстановления добавленных строк в таблице «Модель» нет.

Задание №4. Ответьте на вопросы теста и представьте результаты преподавателю.

1. Вы выполняете разностное резервное копирование базы длимых AdveniurtWorks каждые четыре часа, начиная с 04:00. полная резервная копия создается в полночь. Какие данные будут содержаться в разностной резервной копии сделанной в полдень?

1. A Страницы данных, измененные после полуночи.
2. B. Экстенты, измененные после полуночи.
3. C. Страницы данных, измененные после 08:00
4. D. Экстенты. измененные после 08:00.

2. Вы выполняете полное резервное копирование базы данных Adventure Wortks,, которое завершается в полночь. Разностное резервное копирование выполняется по расписанию каждые четыре часа, начиная с 04:00. Резервное копирование журнала транзакций происходит по расписанию каждые пять минут. Какую информацию будет содержать резервная копия журнала транзакций, созданная в 09:15?

+

1. A. Все транзакции, начатые после 09:10.
2. B. Транзакции, завершенные после 09:10.
3. C. Страницы, измененные после 09:10.
4. D. Экстенты, измененные после 09:10.

Практическое задание:*Диагностика и устранение неисправностей в системах IP-телефонии*

Лабораторная работа

Цель: научиться выявлять возможные неисправности сетевого оборудования.

Оборудование: ПК, сетевые анализаторы; кабельные сканеры.

Теоретические сведения

Локальная вычислительная сеть — это распределенная система, построенная на базе локальной сети связи и предназначенная для обеспечения физической связности всех компонентов системы, расположенных на расстоянии, не превышающем максимальное для данной технологии.

В реальности типичная «среднестатистическая малая ЛВС» состоит из трех условных классов устройств:

- компьютеров с установленными в них сетевыми адаптерами;
- кабельного оборудования, к которому относятся сетевые кабели, патчи, патч-панели и (опционально) шкафы или стойки;
- активного сетевого оборудования, которое также может быть размещено в шкафах или стойках, в том числе в тех же, что и патч-панели (как правило, это коммутаторы и/или концентраторы).

Современные проводные ЛВС реализуются на базе витых пар и оптоволоконных кабелей.

Основные правила прокладки кабеля:

1. Во избежание растяжения сила натяжения для 4-парных кабелей не должна превышать 110 Н (усилие примерно в 12 кг). Как правило, усилие свыше 250 Н приводит к необратимым изменениям параметров UTP-кабеля;
2. Радиусы изгиба установленных кабелей не должны быть менее четырех (некоторые производители настаивают на восьми) диаметров для кабелей UTP горизонтальной системы. Допустимый изгиб в ходе монтажа не менее 3÷4 диаметров;
3. Следует избегать излишней нагрузки на кабели, обычно вызываемой их перекручиванием (образование «барашков») во время протяжки или монтажа, чрезмерным натяжением на подвесных участках трасс, туго затянутыми узкими кабельными хомутами (или «пристреленными» скобами);
4. Кабели горизонтальной системы должны использоваться в сочетании с коммутационным оборудованием и патч-кордами (или перемычками) той же или более высокой категории рабочих характеристик;
5. Качество собранной кабельной системы в целом определяется по компоненту линии с наихудшими рабочими характеристиками.

Тестирование и диагностика сети

Под **диагностикой** принято понимать измерение характеристик и мониторинг показателей работы сети в процессе ее эксплуатации, без остановки работы пользователей.

Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки (утилизации) ее ресурсов или времени реакции прикладного ПО.

Тестирование — это процесс активного воздействия на сеть с целью проверки ее работоспособности и определения потенциальных возможностей по передаче сетевого трафика. Как правило, оно проводится с целью проверить состояние кабельной системы (соответствие качества требованиям стандартов), выяснить максимальную пропускную способность или оценить время реакции прикладного ПО при изменении параметров настройки сетевого оборудования или физической сетевой конфигурации.

Тестирование ЛВС осуществляется на стадии завершения работ по монтажу сети ЛВС и представляет собой осмотр созданной сети на предмет ее соответствия принятым стандартам. Серьезный и грамотный подход к тестированию лвс обеспечивает гарантию длительной, устойчивой и полноценной работы локальной сети и позволяет свести к минимуму работы в соответствии с таким немаловажным этапом, как диагностика сети.

Тестирование ЛВС включает в себя следующие этапы:

- проверка кабель-каналов
- осмотр рабочих узлов
- тестирование коммутационного оборудования

На этапе осмотра кабельных каналов проверяется целостность кабеля, правильность расположения кабельных жгутов, а также расположение кабельных трасс относительно источников помех и соответствие кабельной системы требованиям стандартов. Осмотр рабочих мест выявляет правильность прокладки кабеля вблизи розеточных модулей, а также наличие маркировки. Тестирование коммутационного оборудования определяет текущее состояние сети на предмет ее соответствия документации.

По результатам тестирования составляется отчет – документ, содержащий в себе выводы о техническом состоянии лвс и перечень рекомендаций по устранению выявленных неполадок, текущей эксплуатации и путям развития и модернизации сети в будущем.

Диагностика ЛВС является важной составляющей администрирования локальной сети и представляет собой процесс поиска неисправностей, замедляющих работу программного обеспечения и сети в целом. Последние можно условно разделить на три основные группы:

- физические неисправности
- ошибки в работе сетевых протоколов
- перегрузки в сети

Неисправности физического уровня связаны с выходом из строя сетевых устройств и компонентов. Перегрузки возникают вследствие невозможности сетевых устройств справиться с объемом поступающих к нему запросов. Ошибки в работе протоколов ведут к проблемам взаимодействия сетевых устройств друг с другом.

Для осуществления качественной диагностики ЛВС в мире разработано множество различных диагностических средств, позволяющих быстро определять причины сбоев в работе сетей. В области сетевой диагностики применяется, в частности, специализированное оборудование, такое как анализаторы сетевых протоколов, приборы мониторинга функционирования сети, кабельные и сетевые тестеры, а также специализированное тестирующее программное обеспечение. Так, обнаружить физическую неисправность можно с помощью простейших тестеров, проверяющих работу канала, а инструментальная диагностика ошибок, связанных с перегрузками и некорректной работой сетевых протоколов, осуществляется при помощи сетевых тестеров и анализаторов протоколов.

Поиск неисправностей в сети аппаратными средствами.

Условно, оборудование для диагностики, поиска неисправностей и сертификации кабельных систем можно поделить на четыре основные группы:

- приборы для сертификации кабельных систем;
- сетевые анализаторы;
- кабельные сканеры;
- тестеры (мультиметры).

