

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УДМУРТСКОЙ РЕСПУБЛИКИ

**Автономное профессиональное образовательное учреждение
Удмуртской Республики
«Техникум радиоэлектроники и информационных технологий
имени Александра Васильевича Воскресенского»**

**Практические работы
по МДК 02.01 Монтаж и обслуживание инфокоммуникационных систем с
коммутацией пакетов и каналов**

**специальность 11.02.15 Инфокоммуникационные сети и системы связи
квалификации выпускника – специалист по обслуживанию телекоммуникаций
Форма обучения - очная**

Разработал
преподаватель:

Л.И. Лихачёва

2024 г.

Практическая работа 1

Тема: Исследование работы пространственного коммутатора цифровых каналов

Цель работы: Изучить принципы построения и работы пространственных коммутаторов цифровых каналов.

Практические навыки:

- изображения схемы пространственного коммутатора с указанием всех параметров (номеров используемых мультиплексоров И демультиплексоров, номеров их входов/выходов, номеров и содержимого ячеек памяти);
- расчета числа и характеристик мультиплексоров/демультиплексоров, характеристик управляемой памяти каждого мультиплексора/демультиплексора;
- описания реализации двухсторонней связи в пространственном коммутаторе.

Продолжительность занятия – 2 ч.

Ход работы:

Схематически простейшую коммутационную структуру, реализующую пространственную коммутацию каналов, можно представить в виде прямоугольной решетки, составленной из точек коммутации, разнесенных между собой в пространстве (рис.1).

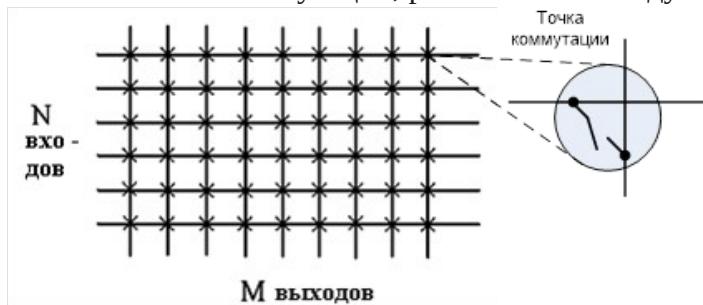


Рис. 1 - Прямоугольная полнодоступная коммутационная схема (коммутатор)

Если к входам и выходам подсоединенны двухпроводные цепи, то на каждое соединение требуется только одна точка коммутации (вторым проводом является общая точка – положительный полюс электропитающей установки узла коммутации). Коммутационные системы для четырехпроводных цепей (цифровая коммутация каналов) требуют установления раздельных соединений — для прямой и обратной ветви цепи передачи.

Пространственная коммутация цифровых каналов (канальных интервалов - КИ) трактов ИКМ заключается в том, что информация переносится из одного тракта ИКМ в другой без изменения временного положения КИ. Это проиллюстрировано примером, показанным на рис. 2, где информация КИ 5 переносится из тракта 1 во второй тракт в то же временное положение. На этом же рисунке показано второе пространственное соединение 2-го тракта с первым для КИ 2



Рис. 2 – Работа пространственного коммутатора цифровых каналов

Пространственный коммутатор (ПК) предназначен для синфазной коммутации каналов определенных входящей и исходящей ИКМ- линий в одном и том же КИ, поэтому он не требует включения в тракт запоминающих устройств (ЗУ).

Рассмотрим пространственный коммутатор на N-входов и M-выходов. Во входы включены соответственно N цифровых линий ИКМ, в выходы - M цифровых линий, каждая ИКМ-линия имеет n-временных каналов (КИ). Такой коммутатор имеет $N \times M$ пространственных точек коммутации, которые могут быть реализованы на мультиплексорах или демультиплексорах.

Мультиплексор (MUX) – это цифровое комбинационное устройство без элементов памяти, у которого имеется несколько входов, информация из которых передается на один выход в соответствии с управляющей (адресной) информацией. На рис 3 показан MUX на 8 входов ($X_0 \div X_7$), он имеет 3 адресных входа ($A_0 \div A_2$).

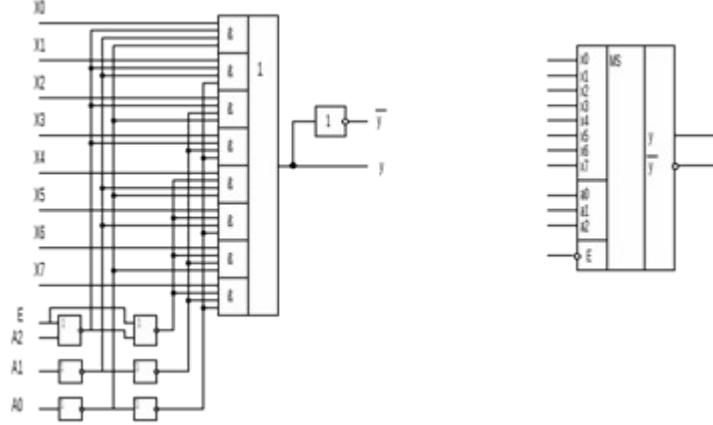


Рис. 3 - Мультиплексор на 8 входов: логическая схема и обозначение

Демультиплексор (DMX) – в отличие от мультиплексора наоборот имеет один вход и несколько выходов, информация на один из них передается с входа в соответствии с управляющей (адресной) информацией (рис. 4).

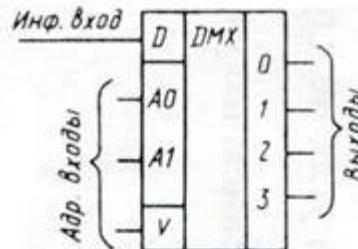


Рис. 4 – Демультиплексор на 4 выхода

На рис. 5 представлена структурная схема ПК 8x16, реализованная на мультиплексорах.

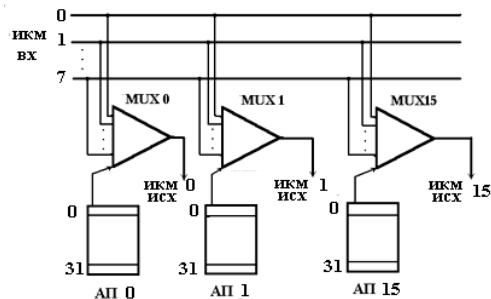


Рис. 5 - Схема пространственного коммутатора 8x16 на мультиплексорах

Такой ПК управляет по входу. Схема имеет 16 мультиплексоров, у которых соответствующие входы запараллелены. С каждым мультиплексором связана своя адресная память (АП), информацию в ячейки которой записывает устройство управления (УУ). Содержимое ячеек АП указывает на то, какой из 8-ми входов мультиплексора должен быть подключен на выход в момент времени (КИ), номер которого совпадает с номером ячейки АП.

Разрядность каждой ячейки АП равна 3 (определяется по формуле адресной памяти, соответствующей требуемому канальному интервалу (КИ), $\log_2 N$, где N – число входящих цифровых линий ИКМ). В одну из этих 32-х ячеек адресной памяти, соответствующей требуемому канальному интервалу (КИ),

УУ предварительно записывает адрес входа (ИКМвх.), который должен быть подключен к заданному выходу (номер выхода определяется номером мультиплексора).

Когда на ПК поступает информация в КИ с номером N, из ячейки адресной памяти с номером мультиплексора информация должна быть проключена на его выход.

Пространственный коммутатор может управляться и по выходу. В этом случае для реализации точек коммутации в ПК используются демультиплексоры (DMX), число которых равно числу входящих цифровых линий и у них одноименные выходы запараллелены (рис. 6). Управляющая информация, поступающая из адресной памяти, определяет, на какой выход демультиплексора должна быть проключена информация с его входа в момент времени, соответствующий номеру КИ входящей цифровой линии и совпадающий с номером ячейки АП. Разрядность ячеек АП демультиплексоров определяется по формуле использования цифровых линий ИКМ-30/32 число ячеек АП равно 32 по числу КИ в тракте.

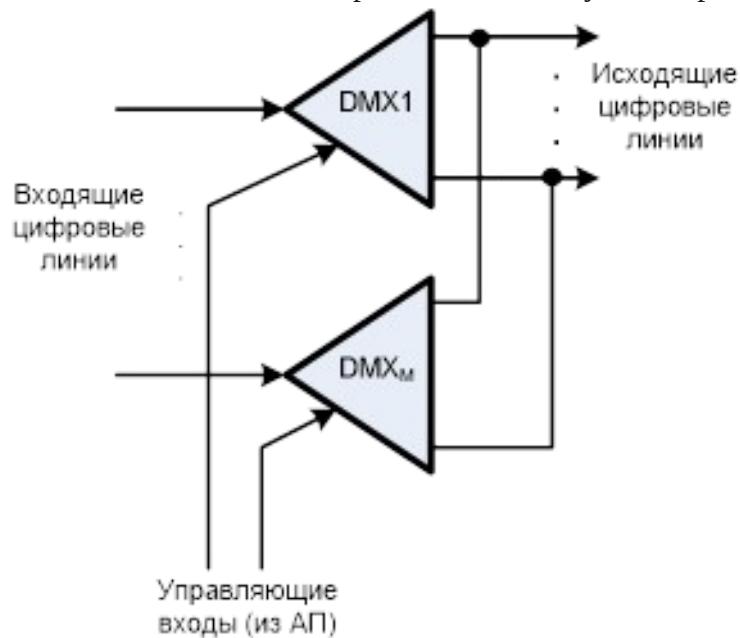


Рис. 6 - Схема пространственного коммутатора на демультиплексорах

В пространственном коммутаторе имеется возможность коммутировать только одноименные (синфазные) каналы. По этой причине коммутационные поля, построенные только на базе ПК, не получили на практике широкого применения.

Задание на выполнение практической работы

В пространственном коммутаторе, имеющем 16 входящих и 16 исходящих цифровых линий ИКМ-30/32, выполнить коммутацию двухстороннего разговорного соединения.

Номера входящей и исходящей ИКМ-линий и номер входящего канального интервала (КИ) приведены в табл. 1 (номер варианта соответствует номеру студента в списке группы).