Приборы для сертификации кабельных систем - проводят все необходимые тесты для сертификации кабельных сетей, включая определение затухания, отношения сигнал-шум, импеданса, емкости и активного сопротивления.

а)

в)

Рисунок 1 – Внешний вид приборов для тестирования ЛВС:
а) сетевой анализатор, б) кабельный сканер

Сетевые анализаторы - это эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем. Сетевые анализаторы содержат высокоточный частотный генератор и узкополосный приемник. Передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить затухание в линии и ее характеристики.

Кабельные сканеры позволяют определить длину кабеля, затухание, импеданс, схему разводки, уровень электрических шумов и оценить полученные результаты. Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания и т.д.) используется метод ―кабельного радара‖, или Time Domain Reflectometry (TDR). Суть эго состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс отсутствует.

Тестеры (омметры) - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не обозначают, где произошел сбой. Проверка целостности линий связи выполняется путем последовательной «прозвонки» витых пар с помощью омметра.

Оборудование для тестирования ВОЛС

Передача информации по оптоволоконным кабелям переживает бурный рост. Сначала оптоволоконная связь захватила область телекоммуникаций, вытеснила медные кабели на магистральных каналах и сегодня пробирается в крупные локальные сети и пресловутую "последнюю милю" между провайдером и "домашней" сетью Ethernet.

Стабилизированные оптические излучатели

применяются для ввода в оптическую линию сигнала, который будет измерен на выходе линии. Поэтому сигнал должен быть стабильным и, по возможности, монохроматическим (иметь определенную длину волны и узкий спектр). Мощность сигнала устанавливают регулировкой силы тока через излучатель.

Рисунок 2 - Внешний вид стабилизированного оптического излучателя

Рисунок 3 - Внешний вид измерителя оптической мощности

Измерители оптической мощности

используются для измерения оптической мощности сигнала и, в паре со стабилизированным оптическим излучателем, для измерения затухания в кабеле. Основным показателем качества измерителя оптической мощности является тип примененного в нем фотодиода.

Оптические аттенюаторы

Используются для моделирования потерь в оптической линии, что применяется для стрессового тестирования линии, при измерении коэффициента ошибок (BER), калибровке и проверке измерителей мощности, тестировании оптоэлектронных и электро-оптических преобразователей, анализе оптического бюджета линии.

Рисунок 4 - Внешний вид оптического аттенюатора

Визуальные дефектоскопы

Такой дефектоскоп состоит из простого источника света для подачи в кабель хорошо видимого красного сигнала в непрерывном или импульсном режиме. Дефектоскоп может использоваться для визуального обнаружения повреждений в кабелях и интерфейсах, обнаружения неоднородностей и оценки качества сварных швов. Свет будет проникать наружу в тех местах, где в оболочке волокна в результате перегиба, разрыва или плохой сварки имеется участок повышенного рассеяния, поэтому для его обнаружения остается только осмотреть кабель на наличие постоянного или мерцающего красного пятна.

Роль модели OSI при устранении неполадок.

Действовать будем по принципам работы Ethernet технологии основанной на эталонной модели OSI.

Три первых уровня модели OSI определяют функции непосредственно передачи данных. От них зависит физическая доставка сигнала по сети. Последние 4 управляют передачей данных на уровне хост машин.

Уровень 1 – Физический.
Уровень 2 – Канальный.
Уровень 3 – Сетевой.
Уровень 4 – Транспортный.
Уровень 5 — Сеансовый.
Уровень 6 – Уровень представлений.
Уровень 7 — Уровень приложений.

Неполадки со связью чаще всего возникают в среде передачи данных, по этой причине искать неисправности мы будем именно на трех первых уровнях модели OSI.

На физическом уровне могут возникать такие неисправности как отсутствие сигнала в линии по следующим наиболее распространённым причинам:

1. Обрыв кабеля.
2. Плохой контакт в месте подсоединения кабеля.
3. Неправильный задел кабеля в разъем.
4. Не подсоединение кабеля.
5. Подключение кабеля не к тому порту.
6. Отсутствие питания на оборудовании.
7. Замыкание контактов кабеля.
8. Неисправность сетевого интерфейса.

Следующие ошибки и неполадки следует искать на канальном уровне модели OSI:

1. Неверно заданная тактовая частота на последовательных интерфейсах.
2. Неверно заданный номер vlan и тип порта.
4. Не правильное указание метода инкапсуляции.

5. Дублирование arp запросов и ответов.
6. Неисправность сетевого интерфейса.

И наконец, последний, сетевой уровень модели OSI, на котором мы будем искать ошибки и неполадки:

1. Неправильное указание IP сети.
2. Неверный IP адрес сетевого интерфейса.
3. Ошибочное указание маски подсети.
5. Неправильный адрес DNS сервера.
6. Неверная маршрутизация.
7. Задание неправильного номера АС для протокола IGRP.
8. Невыполнение активизации работы протокола маршрутизации.
9. Активизация неверного протокола маршрутизации.

На более высоких уровнях могут случаться ошибки администрирования, приводящие к отказу сети:

1. В случае использования DHCP сервера – ошибка в его конфигурации и указание неверное физического адреса пользователя.
2. Неправильное конфигурирование фаерволов.
3. Нерабочий DNS сервер.

Поиск неисправностей в сети. Утилиты TCP/IP.

Windows XP предоставляет в ваше распоряжение широкий набор утилит для управления, конфигурирования и выявления неисправностей среды TCP/IP.

Ping - диагностическая утилита, которая проверяет возможность соединения с удаленным компьютером.

Pathping - усовершенствованная утилита ping, которая также отражает маршрут прохождения и предоставляет статистику потери пакетов на промежуточных маршрутизаторах.

Route - показывает и позволяет изменять конфигурацию локальной таблицу маршрутизации.

Tracert - отслеживает маршрут, по которому пакеты перемещаются на пути к пункту назначения.

Netstat - показывает текущую информацию сетевого соединения TCP/IP. Например, информацию о подключенном хосте и номера используемых портов.

Ipconfig - показывает текущую конфигурацию TCP/IP на локальном компьютере.

Hostname - показывает локально настроенное имя узла TCP/IP ..

Arp - показывает и позволяет изменять кэш протокола ARP (Address Resolution Protocol), где хранится информация о соответствии IP - адресов - MAC - адресам локальных узлов.

Nslookup - утилита командной строки - распознаватель для запросов DNS сервера.

Утилиты выполняются из командной строки.

Чтобы открыть окно командной строки нажмите кнопку Пуск и выберите последовательно команды Все программы -> Стандартные -> Командная строка.

Если не удается подключиться к другому компьютеру, могут иметь место неполадки с подключением или неполадки с именами.

Применение утилит ping и ipconfig.

Чтобы определить причину неполадок, попытайтесь выполнить обмен пакетами (утилита ping) с IP-адресом другого компьютера. Таким компьютером может быть компьютер, с которым вы пытаетесь соединиться, или основной шлюз.

Чтобы определить IP-адрес основного шлюза: наберите в командной строке ipconfig и нажмите клавишу ENTER. Если требуемая информация уходит с экрана, то для просмотра экранов по очереди введите ipconfig | more и нажмите клавишу ENTER. В отображаемых результатах найдите строку Основной шлюз и запишите соответствующий IP-адрес.

Чтобы выполнить обмен пакетами (ping) с другим компьютером: наберите в командной строке: ping адрес, где адрес представляет IP-адрес другого компьютера, и нажмите клавишу ENTER.
Утилита Ipconfig показывает текущую конфигурацию TCP/IP на локальном компьютере.
Ключи утилиты:
/release - освобождает полученный от DHCP IP - адрес.
/renew - получает от DHCP новый IP - адрес.
/all - показывает всю информацию о TCP/IP конфигурации.
/flushdns - очищает кэш локального распознавателя DNS.
/regsiterdns - обновляет адрес в DHCP и перерегистрирует его в DNS.
/displaydns - показывает Содержание лекционного материалае кэша распознавателя DNS.

Практическое задание:*Финальная комплексная практическая работа по эксплуатации систем IP-телефонии*

Лабораторная работа

1. Цель работы

1.1 Изучить виды соединений в сетях IP-телефонии

1.2 Изучить принципы организации соединений в сетях IP-телефонии

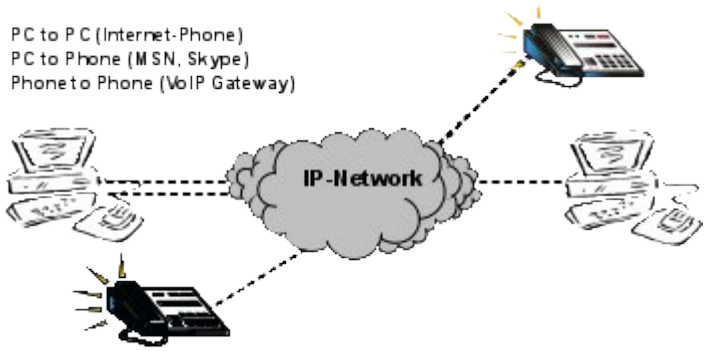
1.2 Освоить принципы построения сетей IP-телефонии

2. Пояснения к работе

2.1 Краткие теоретические сведения

Существует несколько конфигураций IP-телефонии, под каждую из которых существует программное или аппаратное решение.

Можно выделить три наиболее часто используемых сценария IP-телефонии:



Сценарий «компьютер-компьютер» реализуется на базе стандартных компьютеров, оснащенных средствами мультимедиа и подключенных к сети Интернет.

Компоненты сценария «компьютер-компьютер» показаны на рис. 1.8. В этом сценарии аналоговые речевые сигналы от микрофона абонента А преобразуются в цифровую форму с помощью аналого-цифрового преобразователя (АЦП). Отсчеты речевых данных в цифровой форме затем сжимаются кодирующим устройством для сокращения нужной для их передачи полосы в отношении 4:1, 8:1 или 10:1. Выходные данные после сжатия формируются в пакеты, к которым добавляются заголовки протоколов, после чего пакеты передаются через IP-сеть в систему IP-телефонии, обслуживающую абонента Б. Когда пакеты принимаются системой абонента Б, заголовки протокола удаляются, а сжатые речевые данные поступают в устройство, развертывающее их в первоначальную форму, после чего речевые данные снова преобразуются в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) и попадают в телефон абонента Б. Для обычного соединения между двумя абонентами системы IP-телефонии на каждом конце одновременно реализуют как функции передачи, так и функции приема. Под IP-сетью, изображенной на рис. 2.1.2, подразумевается либо глобальная сеть Интернет, либо корпоративная сеть предприятия Intranet[1].