Требуется:

1. Изобразить схему пространственного коммутатора с указанием используемых при коммутации мультиплексоров/демультиплексоров, номера ячеек управляющей памяти и их содержимого при коммутации разговорного соединения.

2. Определить требуемое число и характеристики мультиплексоров/ демультиплексоров, характеристики управляющей памяти мультиплексоров/ демультиплексоров.

3. Указать особенности реализации двухсторонней связи в пространственном коммутаторе.

Таблица 1 Варианты исходных данных для задания

№ варианта	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Входящая ИКМлиния	3	11	15	0	4	11	4	5	6	10	9	12	13	14	2	7	11	3	8	10	1	9	4	7	12
Входящий КИ	15	7	4	21	19	30	11	25	0	31	29	5	18	27	10	26	9	14	29	7	3	1	12	2	24
Исходящая ИКМлиния	12	8	9	14	6	5	12	2	13	8	7	1	0	12	6	4	10	7	13	4	6	15	11	10	1
Реализация ПК	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М

Примечание: М – мультиплексор, Д – демультиплексор. Нумерация ИКМ-линий и КИ в них начинается с нуля!

Содержание отчета

По заданию 1:

1. Схема пространственного коммутатора с указанием всех параметров (номеров используемых мультиплексоров/демультиплексоров, номеров их входов/выходов, номеров и содержимого ячеек памяти).
2. Расчет числа и характеристик мультиплексоров/ демультиплексоров, характеристик адресной памяти каждого мультиплексора/демультиплексора.
3. Описание реализации двухсторонней связи в пространственном коммутаторе.

Контрольные вопросы

1. Какие временные каналы можно коммутировать в пространственном коммутаторе?
2. Какой основной недостаток имеет пространственная коммутация цифровых каналов?
3. Какие логические элементы используются в пространственных коммутаторах цифровых сигналов?
4. Сколько мультиплексоров в пространственном коммутаторе на 14 входящих и 18 исходящих ИКМ-линий?
5. Сколько входов у мультиплексоров пространственного коммутатора на 8 входящих и 12 исходящих ИКМ-линий?
6. Сколько ячеек памяти в адресных ЗУ пространственного коммутатора на 16 входящих и 8 исходящих ИКМ-линий?
7. Какова разрядность адресного ЗУ пространственного коммутатора на 16 входящих и 32 исходящих ИКМ-линий?
8. Какой мультиплексор используется в пространственном коммутаторе при коммутации 14 входящей ИКМ-линии с 5 исходящей линией?
9. Какой вход мультиплексора используется в пространственном коммутаторе при коммутации 5 входящей с 16 исходящей ИКМлинией?
10. Какая информация записывается в ячейках адресного ЗУ мультиплексоров пространственного коммутатора?
11. Каков основной недостаток имеет временная коммутация цифровых каналов?
12. На каких элементах строятся временные коммутаторы?
13. Возможна ли временная коммутация канального интервала 29 с канальным интервалом 17?
14. Какова будет временная задержка при коммутации канального интервала 14 КИ с канальным интервалом 6?
15. Какова будет временная задержка при коммутации канального интервала 11 с канальным интервалом 31?
16. Из чего состоит временной коммутатор?
17. Какова разрядность разговорной памяти временного коммутатора?

18. Какова разрядность адресной памяти временного коммутатора на одну цифровую линию ИКМ-30?
19. Какая информация записывается в ячейки адресной памяти временного коммутатора?
20. Сколько ячеек содержит адресная память временного коммутатора на одну цифровую линию ИКМ-30?
21. В чем отличие разных способов управления работой РЗУ?

Практическая работа 2

Тема: Исследование работы временного коммутатора цифровых каналов

Цель работы: Изучить принципы построения и работы временных коммутаторов цифровых каналов.

Практические навыки:

- изображения схемы временного коммутатора с указанием всех параметров (номеров и содержимого ячеек памяти);
 - описания процесса работы схемы при установлении соединения с указанием параметров работы схемы для реализации коммутации обратного направления.
 - расчета временной задержки информации при коммутации на передачу и на прием.
- Продолжительность занятия – 2 ч.

Ход работы:

Блок или модуль, осуществляющий функцию временной коммутации цифрового сигнала (преобразование его временной координаты), называется временным коммутатором (ВК). Пусть на вход ВК включена входящий цифровая линия ИКМвх1, а с выхода ВК уходит исходящая ИКМисх2 (рис. 1). За каждым временным интервалом закреплен строго определенный канальный интервал цифровой линии ИКМ (например, речевой сигнал абонента).

Пусть абонент А закреплен за канальным интервалом i входящей ИКМ-линии, а абонент В за канальным интервалом j исходящей ИКМ-линии. Изменение порядка следования одного канального интервала исходящей ИКМ-линии по сравнению с входящей означает передачу речевой информации от одного абонента к другому. В этом и заключается принцип временной коммутации (иногда говорят о перестановке канальных интервалов или перемещении информации из канала в канал).

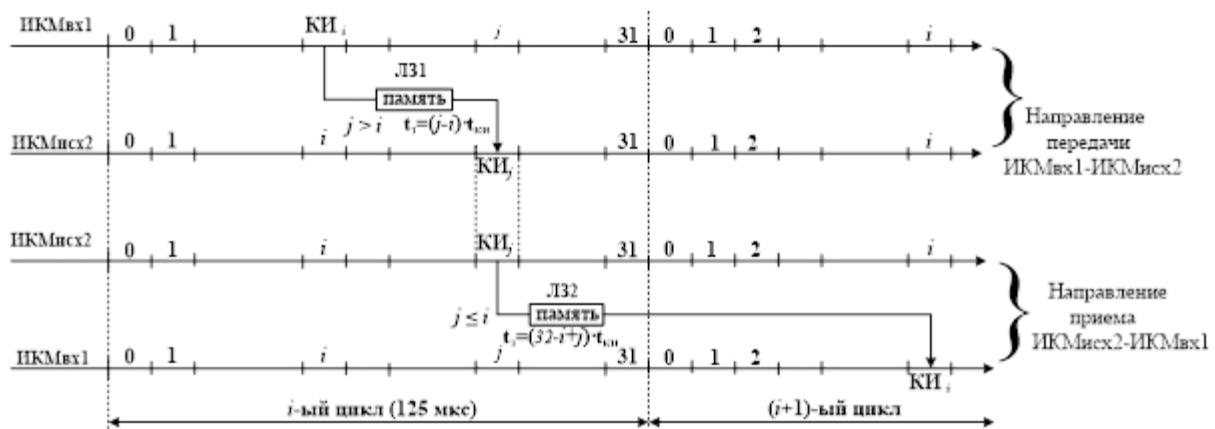


Рис. 7 – Принцип временной коммутации

Операция временной коммутации фактически является просто операцией задержки определенного кодового слова временного канала (информации определенного КИ) на заданное время τ , которое определяется разностью номеров КИ на входе (N_i) и на выходе (N_j) и длительностью одного КИ T_{ki} (для цифрового тракта ИКМ-30/32 она равна 3,9 мкс):

$$\tau = (Nj - Ni) \times T_{ki}, \text{ при условии } j > i, \tau = (32 + Nj - Ni) \times T_{ki}, \text{ при условии } j \leq i.$$

Примечание: во втором случае при $j \leq i$ информация из входного КИ i передается в выходной КИ j следующего цикла ИКМ, отсюда максимальная задержка во ВК будет при коммутации одноименных КИ на входе и выходе ($Nj = Ni$) и она равна длительности цикла ИКМ $32 \times T_{ki} = 125$ мкс.

Для осуществления двухстороннего (дуплексного) разговора абонентов необходимо, чтобы тракт был четырехпроводным. Поскольку электронная коммутация имеет односторонний характер (в силу того, что электронные компоненты имеют только одно направление передачи информации), то временная коммутация, как правило, осуществляется не только прямая (i -й канал с j -м каналом), но и обратная (j -й канал с i -м).

Реализация временной коммутации

Для того чтобы обеспечить желаемую временную коммутацию каналов, звенья временной коммутации принципиально требуют наличия некоторого вида элементов задержки. Задержки легче всего реализовать с помощью запоминающего устройства (ЗУ) с произвольной выборкой (оперативное ЗУ – ОЗУ или RAM), запись в которые производится по мере поступления данных, а считывание при необходимости их передачи. Если для каждого канального интервала (КИ) в цикле ИКМ отведена одна ячейка памяти, то информация каждого канала с временным разделением может храниться без искажения повторной записью в течение времени вплоть до длительности одного полного цикла.

Рассмотрим схему работы временного коммутатора (ВК) (рис. 8). Последовательный цифровой поток ИКМ поступает на вход схемы ВК, которая преобразует информацию из последовательной формы в параллельную. Далее эта информация записывается в речевое (информационное) запоминающее устройство (РЗУ). Адрес записи устанавливается счетчиком временных каналов, который генерирует последовательно номера КИ в цикле ИКМ. Поэтому информация располагается в РЗУ по мере возрастания номера временного канала (КИ).

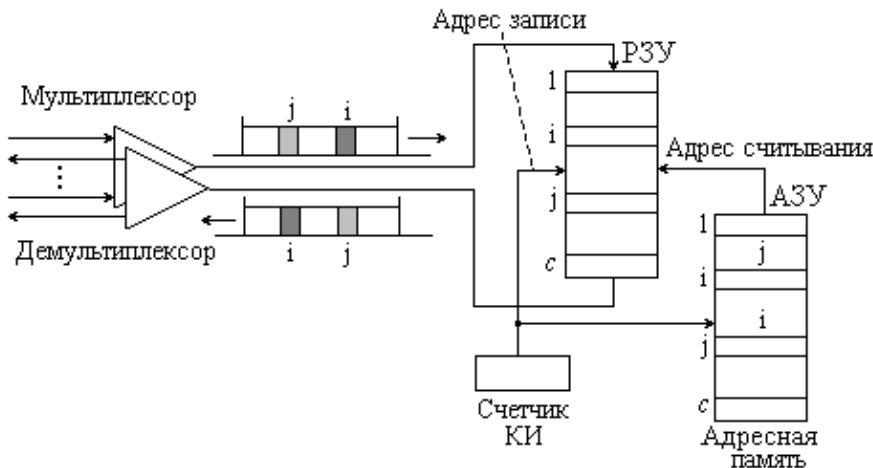


Рис. 8 - Структурная схема временного коммутатора

Считывание этой информации в исходящий тракт производится в соответствии с информацией, записанной в адресном запоминающем устройстве (АЗУ). Опрос этой памяти также производится по тактовым импульсам, приходящим от счетчика временных каналов. Каждый такт соответствует номеру КИ в исходящем цифровом тракте.