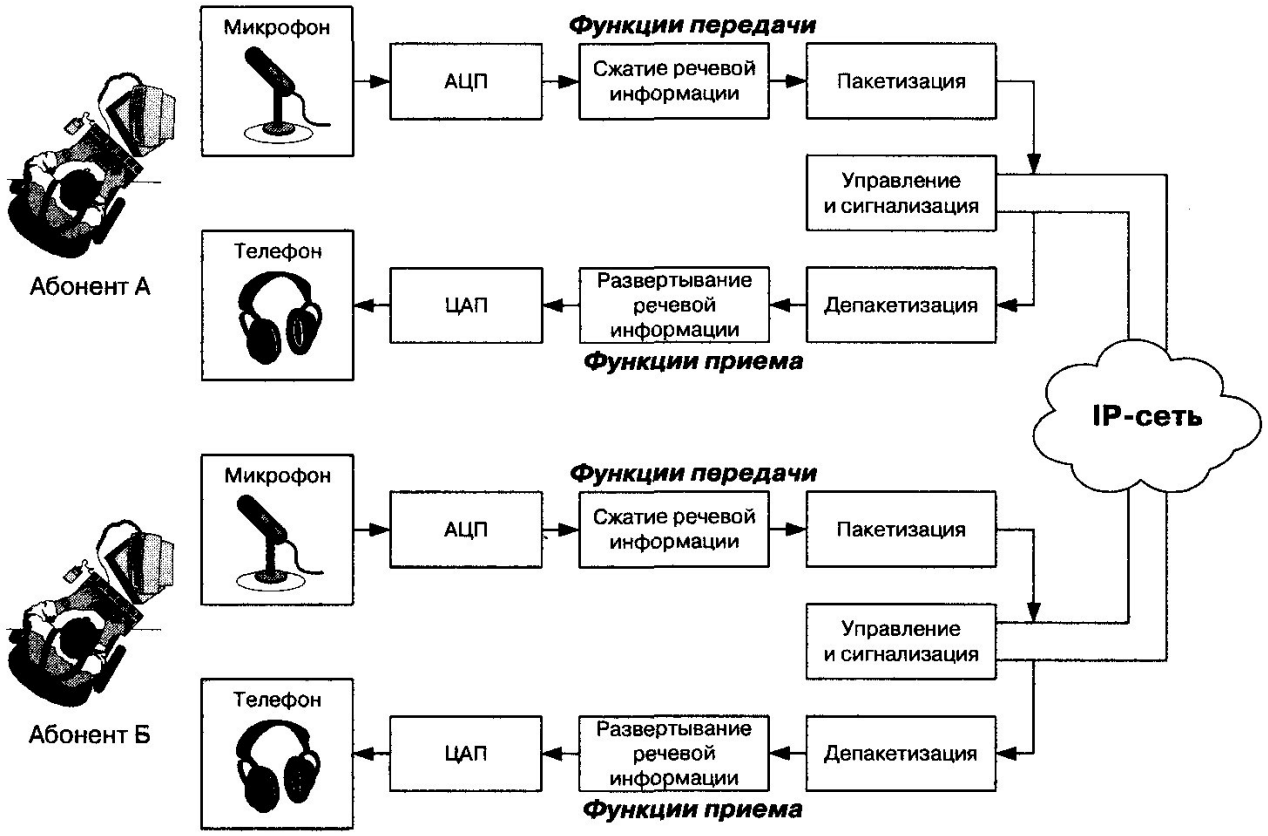


Рисунок 2.1.2 Сценарий IP-телефонии "компьютер-компьютер"

Для поддержки сценария «компьютер - компьютер» поставщику услуг Интернет желательно иметь отдельный сервер (GateKeeper), преобразующий имена пользователей в динамические адреса IP. Сам сценарий ориентирован на пользователя, которому сеть нужна, в основном, для передачи данных, а программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами. Эффективное использование телефонной связи по сценарию «компьютер-компьютер» обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не только видеть документы на Web-сервере, но и обсуждать их Содержание лекционного материалае с помощью IP-телефона. При этом между двумя IP-сетями могут использоваться элементы ТфОП[2], а идентификация вызываемой стороны может осуществляться как на основе E.164[3], так и на основе IP-адресации. Наиболее распространенным программным обеспечением для этих целей является пакет Microsoft NetMeeting, доступный для бесплатной загрузки с узла Microsoft.

Рассмотрим представленный на рис. 1.8 сценарий установления соединения «компьютер-компьютер» более подробно.

Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернет или к другой сети с протоколом IP Рассмотрим возможный алгоритм организации связи между этими абонентами (на примере протокола H.323).

1. Абонент А запускает свое приложение IP-телефонии, поддерживающее протокол H.323.

2. Абонент Б уже заранее запустил свое приложение IP-телефонии, поддерживающее протокол H.323.

3. Абонент А знает доменное имя абонента В элемент системы имен доменов - Domain Name System (DNS), вводит это имя в раздел «кому позвонить» в своем приложении IP-телефонии и нажимает кнопку Return.

4. Приложение IP-телефонии обращается к DNS-серверу (который в данном примере реализован непосредственно в персональном компьютере абонента А) для того, чтобы преобразовать доменное имя абонента Б в IP-адрес.

5. Сервер DNS возвращает IP-адрес абонента Б.

6. Приложение IP-телефонии абонента А получает IP-адрес абонента Б и отправляет ему сигнальное сообщение H.225[4] Setup.

7. При получении сообщения H.225 Setup приложение абонента Б сигнализирует ему о входящем вызове.

8. Абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение H.225 Connect.

9. Приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией H.245[5].

10. После окончания взаимодействия по протоколу H.245 и открытия логических каналов абоненты А и Б могут разговаривать друг с другом через IP-сеть.

В этом примере не показаны некоторые служебные детали, которые необходимы поставщику услуг для развертывания сети IP-телефонии.

При описании других сценариев в этой главе вместо громоздкого изображения компонентов оконечного устройства будет приводится только упрощенное изображение терминала IP-телефонии. Таким аналогом рис. 1.8 является упрощенное представление того же сценария на рис. 2.1.3. К детальному рассмотрению процедур аналогово-цифрового и цифро-аналогового преобразования, сжатия, пакетизации и др. мы вернемся в следующей главе.

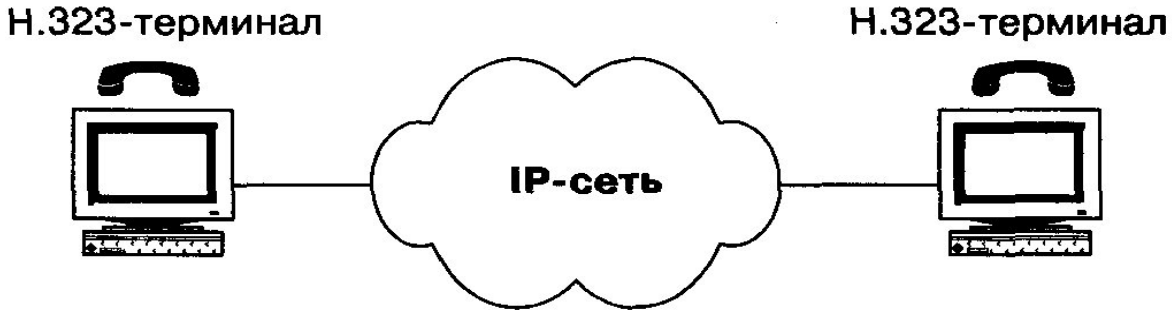


Рис. 2.1.3 Упрощенный сценарий IP-телефонии "компьютер-компьютер"

Замена изображений имеет и более глубокий смысл. Название сценария «компьютер - компьютер» отнюдь не означает, что в распоряжении пользователя обязательно должен быть стандартный PC с микрофоном и колонками, как это представлено на рис. 2.1.2. Главным требованием для такой схемы является то, что оба пользователя должны иметь подключенные к сети персональные компьютеры. И эти PC должны быть всегда включены, подсоединены к сети и иметь в запущенном виде программное обеспечение IP-телефонии для приема входящих вызовов.

Принимая во внимание эти обстоятельства, под названием «компьютер» во всех сценариях мы будем понимать терминал пользователя, включенный в IP-сеть, а под названием «телефон» - терминал пользователя, включенный в сеть коммутации каналов любого типа: ТфОП, ISDN или GSM.

Следующий сценарий - «телефон-компьютер» - находит применение в разного рода справочно-информационных службах Интернет, в службах сбыта товаров или в службах технической поддержки. Пользователь, подключившийся к серверу WWW какой-либо компании, имеет возможность обратиться к оператору справочной службы. Это вполне соответствует стилю жизни современных потребителей, связанному с потребностью в дополнительных удобствах и экономии времени.

Во втором сценарии «компьютер - телефон» соединение устанавливается между пользователем IP-сети и пользователем сети коммутации каналов (рис. 2.1.4). Предполагается, что установление соединения инициирует пользователь IP-сети.