На рис. 8 адрес входящего канала i записан в адресной памяти на месте КИ j . И наоборот, адрес входящего канала j записан в адресной памяти на месте КИ i . Это означает, что при чтении из адресной памяти во время КИ j на вход РЗУ поступит адрес i . В результате в этом КИ (j) будет считана информация, поступившая по входящему КИ (i).

Таким образом, в течение каждого канального интервала к РЗУ производится два обращения. Первое обращение (Запись), когда некоторое управляющее устройство (на рис. 8 показано как счетчик КИ) выбирает номер КИ, который определяет адрес записи информации в требуемую ячейку РЗУ. Второе обращение (Чтение), когда содержимое адресной памяти (АЗУ),

соответствующее определенному КИ, выбирается в качестве адреса считывания информации из соответствующей ячейки РЗУ.

Для управления работой РЗУ используются два способа: 1) последовательная запись и произвольное чтение;
2) произвольная запись и последовательное чтение.

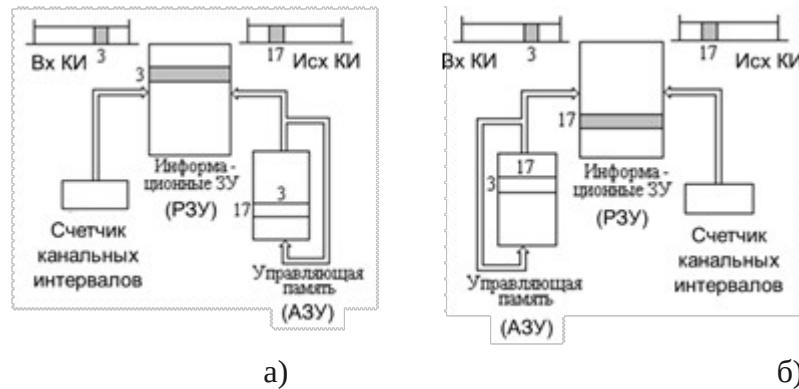


Рис. 9 Способы работы РЗУ временного коммутатора:

- а) последовательная запись – произвольное чтение; б) произвольная запись – последовательное чтение

На рисунке 9 показан принцип работы временной коммутации для обоих способов управления с иллюстрацией способа доступа к памяти при передаче информации из КИ №3 в КИ №17. Заметим, что оба способа работы звена временной коммутации используют циклическую управляющую память, доступ к которой осуществляется синхронно с работой счетчика временных интервалов (КИ).

Согласно первому способу работы РЗУ, показанному на рис. 9а, определенные ячейки памяти закрепляются за соответствующими канальными интервалами (КИ) входящего тракта ИКМ. Информация каждого входящего КИ запоминается в последовательных ячейках памяти, что обеспечивается увеличением на 1 содержимого счетчика по модулю 32 на каждом КИ. Как уже отмечалось, информация, принятая в течение КИ №3, автоматически запоминается в третьей ячейке РЗУ. При выдаче информации из РЗУ управляющая информация, поступающая из адресной памяти, определяет адрес считывания информации для заданного КИ. Как уже было указано, семнадцатое слово адресной памяти содержит число 3, т.е. содержимое РЗУ по адресу 3 должно быть прочитано и передано по исходящему тракту в течение КИ №17.

Второй способ работы звена временной коммутации, показанный на рисунке 9б, является противоположностью первого. Поступающая на вход информация записывается в ячейки РЗУ в соответствии с адресом, хранящимся в адресной памяти; однако считывание информации производится последовательно ячейка за ячейкой под управлением счетчика канальных интервалов. Как показано в данном примере, информация, принятая в течение канального интервала 3, записывается непосредственно в РЗУ по адресу 17, откуда автоматически считывается в исходящий канал с номером 17 исходящего тракта ИКМ.

Заметим, что оба способа работы звена временной коммутации, показанные на рисунке 9, определяют соответственно *управление по выходу и по входу*. В примере многозвенной коммутационной схемы, рассматриваемой в следующем практическом занятии, удобно один способ работы использовать на одном звене временной коммутации, а второй способ — на другом звене.

Задание 2. Во временном коммутаторе на одну линию ИКМ-30/32 реализовать коммутацию входящего разговорного канального интервала (КИ) с исходящим КИ в соответствии с данными табл. 2 (номер варианта соответствует номеру студента в списке группы).

Таблица 2. Варианты исходных данных для задания 2

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Требуется:

1. Изобразить схему временного коммутатора с указанием номеров ячеек разговорного (РЗУ) и адресного (АЗУ) запоминающих устройств и содержимого этих ячеек в двоичном коде.
 2. Описать процесс работы схемы при установлении соединения. Указать особенность реализации двухсторонней связи.
 3. Определить временную задержку информации при коммутации указанных КИ на передачу и на прием.

Содержание отчета

1. Схема временного коммутатора с указанием всех параметров (номеров и содержимого ячеек памяти).
 2. Описание процесса работы схемы при установлении соединения с указанием параметров работы схемы для реализации коммутации обратного направления.
 3. Расчет временной задержки информации при коммутации на передачу и на прием.

Контрольные вопросы

1. Каков основной недостаток имеет временная коммутация цифровых каналов?
 2. На каких элементах строятся временные коммутаторы?
 3. Возможна ли временная коммутация канального интервала 29 с канальным интервалом 17?
 4. Какова будет временная задержка при коммутации канального интервала 14 КИ с канальным интервалом 6?
 5. Какова будет временная задержка при коммутации канального интервала 11 с канальным интервалом 31?
 6. Из чего состоит временной коммутатор?
 7. Какова разрядность разговорной памяти временного коммутатора?
 8. Какова разрядность адресной памяти временного коммутатора на одну цифровую линию ИКМ-30?
 9. Какая информация записывается в ячейки адресной памяти временного коммутатора?
 10. Сколько ячеек содержит адресная память временного коммутатора на одну цифровую линию ИКМ-30?
 11. В чем отличие разных способов управления работой РЗУ?

Практическая работа 3

Пространственная коммутация цифровых сигналов на примере цкп "в - п - в" системы ewsd

Пространственную коммутацию цифровых сигналов рассмотрим на примере цифрового коммутационного поля, построенного по принципу "Время - пространство - время" (В-П-В) системы EWSD. Коммутационное поле станции EWSD состоит из временных и пространственных звеньев (рисунок 8). Особенностью EWSD является использование в ЦКП цифровых линий со скоростью передачи информации 8192 Кбит/с. Это означает организацию 128-и восьмибитовых временных интервалов в одном цикле ИКМ длительностью 125 мксек.

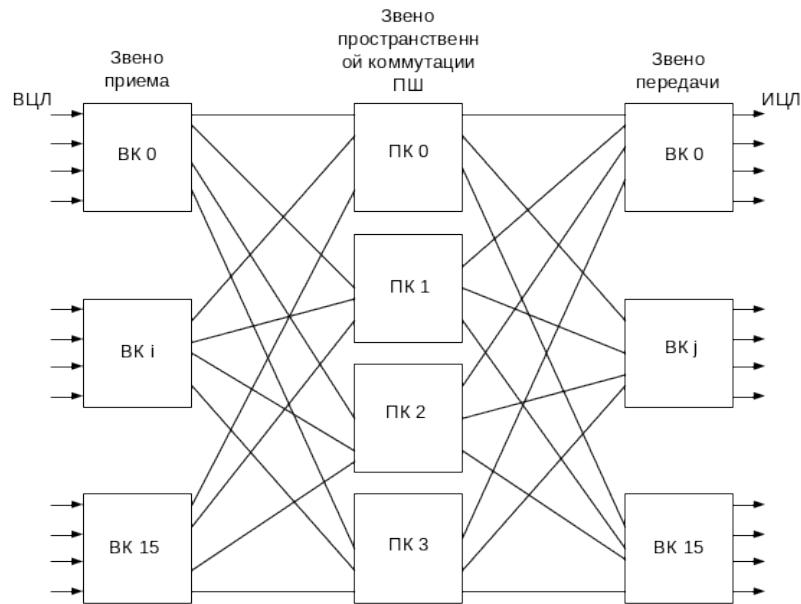


Рисунок 8 – Цифровое коммутационное поле «В – П – В»

Звенья приема и передачи типа «В» строятся с использованием временных коммутаторов с параметрами 4×4 ЦЛ. В каждом звене, используется максимум по 16 временных коммутаторов. С учетом того, что в цифровой линии организовано 128 ВИ, емкость временного коммутатора, выраженная во временных интервалах, составит 512×512 .

Для записи пользовательской информации в ЗУИ каждого временного коммутатора приема и передачи используется по 512 восьмиразрядных ячеек памяти. Запись кодовой комбинации в ЗУИ временных коммутаторов **приема** осуществляется по 1-му режиму построения ВК. Запись кодовой комбинации в ЗУИ временных коммутаторов **передачи** осуществляется по 2-му режиму построения ВК.

Для записи управляющей информации в ЗУА каждого временного коммутатора приема и передачи используется по 512 девятиразрядных ячеек памяти. Ячейки девятиразрядные, так как максимальный номер ячейки памяти ЗУИ равен 511. Содержимое ячейки ЗУА в звене **приема** - это номер ячейки ЗУИ, откуда следует считать кодовую комбинацию. Содержимое ячейки ЗУА в звене **передачи** - номер ячейки памяти ЗУИ, куда следует записать кодовую комбинацию. Номера ячеек памяти ЗУА в звеньях приема и передачи информации соответствуют номеру канала промежуточного шнура (ПШ) и номеру цифровой линии ПШ.

Пространственное звено ЦКП EWSD построено на 4 пространственных коммутаторах (ПК) с параметрами 16×16 ЦЛ. Число электронных, контактов в матрице ЭК зависит от количества временных коммутаторов в звеньях приема и передачи и составляет $16 \times 16 = 256$. Количество матриц ЗУА в одном пространственном коммутаторе определяется, числом исходящих цифровых линий к временным коммутаторам звена передачи и составляет 16. Емкость ЗУА одного пространственного коммутатора определяется количеством временных интервалов в одной цифровой линии промышнера и составляет 128 ячеек. Разрядность ячеек памяти ЗУА определяется максимальным адресом электронного контакта и составляет 4.

Последовательность коммутации в ЦКП "В-П-В" опишем следующим образом:

1) При поступлении заявки на поиск соединительного пути в ЦКП "В-П-В" управляющее устройство ЦКП определяет координаты пути, предоставленного абоненту для разговора:

- номера входящей и исходящей цифровых линий;
- номера временных интервалов в цифровых линиях.

Из таблиц пересчета считаются данные о номерах временных коммутаторов приема и передачи, в которые включены входящая и исходящая цифровые линии.

2) УУ ЦКП определяет свободный временной канал промшнуря и проверяет условие его доступности временными коммутаторам звеньев приема и передачи. По таблицам пересчета определяются номера ячеек памяти, соответствующие временному интервалу промшнуря, в следующих адресных запоминающих устройствах:

- ЗУА временного коммутатора звена приема,
- ЗУА пространственного коммутатора,
- ЗУА временного коммутатора звена передачи.

3) В ячейки памяти ЗУА записывается управляющая информация:

- В ячейку памяти ЗУА временного коммутатора приема записывается номер ячейки памяти ЗУИ своего временного коммутатора, откуда следует считать кодовую комбинацию.
- В ячейку памяти ЗУА пространственного коммутатора записывается номер электронного контакта, который следует открыть во временном интервале промшнуря.
- В ячейку памяти ЗУА временного коммутатора передачи записывается номер ячейки памяти ЗУИ своего временного коммутатора, куда следует поместить кодовую комбинацию.

4) При установлении соединения в ЦКИ "В-П-В" используется произвольная запись данных в три ЗУА: ЗУА ВКпр, ЗУА ПК, ЗУА Вкпер. Данные из всех ЗУА считаются одновременно во время, соответствующеециальному каналу промшнуря. При наступлении ВИ промшнуря считывается кодовая комбинация из ячейки памяти ЗУИ временного коммутатора приема, одновременно открывается нужный электронный контакт в пространственном коммутаторе, в это же время кодовая комбинация записывается в ячейку памяти ЗУИ временного коммутатора передачи в соответствии с адресом, записанным в ЗУА.

Для упрощения индексов в формулах, приведенных ниже, звено приема в дальнейшем будем обозначать индексом А, звено пространственной коммутации - индексом В, а звено передачи - индексом С.

Задание на выполнение практической работы

В коммутационном поле со структурой «время-пространство-время» (В-П-В) на 8 входящих и 8 исходящих линий ИКМ-30/32 установить одностороннее соединение заданного КИ входящей ИКМ-линии с заданными КИ исходящей ИКМ-линии с использованием свободного КИ внутренней ИКМ-линии в соответствии с данными табл. 1 (номер варианта соответствует номеру студента в списке группы).

Требуется:

1. Определить требуемое число и характеристики пространственных и временных коммутаторов, необходимых для построения коммутационного поля.
2. Изобразить схему коммутационного поля с указанием используемых при коммутации временных и пространственных коммутаторов, номеров ячеек управляющих и разговорных ЗУ, содержимого этих ячеек. Примечание: на входящей ступени временной коммутации использовать управление по выходу, а на исходящей ступени – по входу.
3. Описать процесс работы схемы при коммутации одностороннего разговорного тракта заданных входящей ИКМ-линии и входящего КИ с исходящей ИКМ-линией и исходящим КИ с использованием заданного КИ внутренней линии.
4. Определить суммарную временную задержку информации при коммутации указанных КИ через коммутационное поле в прямом и обратном направлении.

Таблица 1 Варианты исходных данных

№ варианта	1	2	3	4	5	6	7	8	9	1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5
------------	---	---	---	---	---	---	---	---	---	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------

Входящая ИКМ-линия	0	2	5	1	7	3	6	4	1	5	2	6	3	0	4	1	5	7	3	6	2	4	5	7	0	
Входящий КИ	5	1	4	1	2	5	2	4	1	3	1	2	1	8	6	4	3	0	5	1	9	2	8	1	8	2
Кодовый отсчет речевого сигнала	2	8	1	5	3	4	2	0	1	8	6	2	1	9	1	7	5	8	6	1	7	3	0	4	4	
Номер свободного КИ внутри линии	2	2	1	4	3	0	1	7	2	6	1	8	9	1	9	1	8	6	1	7	2	8	1	3	2	
Исходящая З ИКМ-линия	0	2	4	2	7	3	5	1	4	1	6	4	2	7	5	3	4	6	7	3	7	0	5	2	6	
Исходящий КИ	1	2	4	7	3	0	2	4	1	6	1	5	2	1	6	8	4	1	9	2	4	1	6	2	1	
Реализация ПК	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	М	Д	

Примечание: М – мультиплексор, Д - демультиплексор

Нумерация ИКМ-линий и КИ в них начинается с нуля.

ПРИМЕР РЕШЕНИЯ ЗАДАЧИ.

В ЦП "В-П-В" определить номера и содержимое ячеек памяти ЗУИ и ЗУА при коммутации 78-го временного интервала 31-й входящей ЦЛ с 100-м временным интервалом 45-й исходящей ЦЛ по свободному 39-му временному интервалу промшнтра через ПК З.

Передаваемая кодовая комбинация – 121.

Исходные данные к задаче показаны на рисунке 9.



Рисунок 9 – Исходные данные к задаче

РЕШЕНИЕ:

1) Определение номеров ВК на звеньях приема (A) и передачи (C). $N_{BK} = \overline{0.15}$.

$$N_{BK}^A = \lfloor N_{ВЦЛ} / 4 \rfloor = 31 / 4 = 7$$

$$N_{BK}^C = \lfloor N_{ИЦЛ} / 4 \rfloor = 45 / 4 = 11$$

2) Определение номера цифровой линии (входящей исходящей) внутри одного временного коммутатора в звеньях А и С. $N_{WK} = \overline{0.3}$

$$N_{ЦП}^A = N_{ВЦЛ} - 4 * N_{BK}^A = 31 - 4 * 7 = 3$$

$$N_{ЦП}^C = N_{ИЦЛ} - 4 * N_{BK}^C = 45 - 4 * 11 = 1$$

3) Определение номера ячейки памяти ЗУИ на звене приема (А) и ее содержимого. $N_{яп}^{ЗУИ} = \overline{0,511}$.

$$N_{яп_а}^{ЗУА} = 128 * N_{ЦЛ}^A + N_{ВИ}^{ВЦЛ} = 128 * 3 + 78 = 462$$

Содержимое ЯП ЗУИ – 01111001

4) Определение номера ячейки памяти ЗУА на звене приема (А) и ее содержимого $N_{яп}^{ЗУА} = \overline{0,511}$

$$N_{яп_а}^{ЗУА} = 128 * N_{ЦЛ}^{ПШ} + N_{ВИ}^{ПШ} = 128 * 3 + 39 = 423$$

$$N_{ЦЛ}^{ПШ} = N_{ПК} = 3$$

Содержимое ЯП ЗУИ – 111001110 (Число 462)

5) Определение номера электронного контакта в пространственном коммутаторе. $N_{ЭК} = \overline{0,15}$.

$$N_{ЭК} = N_{ВК}^A = 7$$

6) Определение номера матрицы ЗУА в звене (В). $N^{ЗУА} = \overline{0,15}$.

$$N_{ЗУА} = N_{ВК}^C = 11$$

7) Определение номера ячейки памяти ЗУА на звене (В) и ее содержимого $N_{яп}^{ЗУА} = \overline{0,127}$.

$$N_{яп_в}^{ЗУА} = N_{ВИ}^{ПШ} = 39$$

Содержимое ЯП ЗУА - 0111 (Номер электронного контакта).

8) Определение номера ячейки памяти ЗУИ на звене передачи (С) и ее содержимого..

$$N_{яп_с}^{ЗУИ} = 128 * N_{ЦЛ}^C + N_{ВИ}^{ИЦЛ} = 128 * 1 + 100 = 228$$

Содержимое ЯП ЗУИ - 01111001.

9) Определение номера ячейки памяти ЗУА на звене передачи (С) и ее содержимого..

$$N_{яп_с}^{ЗУА} = 128 * N_{ПК} + N_{ВИ}^{ПШ} = 128 * 3 + 39 = 423$$

Содержимое ЯП ЗУА - 011100100

Пространственный эквивалент решения задачи показан на рисунке 10.

В ЗУИ звена приема пользовательская информация записывается последовательно, в тakt с ВЦЛ. В приведенной задаче запись информации осуществляется в ЗУИ 7-го ВК приема во временном интервале, соответствующем 31-й входящей цифровой линии и 78-му временному каналу. Из матрицы ЗУИ звена приема информация считывается произвольно, т.е. по адресу, записанному в ячейке памяти ЗУА. В приведенной задаче считывание информации осуществляется из ЗУИ 7-го ВК приема во временном интервале, соответствующем 3-й цифровой линии промшнур и 39-му ВИ в ней.

В ЗУИ звена передачи пользовательская информация записывается произвольно в соответствии с адресом, содержащимся в ЗУА. В приведенной задаче запись информации осуществляется в ЗУИ 11-го ВК передачи во временном интервале, соответствующем 3-й цифровой линии промшнур и 39-му ВИ. Из матрицы ЗУИ звена передачи информация считывается последовательно, в тakt с ИЦЛ. В приведенной задаче считывание информации осуществляется из ЗУИ 11-го ВК передачи во временном интервале, соответствующем 45-й исходящей цифровой линии и 100-му ВИ.