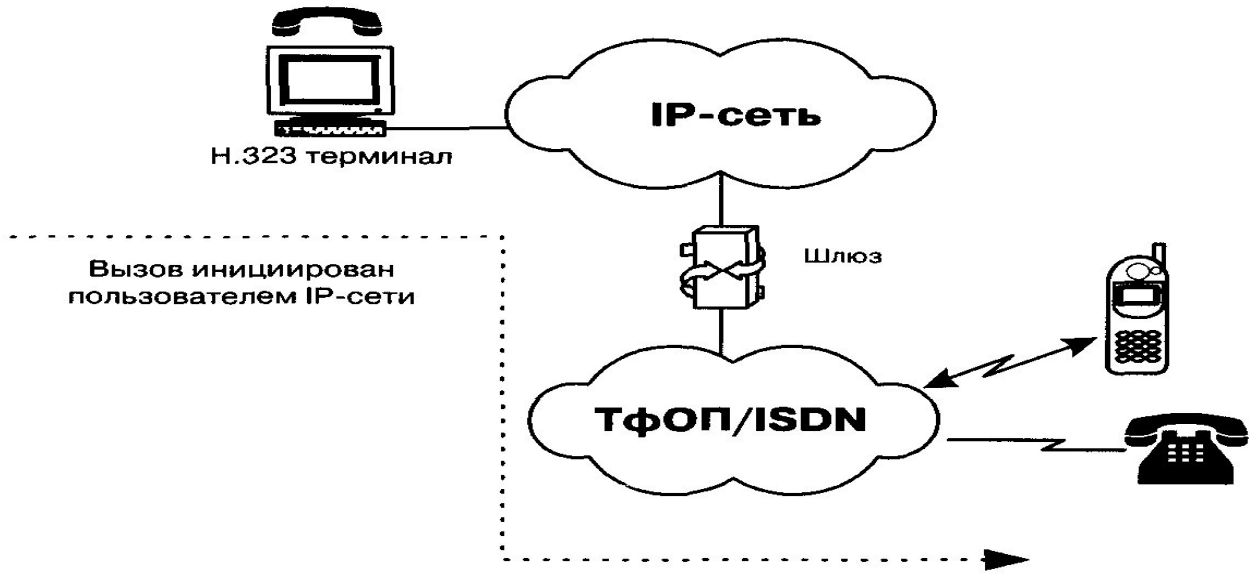


Рисунок 2.1.4 Вызов абонента ТфОП пользователем IP-сети по сценарию "компьютер - телефон"

Шлюз для взаимодействия сетей ТфОП и IP может быть реализован как отдельным устройством, так и интегрирован в существующее оборудование ТфОП или IP-сети. Показанная на рисунке сеть коммутации каналов может быть корпоративной сетью или сетью общего пользования.

Возможна и иная разновидность второго сценария, когда соединение устанавливается между пользователем IP-сети и абонентом ТфОП, но инициирует его создание абонент ТфОП (рис. 2.1.5).

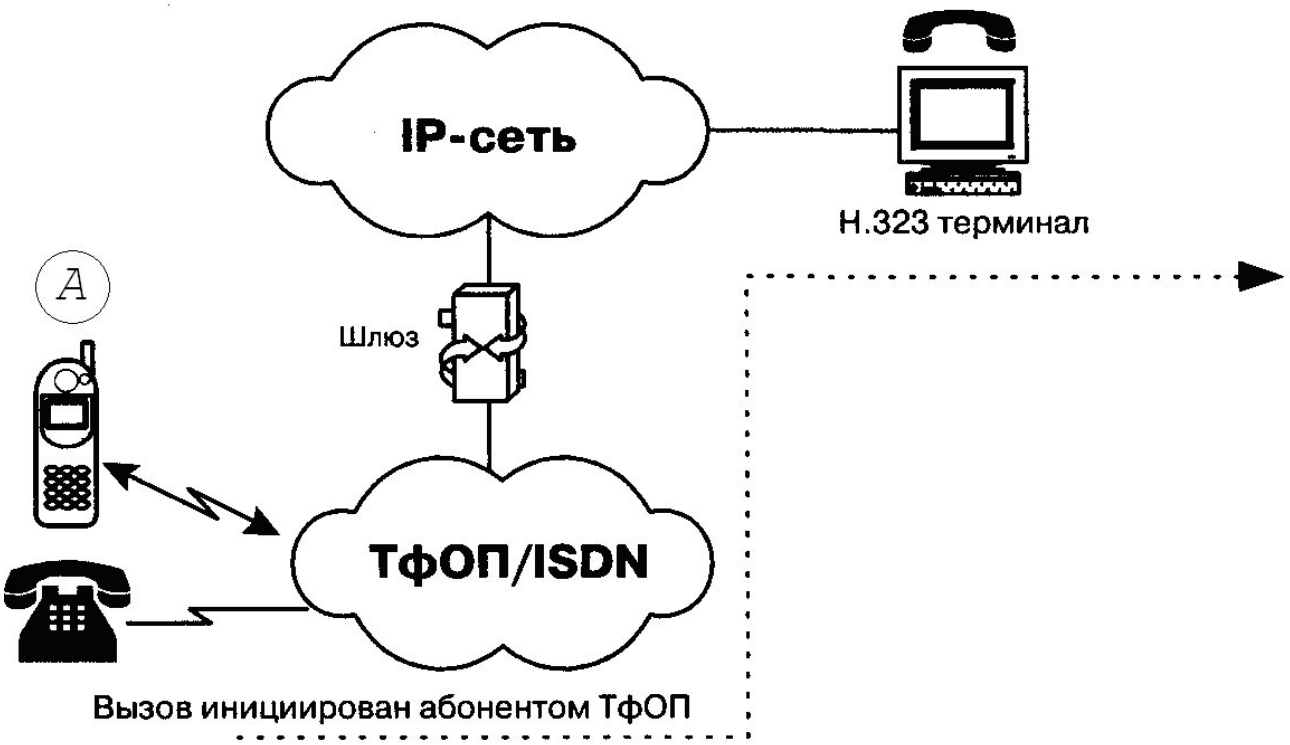


Рисунок 2.1.5 Пользователя IP-сети вызывает абонент ТФОП по сценарию "телефон-компьютер"

Рассмотрим несколько подробнее пример представленной на рис. 2.1.5 упрощенной архитектуры системы IP-телефонии по сценарию «телефон-компьютер». При попытке вызвать справочно-информационную службу, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент А вызывает близлежащий шлюз IP-телефонии. От шлюза к абоненту А поступает запрос ввести номер, к которому

должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если это служба платная. Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции[6]. Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям «компьютер-компьютер» и «компьютер-телефон», не нанося при этом ущерба интересам операторов традиционных телефонных сетей.