Запись управляющей информации во все ячейки памяти ЗУА всех звеньев - произвольная, а считывание из ячеек памяти ЗУА - последовательное, в соответствии с очередностью каналов промшнур (в задаче задан ЗПШ, 39ВИ). В момент времени, соответствующий 39-му временному интервалу 3-й цифровой линии ПШ происходит следующее:

1. Пользовательская информация 01111001 считывается из 462-й ячейки памяти ЗУИ 7-го временного коммутатора.

2. Открывается ЭК7 в пространственном коммутаторе ПКЗ. При этом пользовательская информация, поступающая по 7-й цифровой линии от ВК7 звена приема коммутируется через ЭК7 на цифровую линию 11 к ВК11 звена передачи.

3. Пользовательская информация записывается в 228-ю ячейку памяти ЗУИ временного коммутатора 11 звена передачи.

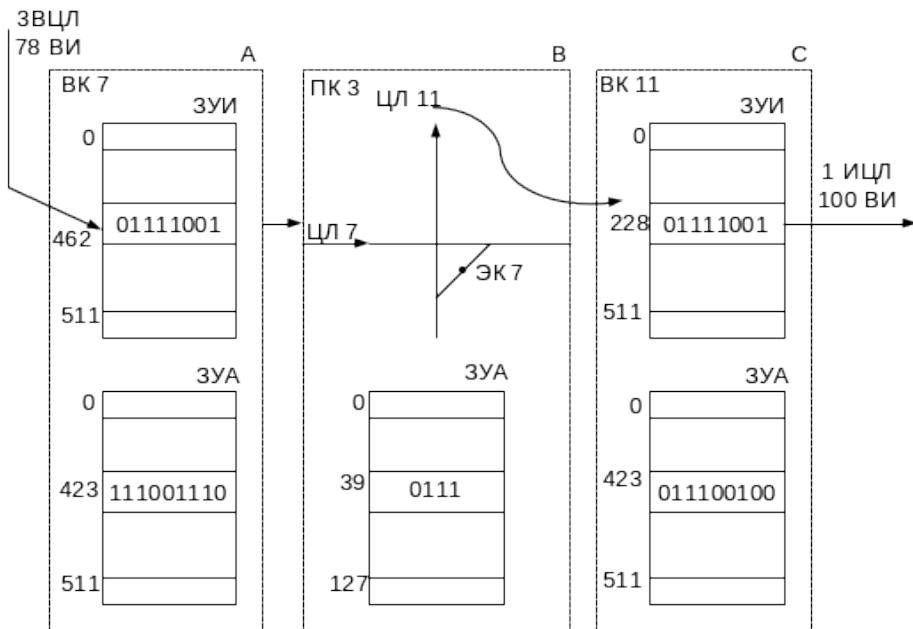


Рисунок 10 - Пространственный эквивалент решения задачи

Практическая работа 4

Тема: Знакомство с АТС для малого и среднего бизнеса HiPath 3000 фирмы Siemens

Цель работы: Изучить и освоить основы коммутации на платформе HiPath 3000, выявить возможности и приоритеты.

Практические навыки:

- правильного подключения и инициализации станции;
- безошибочного выполнения действий по подключению.

Продолжительность занятия – 2 ч.

Ход работы:

В системе HiPath 3000 реализован целый ряд дополнительных коммуникационных функций для предприятий малого и среднего бизнеса. Доступ к общедоступной телефонной сети осуществляется через операторов аналоговых или ISDN-сетей или через интернет-подключения к альтернативным провайдерам услуг интернет-телефонии (ISP/ITSP). IP-телефоны со встроенными мини-коммутаторами можно без проблем интегрировать в существующую инфраструктуру LAN, используя концепцию one wire to the desk (одного кабеля к рабочему месту). Беспроводную связь для работы приложений передачи голоса и данных можно также организовать с использованием базовых станций WLAN. Цифровые системные телефоны (UP0/E) можно использовать совместно с IP-телефонами, заменять одни на другие и модернизировать. При этом можно по-прежнему пользоваться традиционными аналоговыми телефонами, факсовыми аппаратами и домофонами, а также беспроводными телефонными аппаратами на базе технологии DECT. Функции голосовой почты уже интегрированы в малые системы. Для удовлетворения требований предприятий более крупного размера предусмотрено интегрированное решение HiPath Xpressions Compact, которое позволяет организовывать ящики голосовой почты с набором специальных функций и функцию автосекретаря (дежурного оператора), управляемого командами меню. Во всех моделях системы HiPath 3000 применяется интерфейс телекоммуникационных технологий с

использованием вычислительной техники CSTA (Computer Supported Telecommunications Applications), используемый для реализации децентрализованных (1-st party) и централизованных, на базе сервера (3-ed party), решений CTI.

Системные интерфейсы

На сетевой стороне:

Евро-ISDN:

Интерфейс базового доступа S0 с протоколом DSS1

– Системное подключение

– Подключение точки-многоточка

Интерфейс первичного доступа S2M

с протоколом DSS1

Аналоговые линии:

Подключение аналоговой линии с возможностью прямого набора номера (DDI/DID)

Поддержка Интернет-телефонии: Системное подключение; Подключение пользователя

На стороне пользователя:

Аналоговое: Для подключения аналоговых оконечных устройств, например, факсовых аппаратов, телефонов, модемов

Цифровое: Для подключения цифровых двухканальных системных телефонов (UP0/E);

Для подключения базовых станций DECT

Евро-ISDN: Абонентская шина S0 для подключения до 8 оконечных устройств с независимым питанием каждое (например, факсовых аппаратов стандарта Group 4, платы ISDN-ПК)

HG 1500: Интерфейсы 2x10/100 BaseT, шлюз 10/100 Мбит/с для интеграции с LAN.

Подключение к внешним LAN и интернет соответственно через интерфейсы ISDN и DSL.

V 24 с протоколом CSTA: Для подключения приложений, применяемых в гостиничном бизнесе, и приложений для обслуживания клиентов

Интерфейс E&M: HiPath 3800

S0 FV, S2MFV или PRI с протоколами CorNet-N, CorNet-NQ и Q-Sig: Постоянное цифровое подключение

LAN-интерфейс: 10 Мбит/с для системного администрирования через TCP/IP

Технические характеристики

Электропитание:

Системы по умолчанию ориентированы на питание от общей сети. При возможных перебоях в электропитании задействуются источники бесперебойного питания (UPS). Номинальное входное напряжение (переменный ток)-88-264В. Номинальная частота-50-60Гц. Питание от аккумуляторных батарей (постоянный ток)-48В.

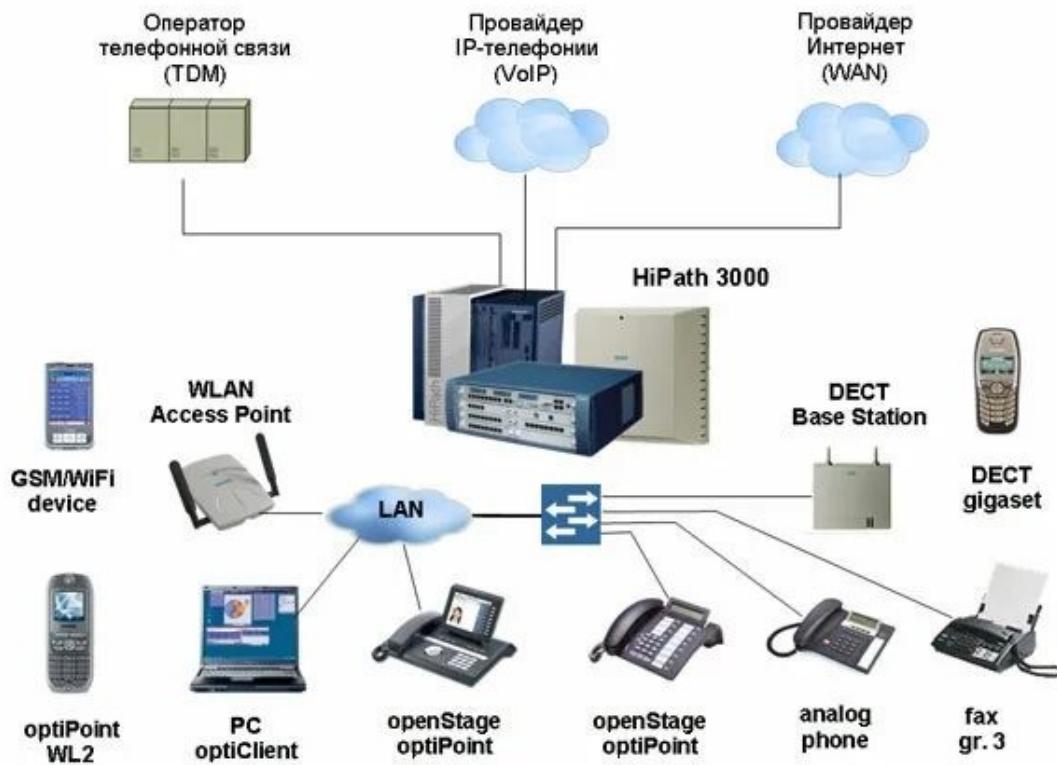
Эксплуатационные условия

окружающей среды: температура от +5 до + 40, относительная влажность воздуха-5-85%.

Дальность действия:

Между HiPath 3000 и системным телефоном: макс. 500 м. Прибл. 1000 м с подключаемым источником питания, в зависимости от типа сети. Между объединенными в сеть системами HiPath в помещениях, принадлежащих компаний:

Постоянное подключение S0: прибл. 1000 м Постоянное подключение S2M: макс. 250 м, в зависимости от типа сети. Для повышения дальности действия может потребоваться установка сетевых адаптеров. Дальность действия в общедоступной сети не ограничена.



Подключение и запуск станции:

При развёрнутой кроссировке необходимо проследить правильность подключения на патч-панели витой пары, подключение патч-кордов и разведение кабелей от интерфейсов всех типов HiPath 3000

После инициализации АТС нужно проследить загрузку модулей и плат (HiPath 3800) по встроенным индикаторам- зелёного и красного цвета, а также загрузку базовых станций Cordless.

Если аппаратные терминалы отображают 1 января 0000 года- АТС готова к первичному администрированию. Установить язык можно с помощью пароля на терминале * 95 и подменю 48 Настроить IP адреса и маску подсети.