Третий сценарий «телефон-телефон» в значительной степени отличается от остальных сценариев IP-телефонии своей социальной значимостью, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной возможности междугородной и международной телефонной связи.

Как правило, обслуживание вызовов по такому сценарию IP-телефонии выглядит следующим образом. Поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу или станции ТфОП и по сети Интернет или по выделенному каналу к аналогичному шлюзу, находящемуся в другом городе или другой стране.

Типичная услуга IP-телефонии по сценарию «телефон-телефон» использует стандартный IP-телефон, а вместо междугороднего компонента ТфОП использует либо частную IP-сеть, либо сеть Интернет. Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования и, соответственно, не платить за междугороднюю/международную связь операторам этих сетей.

Как показано на рис. 2.1.6, поставщики услуг IP-телефонии предоставляют услуги «телефон-телефон» путём установки шлюзов IP-телефонии на входе и выходе IP-сетей. Абоненты подключаются к шлюзу поставщика через ТфОП, набирая специальный номер доступа. Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента (Calling Line Identification). После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному телефону. Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть.

Полная стоимость такой связи будет складываться для пользователя из расценок ТфОП на связь с входным шлюзом, расценок Интернет-провайдера на транспортировку данных и расценок удалённой ТфОП на связь выходного шлюза с вызванным абонентом.

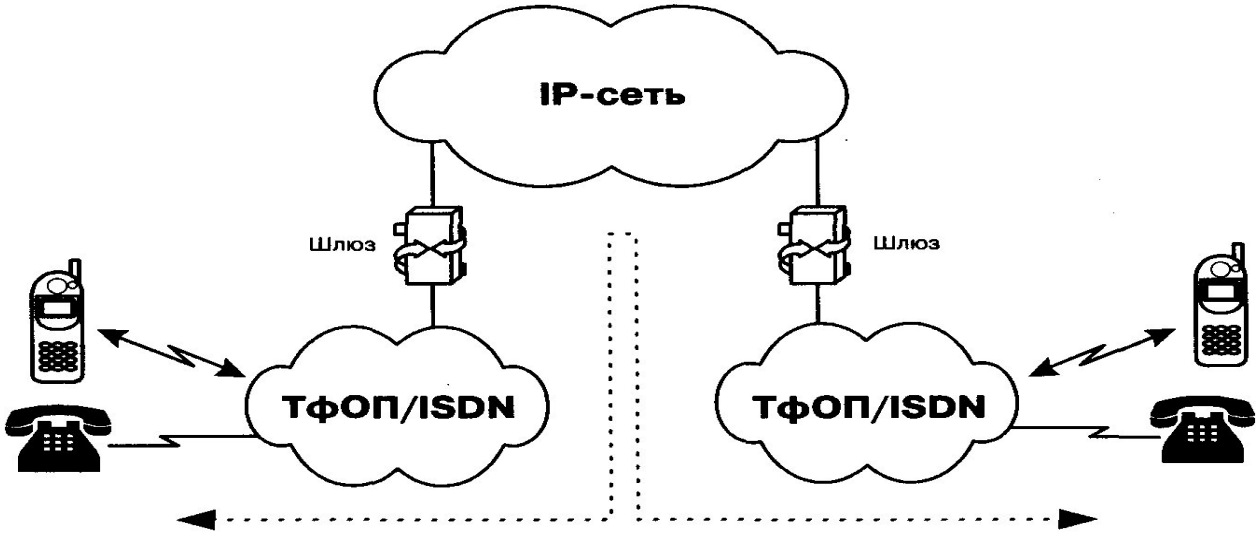


Рисунок 2.1.6 Соединение абонентов ТфОП через транзитную IP-сеть по сценарию "телефон-телефон"

Одним из алгоритмов организации связи по сценарию «телефон-телефон» является выпуск поставщиком услуги своих телефонных карт. Имея такую карту, пользователь, желающий позвонить в другой город, набирает номер поставщика данной услуги, затем в режиме донабора вводит свой идентификационный номер и PIN-код, указанный на карте. После процедуры аутентификации он набирает телефонный номер адресата.

3. Задание

3.1 Ознакомиться с видами соединений

3.2 Зарисовать схемы организации связи

3.3 Ответить на контрольные вопросы

4. Содержание лекционного материалае отчета:

1. Цель работы.
2. Схемы связи
3. Ответы на контрольные вопросы
4. Вывод о применении схем IP телефонии

Контрольные вопросы:

1. Как работает схема IP-телефонии «компьютер-телефон»?
2. Какое терминальное оборудование используется в схеме связи «компьютер-компьютер»?
3. Как АЦП и ЦАП влияют на связь в процессе разговора между абонентами?
4. Для чего предназначен H.323 терминал?
5. Что такое ТФОП?
6. Что определяет формат E.164?
7. Какие услуги связи организуются при подключении абонентом IP-телефонии?
8. Для чего предназначен шлюз?
9. Что такое VoIP?
10. Какую функцию выполняет протокол H.245?

Контрольные вопросы по итогам курса

1. Дайте определение термину «техническое обслуживание (ТО)».
2. Перечислите основные методы ТО.
3. Опишите статистический метод ТОсетевых объектов.
4. Дайте определение термину «техническое обслуживание (ТО)».
5. Перечислите основные методы ТО. Опишите профилактический метод ТО
6. оборудования.
7. Перечислите основные группы задач систем управления сетями.
8. Опишитезадачи,выполняемыефункциональнойгруппойуправленияконфигурацией сети
9. Перечислите основные группы задач систем управления сетями.
10. Опишите задачи, выполняемые функциональной группой обработки ошибок.
11. Перечислите основные группы задач систем управления сетями.
12. Опишитезадачи,выполняемыефункциональнойгруппойанализапроизводительности и надёжности.
13. Перечислите основные группы задач систем управления сетями.
14. Опишитезадачи,выполняемыефункциональнойгруппойуправлениябезопасностью.
15. Перечислите этапы контроля функционирования ЛВС. Опишитегруппы средств мониторинга и анализа сети.
16. Перечислите задачи, решаемые анализаторами сетевых протоколов.
17. Опишите принцип его работы и состав.
18. Проанализируйте общие свойства анализаторов протоколов.