В случае успешной настройки через терминал необходимо подключить ПК через LAN или V 24 непосредственно к АТС.

Задание:

1. Правильное подключение и инициализация станции.
2. Безошибочное выполнение действий по подключению.

Практическая работа 5

Тема: Практическое применение интерфейсов в АТС Н 3500 и Н 1120

Цель работы: С помощью программного продукта HiPath Manager E изучить применение и типы интерфейсов HiPath 3000, а также уметь создавать различные группы и конфигурирование линий АТС.

Практические навыки:

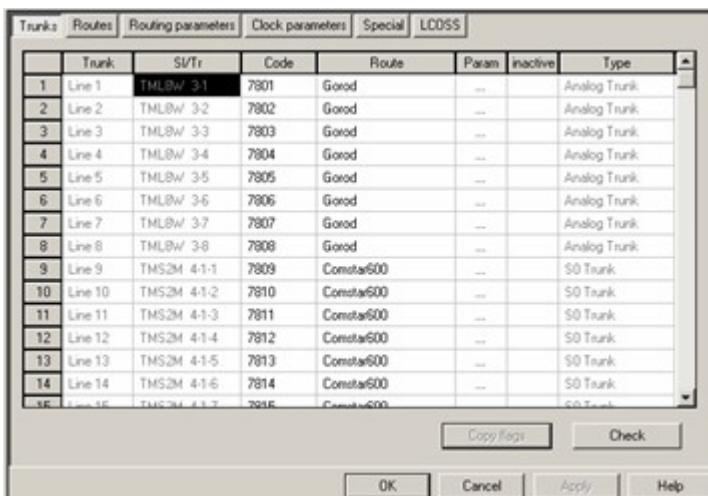
- правильной загрузки всех данных на станции HiPath 3000;
- безошибочного выполнения команд в программном продукте Siemens HiPath Manager E;
- выставления всех параметров системы.

Продолжительность занятия – 2 ч.

Ход работы:

Конфигурирование внешних линий.

Внешние линии конфигурируются в диалоговом окне Lines/networking.



Значения полей диалогового окна **Lines/networking/ Trunks**, описывается следующим:

Trunk -Порядковый номер линии.

SI/Tr -Название модуля / номер слота / номер порта

Code -Код директивного доступа к транку.

Route -Направление, к которому принадлежит данная линия

Направление – группа линий, объединенных определенными свойствами.

Param -Двойной щелчок по данному полю открывает диалог настроек данной конкретной линии.

inactive -Показывает состояния линии (* - линия не активна)

Type- Тип линии:

Analog Trunk – для аналоговых линий

S0 Trunk, CorNet Trunk, QSIG network - для цифровых линий

Параметры аналоговых линий.

Назначение флагов бокса **flags** описано следующим:

DTMF DID- Позволяет тоновый набор на данной линии.

Trunk supervision -Контроль линии.

Назначение остальных параметров описано следующим:

Dialing metod

Тип набора:

Automatic – автоопределение

DTMF – тональный

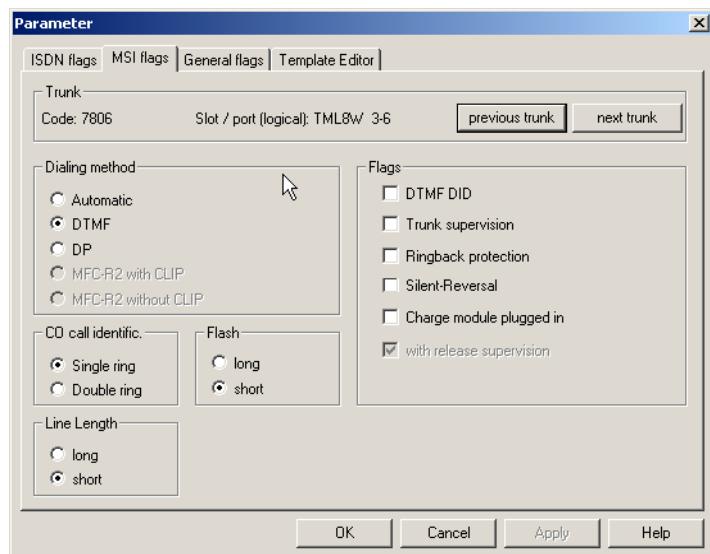
DP - импульсный

Line Length

Чувствительность:

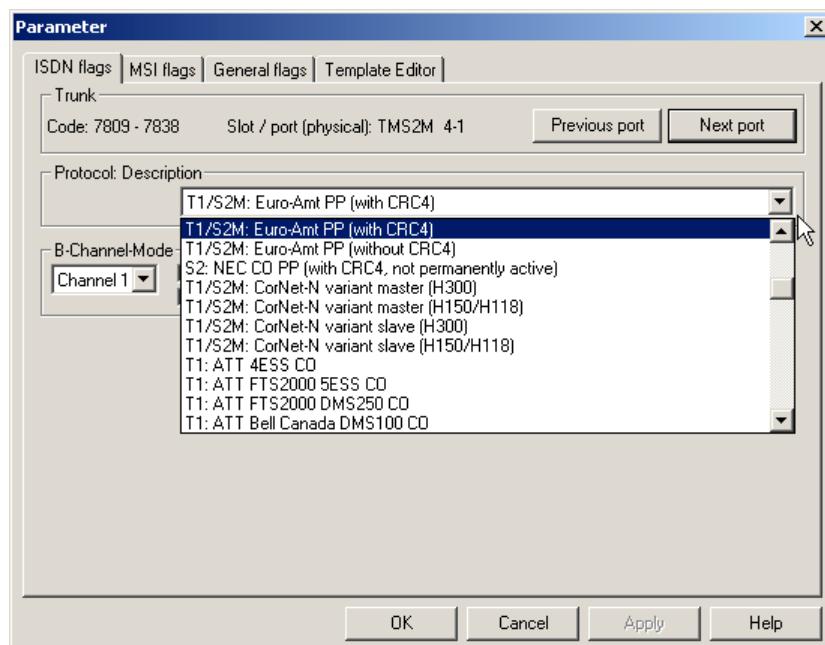
Long – высокая

Short – низкая



Параметры цифровых линий.

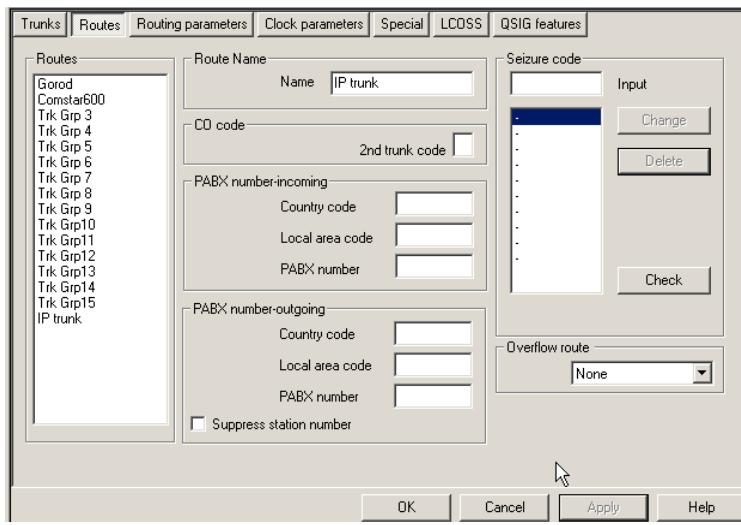
Данная вкладка диалога **Parameters** определяет логический протокол, действующий на данной цифровой линии.



Для установки протокола на цифровую линию E1 либо So (модули **TMS2/TS2** либо **STMD/STLS**), достаточно сконфигурировать один из **b**-каналов линии.

Создание направлений.

Направления - группы линий, объединенных определенными свойствами, конфигурируются в **Lines/networking / Routes**.



В системах HiPath 3000 может быть организовано до 16 направлений. Каждому направлению может быть присвоено имя (поле **Route Name**). Блоки **PABX number – incoming** и **PABX number – outgoing** определяют цифровые последовательности, отправляемые системой в цифровую сеть по данному направлению (идентификатор системы (только для цифровых линий)). Поле **Seizure Code** определяет префикс выхода на данное направление (не используется при активизации **LCR**). Поле **Overflow rout** определяет направление переполнения для данного (не используется при активизации **LCR**). Поле **Suppress station number** позволяет запретить отправку **DID** абонента в цифровую сеть (не отправлять **DID** в виде АОН).

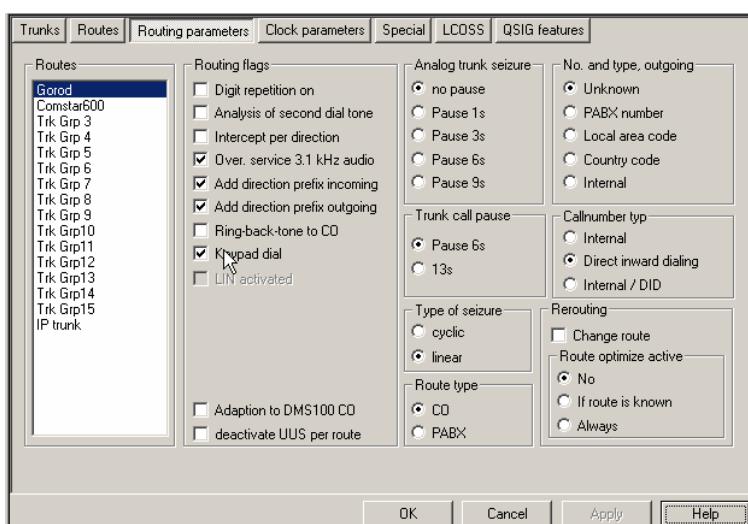
Для формирования АОН используются следующие данные:
DID -поле в **Setup Station**;
CLIP -поле в **Setup Station**

Country code Local area Code PBX number -поля блока **PABX number-outgoing** вкладки **Routes**.

Содержимое полей будет отослано в виде АОН, в зависимости от данных блока **No. And type,outgoing** вкладки **Routing parameters**.

Параметры направлений.

Во вкладке **Routing parameters**, определяются параметры направлений.



Значение флагов бокса **Routing flags** описано следующим:

Digits repetition on- Повторение префикса в линию (не работает с LCR)

Analisis of second dial tone -Ожидание второго диал-тона после набора «8».

Add direction prefix incomming -Отображение префикса выхода на направление на дисплее Optipont терминала при входящей связи.

Add direction prefix outgoing-Отображение префикса выхода на направление на дисплее Optipont терминала при исходящей связи.

Analog trunk seizure -Пауза между занятием транка и началом набора.

Trunk call pause- Пауза между освобождением и повторным занятием Транка.

Type of seizure-Способ занятия линий в направлении

Route type -Тип направления:

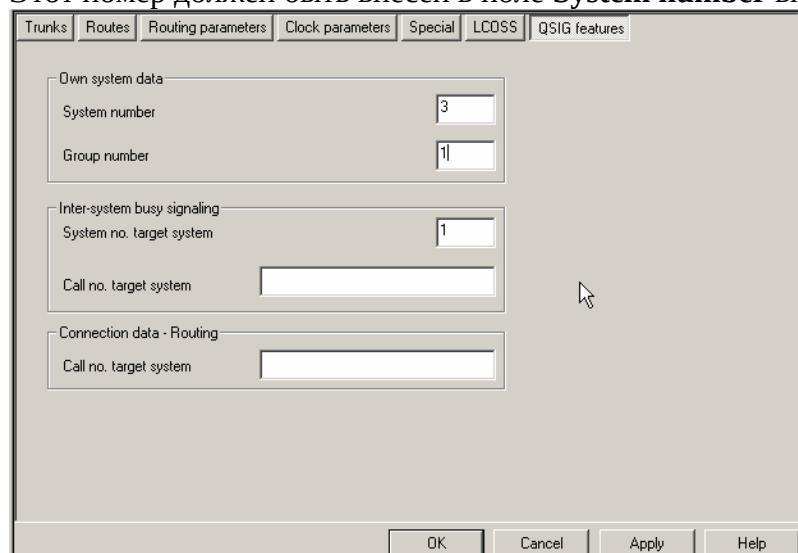
CO – данные о правах не передаются

PABX - данные о правах передаются

No. and type outgoing Определяет: какие поля из **PABX number – incoming** и **PABX number – outgoing** диалога **Routes** передавать в цифровую сеть как АОН(идентификатор системы).

При построении сети станций (IP сеть либо TDM с протоколом Cornet N) и реализации межстанционного роуминга для **HiPath Cordless**, каждая система HiPath 3000 должна иметь свой уникальный номер во всей сети.

Этот номер должен быть внесен в поле **System number** вкладки **QSIG features**.



Задание:

- 1.Запустить приложение HiPath Manager E и провести первоначальные настройки.
- 2.Сконфигурировать различные группы абонентов (группы перехвата, группы поиска).
- 3.Сконфигурировать все возможные линии на АТС фирмы Siemens.

Практическая работа 6

Тема: Первичная настройка АТС и установка новой версии системы

Цель работы: Изучить на практике первичное администрирование станций HiPath 3000 с помощью программного продукта HiPath Manager E.

Практические навыки:

- правильного извлечения и загрузки файла пользовательских настроек системы (KDS-файла);
- конфигурации абонентов системы и установки их параметров.

Продолжительность занятия – 2 ч.

HiPath 3000 Manager E – программная оболочка, являющаяся основным средством администрирования систем **HiPath3000**.

HiPath 3000 Manager E является Windows-приложением, совместимым с Windows 95,98, NT,2000, XP.

Данная программа позволяет:

- Извлекать и загружать файл настроек системы (KDS-файл);
- Изменять KDS-файл
- Сохранять KDS-файл на локальном диске и др. носителях;
- Загружать в систему файлы языковой поддержки (LNG-Файл);
- Заменять операционную систему **HiPath3000**;
- Производить мониторинг системы **HiPath3000**;
- Производить другие процедуры администрирования.

При установке по умолчанию, компоненты приложения будут расположены на локальном диске в **C:\Program Files\Siemens\HiPath3000Manager E**.

Запуск приложения **HiPath3000 Manager E**:

При запуске, приложение требует ввести имя пользователя и пароль.

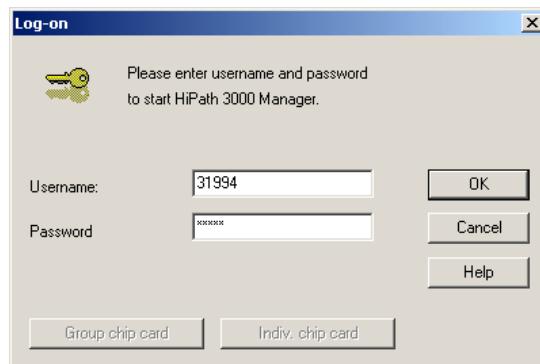
Эта процедура авторизации позволяет вынести решение о доступе пользователя к администрированию системы и об уровне доступа.

Для получения доступа к администрированию системы, необходимо ввести следующие данные:

Имя пользователя: 31994

Пароль: 31994

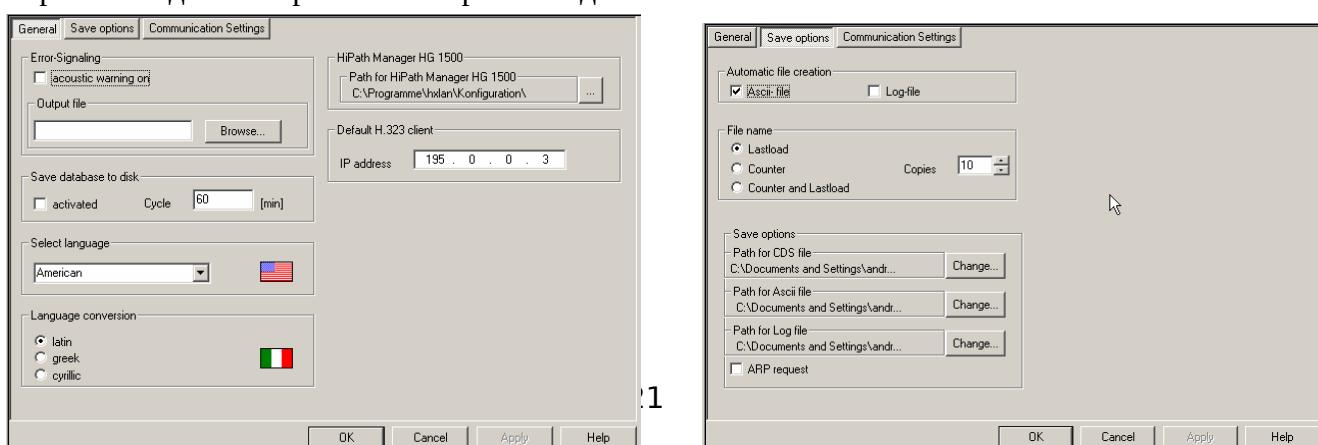
Описанные имя пользователя и пароль являются стандартными по умолчанию.
Их значения впоследствии можно изменить. Ниже показано окно авторизации:



Настройка оболочки **HiPath3000 Manager E**:

Настройки оболочки производятся в меню **Options/Program options**.

Это меню называется вкладкой основных настроек. Меню ниже является вкладкой настроек сохранения- для выбора места сохранения данных.



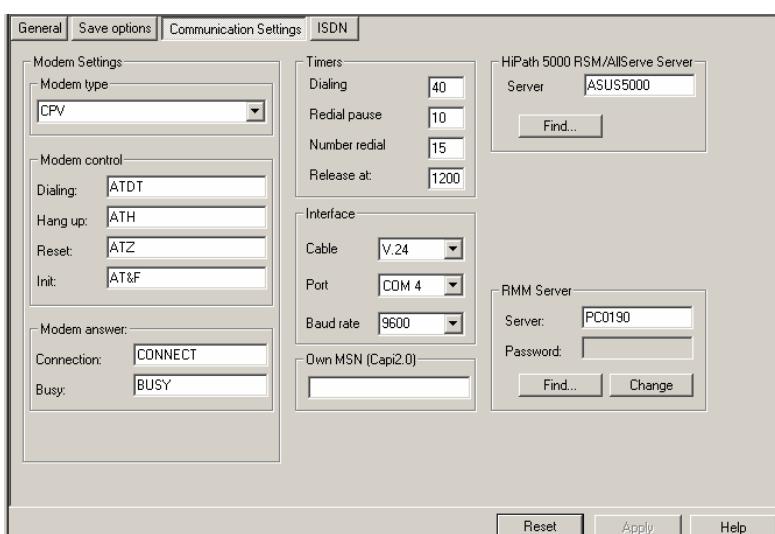
Вкладка настроек соединения (см. ниже) с системой содержит поля, определяющие тип и параметры соединения администрирующего компьютера с системой HiPath 3000.

В поле **interface/port** указывают порт компьютера, к которому подключен кабель V.24 прямого соединения с системой, либо порт, к которому подключен модем (при удаленном администрировании системы).

В поле **interface/baud rate** необходимо указать скорость интерфейса.

При прямом кабельном соединении необходимо **точно** указать скорость соединения. Она должна соответствовать скорости, выставленной для соответствующего порта V.24 в системе HiPath 3000.

В поле **init** блока **Modem settings/modem control** необходимо выставить команду инициализации модема **AT&F**. Такая строка инициализации подходит для большинства типов модемов.



Первоначальная инициализация системы включает в себя:

- Установку национальных параметров (тоновые и временные параметры, характерные для России).
- Загрузку языкового файла, необходимого для правильного отображения информации на дисплеях Optipoint 500 терминалов (если языковой файл не был загружен предварительно).
- Изменение скорости интерфейсов V.24 системы (Необязательная процедура, большей скорости интерфейса соответствует меньшее время, необходимое на передачу данных).

Установка национальных параметров системы.

Установка национальных параметров системы осуществляется с системного телефона (1-й и 2-й цифровые порты в системе), либо с помощью эмулятора цифрового телефона, встроенного в HiPath 3000 Manager E.