19. Перечислите виды анализаторов протоколов. Опишите принцип
20. работы программных анализаторов протоколов.
21. Назовитеособенностипримененияпрограммныханализаторовпротоколов при использовании в сети коммутаторов.
22. Перечислите виды анализаторов протоколов. Опишите принципработы аппаратных анализаторов протоколов.
23. Сделайте вывод о необходимости применения экспертных систем длядиагностики неисправностей на узлах ЛВС. Перечислите подсистемысредств мониторинга и анализа сетей, используемые для реализацииэкспертных систем.
24. Дайтехарактеристикуэкспертнойсистемедлядиагностикинеисправностей на узлах ЛВС как системе искусственного интеллекта.
25. Перечислите категории диагностической информации, предоставляемой
26. системой экспертного анализа администратору сети.
27. Опишите задачи, выполняемые типовой экспертной системой (ЭС)диагностики причин аномальной работы сетей.
28. Перечислите ограниченияпростейших ЭС. Приведите классификацию ЭС.
29. Изложите по структурной схеме принцип работы экспертной системы(ЭС) анализа причин аномальной работы для решения сложных
    задачаглобальногопоисканаилучшего
30. решениясредимножестварешений.Опишите процесс рассуждения ЭС.
31. Опишитестандартныйинтернет-протоколдляуправленияустройствами в IP-сетях SNMP (SimpleNetworkManagementProtocol).
32. Объясните схему взаимодействия Менеджер-SNMP-Агент.
33. Сформулируйте назначение протокола удалённого мониторингаRMON. Опишите виды и назначение зондов RMON.
34. Сформулируйте особенности мониторинга коммутируемых сетей
35. Перечислитезадачи,предусмотренные планомфункционирования системы.
36. Опишите мероприятия по выполнению Плана на разных этапах.
37. Опишите допущения и посылки, применяемые при разработке Плана
38. восстановления функционирования системы.
39. Изложите структуру проекта планирования восстановления данных.
40. Опишите группы задач, выполняемых при восстановлении данных.
41. Сформулируйте задачи, выполняемые при проведении мероприятий по
42. восстановлению данных после сбоя.

ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Вопросы для подготовки к экзамену

1. Дайте определения терминам «телекоммуникация», «сигнал».
2. Опишите работу системы телекоммуникации (СТК) по структурной схеме.
3. Назовите назначение и составные части первичной и вторичной сетейсети страны РФ.
4. Опишите структуру Федеральной сети Российской Федерации, назначение ее элементов.
5. Перечислитекомплекс работ по развёртываниюфизическойинфраструктуры сетей.
6. Назовите этапы развёртывания сетевой инфраструктуры предприятия.
7. Перечислите групповые роли и задачи персонала на этапе разработкиновой компьютерной системы.
8. Опишите действия, которые необходимо выполнить до развёртыванияцелевой операционной системы на целевом компьютере
9. Перечислите мероприятия, проводимые в процессе техническойэксплуатации(ТЭ)ЛВС
10. и рекомендуемыеметодытехническогообслуживания объектов ТЭ:
11. Перечислите виды отказов объектов технической эксплуатации идайте их краткую характеристику
12. Назовите виды управляемого технического обслуживания сети.
13. Рассмотрите особенности непрерывного эксплуатационного контроля.
14. Перечислите заключения о работоспособности объекта, выносимые порезультатам оперативно-технического контроля состояния сети.
15. Дайте определения терминам «Маршрутизатор», «Маршрутизация».
16. Перечислите основные действия маршрутизатора, выполняемые им дляреализации своих функций.
17. Перечислитегруппыметодовдоступакомпьютеровксети.
18. Рассмотрите подробней методы случайного доступа к сети.
19. Опишите методы коммутации в телекоммуникационных сетях (ТКС).
20. Перечислите основные технологии масштабирования. Опишитетехнологию нивелирования времени ожидания связи
21. Перечислите основные технологии масштабирования. Опишитетехнологию распределения.
22. Объясните порядок работ при проектировании ЛВС, перечислитеруководящие документы, регламентирующие данный вид работ, составпроектной документации ЛВС (стадия «П»).
23. Перечислите состав и краткое Содержание лекционного материалае рабочей документации припроектировании ЛВС (стадия «Р»), их соответствие различным этапам работ.
24. Дайте определение термину «техническое обслуживание (ТО)».
25. Перечислите основные методы ТО. Опишите статистический метод ТОсетевых объектов.
26. Опишите способы и системы переключения на резерв для кабельных,
27. волноводных и радиорелейных линий связи, а также виды переключений,
28. применяемые на практике.
29. Опишите способы увеличения надёжности кабельной системы и сети
30. Перечислите способы резервирования систем оптической связи.
31. Опишите способ линейного резервирования.
32. Перечислите способы резервирования систем оптической связи.
33. Опишите способ системного резервирования.
34. Перечислите группы мероприятий по техническому обслуживанию
35. (ТО) технических компонентов ЛВС, мероприятия, проводимые при ТО
36. существующей ЛВС.

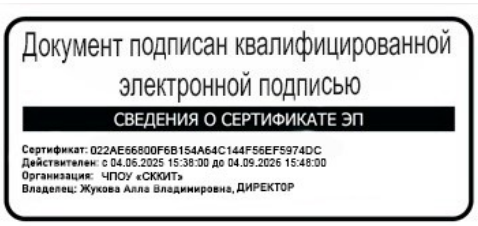
37. Перечислите основные этапы при проведении аудита ЛВС, переченьработ по техническому обслуживанию ЛВС.
38. Опишите функции, выполняемые системой управления компьютерами
39. и их системным и прикладным ПО (System Management System).
40. Перечислите функциональные группы системы управления сетями
41. IBM, ориентированных на пользователя. Опишите функцию управления
42. конфигурацией
43. Опишите протоколы, разработанные для управления ЛВС.
44. Дайте характеристику методам, позволяющим уменьшить рискполной утраты работоспособности системы.
45. Сформулируйте задачи управления безопасностью сети. Перечислитеуровни, на которых осуществляется обеспечение безопасности данных.
46. Приведите классификацию инструментов защиты по типу механизмаслежения.

Перечень практических заданий к другим формам контроля

1. Создать пользователя USER1 в domain при помощи оснастки «Active Directory– пользователи и компьютеры»
2. Создать пользователя USER1 в domain на основании шаблонов.
3. Создать пользователей средствами командной строки
4. Создать пароль для входа пользователю USER1 в domain
5. Создать группы BUH1 и BUH2 в domain при помощи оснастки «Active
6. Directory– пользователи и компьютеры»
7. Создать группы BUH1 и BUH2 средствами командной строки
8. Создать группы BUH1 и BUH2 и распределить пользователей USER1 и USER12 по группам в domain соответственно.
9. Выполнить установку WinRoute
10. Выполнить базовую настройку политики трафика в WinRoute
11. Выполнить настройку DHCP-сервера в WinRoute
12. Выполнить настройку DNS Форвардера в WinRoute
13. Выполнить установку CommView Remote Agent и продемонстрировать возможности наблюдения трафика сети.
14. Построить схему сети с использованием программы 10-Strike LANState

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрена и утверждена
на Педагогическом совете
от 19.03.2026 Протокол №
03



УТВЕРЖДАЮ
Директор ЧПОУ
«СККИТ»
А.В. Жукова
«19» марта 2026

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Пятигорск – 2026

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ВИДОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Рекомендации по подготовке к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Рекомендации по подготовке к практическим занятиям

При подготовке к практическому занятию студент должен ознакомиться с планом, выполнить все инструкции, предложенные преподавателем.

Результатом работы является свободное владение теоретическим материалом, полные ответы на поставленные вопросы, коллективное обсуждение проблемных тем.

Методические рекомендации по подготовке докладов

Доклад – публичное сообщение, представляющее собой развернутое изложение на определенную тему.

Различают следующие виды докладов: научный доклад и учебный доклад. Научные доклады готовятся научными работниками для представления своих результатов на научной конференции, научном семинаре и др. К учебным докладам относятся студенческие доклады и любые другие доклады, подготавливаемые обучающимися средних образовательных учреждений.

Для того, чтобы облегчить работу над докладом, предлагаем разбить процесс на несколько последовательных этапов. Надеемся, что знакомство с ними поможет вам овладеть необходимым инструментарием и разобраться в принципах построения письменной работы.

Этапы подготовки доклада

1. Подготовка и планирование.
2. Выбор и осознание темы доклада
3. Подбор источников и литературы.
4. Работа с выбранными источниками и литературой.
5. Систематизация и анализ материала.
6. Составление рабочего плана доклада.
7. Письменное изложение материала по параграфам.
8. Редактирование, переработка текста.
9. Оформление доклада.
10. Выступление с докладом.

При подготовке доклада рекомендуется придерживаться следующих правил:

Во-первых, необходимо четко соблюдать регламент.

Для того чтобы уложиться в отведенное время необходимо:

а) тщательно отобрать факты и примеры, исключить из текста выступления все, не относящееся напрямую к теме;

б) исключить все повторы;

в) весь иллюстративный материал (графики, диаграммы, таблицы, схемы) должен быть подготовлен заранее;

г) необходимо заранее проговорить вслух текст выступления, зафиксировав время и сделав поправку на волнение, которое неизбежно увеличивает время выступления перед аудиторией.

Во-вторых, доклад должен хорошо восприниматься на слух.

Это предполагает:

а) краткость, т.е. исключение из текста слов и словосочетаний, не несущих смысловой нагрузки;

б) смысловую точность, т.е. отсутствие возможности двоякого толкования тех или иных фраз;

в) отказ от неоправданного использования иностранных слов и сложных грамматических конструкций.

Доклады оцениваются по следующим критериям:

- соблюдение требований к его оформлению;
- необходимость и достаточность информации для раскрытия темы;
- умение обучающегося свободно излагать основные идеи, отраженные в докладе;
- способность учащегося понять суть задаваемых ему вопросов и сформулировать точные ответы на них.

Методические рекомендации по подготовке конспектов

При подготовке конспекта рекомендуется придерживаться такой последовательности:

1.Прочтите текст.

2.Определите цель изучения темы (какие знания должны приобрести и какими умениями обладать).

3.Выделите основные положения.

4.Проанализируйте основные положения.

5.Сделайте выводы.

6.Составьте краткую запись.

Работа с литературными источниками

В процессе обучения студенту необходимо самостоятельно изучать учебно-методическую литературу. Самостоятельно работать с учебниками, учебными пособиями, Интернет-ресурсами. Это позволяет активизировать процесс овладения информацией, способствует глубокому усвоению изучаемого материала.

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Различают два вида чтения; первичное и вторичное. Первичное - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного слова. Содержание не всегда может быть понятно после первичного чтения.

Задача вторичного чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания.

При работе с литературой рекомендуется вести записи.

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Промежуточная аттестация

Каждый семестр заканчивается сдачей зачетов (экзаменов). Подготовка к сдаче зачетов (экзаменов) является также самостоятельной работой студентов. Студенту необходимо к зачету (экзамену) повторить весь пройденный материал по дисциплине в рамках лекций и рекомендуемой литературы.

Методические рекомендации по работе с Интернет-ресурсами

Среди Интернет-ресурсов, наиболее часто используемых студентами в самостоятельной работе, следует отметить электронные библиотеки, образовательные порталы, тематические сайты, библиографические базы данных, сайты периодических изданий. Для эффективного поиска в WWW студент должен уметь и знать:

- чётко определять свои информационные потребности, необходимую ретроспективу информации, круг поисковых серверов, более качественно индексирующих нужную информацию,
- правильно формулировать критерии поиска;
- определять и разделять размещённую в сети Интернет информацию на три основные группы: справочная (электронные библиотеки и энциклопедии), научная (тексты книг, материалы газет и журналов) и учебная (методические разработки, рефераты);
-давать оценку качества представленной информации, отделить действительно важные сведения от информационного шума;
- давать оценки достоверности информации на основе различных признаков, по внешнему виду сайта, характеру подачи информации, её организации;
- студентам необходимо уметь её анализировать, определять её внутреннюю непротиворечивость.

Запрещена передача другим пользователям информации, представляющей коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайны, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.

При работе с Интернет-ресурсами обращайте внимание на источник: оригинальный авторский материал, реферативное сообщение по материалам других публикаций, студенческая учебная работа (реферат, курсовая, дипломная и др.). Оригинальные авторские материалы, как правило, публикуются на специализированных тематических сайтах или в библиотеках, у них указывается автор, его данные. Выполнены такие работы последовательно в научном или научно-популярном стиле. Это могут быть научные статьи, тезисы, учебники, монографии, диссертации, тексты лекций. На основе таких работ на некоторых сайтах размещаются рефераты или обзоры. Обычно они не имеют автора, редко указываются источники реферирования. Сами сайты посвящены разнообразной тематике. К таким работам стоит относиться критически, как и к сайтам, где размещаются учебные студенческие работы. Качество этих работ очень низкое, поэтому, сначала подумайте, оцените ресурс, а уже потом им пользуйтесь. В остальном с Интернет-ресурсами можно работать как с обычной печатной литературой. Интернет – это ещё и огромная библиотека, где вы можете найти практически любой художественный текст. В интернете огромное количество словарей и энциклопедий, использование которых приветствуется.