Эмулятор может быть активирован с помощью радиокнопки **Online** диалогового окна **Transfer**.

При первом сеансе администрирования необходимо: ***95 31994 V 31994 V 31994 V**

После сброса в заводские установки необходимо: **31994 V**

При последующих сеансах необходимо: ***95 31994 V 31994 V 29 5 V * 41 V**

После выполнения описанных действий, система перезагрузится. Тоновые и временные параметры после загрузки будут соответствовать российским.

Изменение скорости интерфейсов V.24 системы.

Изменение скорости интерфейсов не является необходимой операцией, однако увеличение скорости интерфейса уменьшает время, необходимое на передачу данных между компьютером и системой во время сеанса администрирования.

По умолчанию (после сброса в заводские установки) скорость всех интерфейсов V.24 системы равна 9600 бод.

Для ускорения процессов администрирования можно увеличить скорость интерфейса до 19200 бод.

При первом сеансе администрирования: *95 31994 V 31994 V 31994 V

после сброса в заводские установки: 31994 V

(состояние системы при поставке) 22 13 V * 3 V

При последующих сеансах: *95 31994 V 31994 V 22 13 V * 3 V

Загрузка языкового файла.

Загрузка языкового файла (LNG-файл) производится с помощью HiPath 3000 Manager E. Языковые файлы для различных версий систем HiPath 3000 инсталлируются на компьютер администратора вместе с приложением HiPath 3000 Manager E и расположены в корневом каталоге инсталлированного приложения в папке LNG. Обычно в C:\Program Files\Siemens\HiPath3000Manager E\LNG\

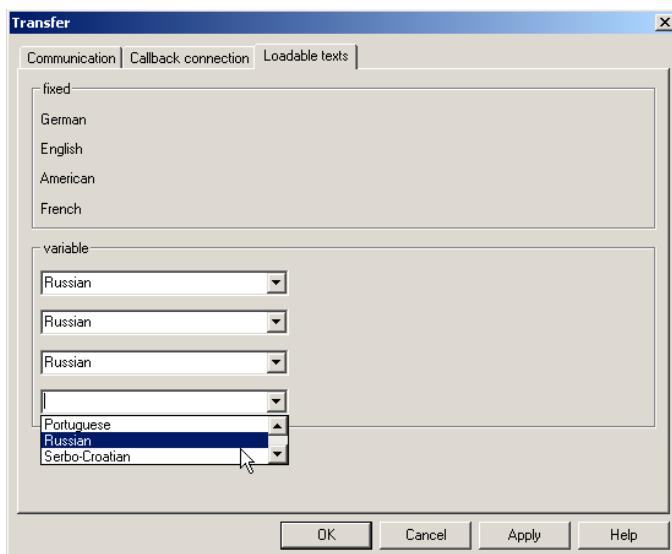
Версия загружаемого LNG –файла должна максимально соответствовать версии программного обеспечения системы.

Например: для станции с ПО версии 560S.09.366 подойдет файл LNG с версией 560S.09.365.

1. Открыть в HiPath 3000 Manager E соответствующий языковой файл (версию выбираемого LNG –файла можно определить в поле Info диалога Open customer database)

Примечание: поле «тип файла» диалога Open customer database должно содержать: LNG files (*.lng)

2. Во вкладке Loadable texts диалога Transfer установить значения полей с выпадающими списками в Russian.



3. Применить изменения нажатием Apply.

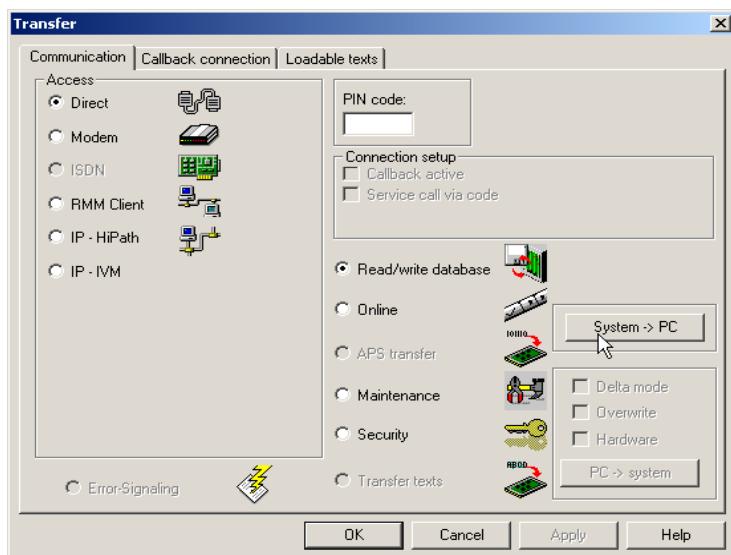
4. Во вкладке Communication активировать радиокнопку Transfer text и нажать кнопку Transfer text.

Извлечение и загрузка файла пользовательских настроек системы (KDS-файла).

Внесение любых изменений в настройки системы HiPath3000 происходит в режиме **Offline**. Такой подход подразумевает совершение следующих действий:

- Извлечение файла настроек из системы в оболочку HiPath3000 Manager E;
- Внесение необходимых изменений в настройки (манипуляции в оболочке);
- Загрузка измененного **файла настроек** в систему / загрузка **только изменений**.

Извлечение и загрузка файла настроек производится с помощью диалогового окна **Transfer**.



В поле **Access** указывается тип соединения:

Direct - прямое кабельное соединение.

Modem - модемное соединение (требуется указать № модема IMODC).

IP-HiPath - соединение через IP сеть (возможно только в случае наличия модуля **HXGM3/HXGS3/HXGR3** либо модуля **LIM**). При данном типе соединения требуется указать IP адрес центрального модуля системы (конфигурируется в диалоге **Network/basic settings**).

При извлечении и загрузке файла настроек системы должна быть активирована радиокнопка **Read/Write database**.

- Кнопка **System -> PC** активирует извлечение файла настроек в оболочку;
- Кнопка **PC -> System** активирует загрузку измененного файла в систему;

Конфигурирование абонентов системы.

Для определения параметров и свойств абонентских телефонов используется диалог **Setup station**.

Во вкладке **Station** определяется внутренний номер, номер **DID**, имя абонента, **Clip**.

DID – Direct Inward Dialing используется для адресации абонентов в цифровых сетях при входящих вызовах.

Clip - Значение которое будет отослано в цифровую сеть при исходящем вызове (идентификатор абонента).

Station Key programming Fax / Modem Emergency								
	Call no.	DID	Name	Status	Type	Type	Access	CLIP
1	100	100	ИВАНОВ И.И.	<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 1 Master	5551155
2	101	101		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 2 Master	
3	102	102		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 3 Master	
4	103	103		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 4 Master	
5	104	104		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 5 Master	
6	105	105		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 6 Master	
7	106	106		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 7 Master	
8	107	107		<input checked="" type="radio"/> *	No Port	Standard	SLM08 1 - 8 Master	
9	108	108		<input checked="" type="radio"/> *	No Port	Standard	SLMA2 2 - 1	
10	109	109		<input checked="" type="radio"/> *	No Port	Standard	SLMA2 2 - 2	
11	110	110		<input checked="" type="radio"/> *	No Port	Standard	SLMA2 2 - 3	
12	111	111		<input checked="" type="radio"/> *	No Port	Standard	SLMA2 2 - 4	
	112	112		<input checked="" type="radio"/> *	No Port	Standard	SLMA2 2 - 5	

Во вкладке также присутствуют информационные поля:

inactive - если телефон не активен

type- Полное название для цифровых, Р.О.Т для аналоговых

Access -Тип модуля/ номер модуля/ номер порта

Param- Двойной щелчок по данному полю открывает диалог **Setup station: Parameters**.

Установка параметров абонентов.

Необходимо открыть диалоговое окно **Setup station: Parameters/Flag status**.

Name	Call number	CLIP/LIN	Direct inward	Type	Access	Mobile code
ИВАНОВ И.И.	100	5551155	100	No Port	SLM08 1 - 1	<input checked="" type="radio"/>

Flag status [Activated features | Workpoint Client | Groups | Forwarding | Template Editor | ISDN flags]

<input type="checkbox"/> Override class of service	<input checked="" type="checkbox"/> Prevention of voice calling off	<input type="checkbox"/> Display of Emergency text
<input type="checkbox"/> Associated dialing/services	<input type="checkbox"/> Telephone lock intercept	<input type="checkbox"/> Voice recording
<input type="checkbox"/> Call Waiting rejection on	<input type="checkbox"/> DISA class of service	<input type="checkbox"/> Discreet Call
<input type="checkbox"/> Headset	<input type="checkbox"/> Door release DTMF	<input type="checkbox"/> Discreet Call Lock
<input type="checkbox"/> Override Do Not Disturb	<input checked="" type="checkbox"/> autom. connection, CSTA	<input type="checkbox"/> Incoming CDP/Analog
<input checked="" type="checkbox"/> Missed Calls List	<input type="checkbox"/> Ringback protection	
<input type="checkbox"/> MCID access	<input type="checkbox"/> Transit allowed via Hook-on	
<input checked="" type="checkbox"/> FWD external permitted	<input type="checkbox"/> No group ringing on busy	
<input checked="" type="checkbox"/> Compress display data	<input type="checkbox"/> Central busy signaling	
<input checked="" type="checkbox"/> Entry in telephone directory	<input type="checkbox"/> Virtual station	Operating mode
<input type="checkbox"/> Edit tel. number	<input type="checkbox"/> Call prio./immed. tone call wait.	<input type="checkbox"/>
<input type="checkbox"/> Keypad dial	<input type="checkbox"/> Silent monitoring	Language
<input type="button" value="Apply flags to ..."/>		

- 1** Право на врывание в разговор; **2** Доступ к ассоциированному набору/сервисам; **3** Запрет второго вызова; **4** Использование гарнитуры с цифровым аппаратом; **5** Право на вызов аппарата с установленным режимом «не беспокоить»; **6** Сохранение списка потерянных вызовов; **7** Не используется; **8** Разрешение внешней переадресации; **9** Сжатие данных для дисплея цифровых телефонов; **10** Внесение во внутреннюю телефонную книгу; **11** Подтверждение набранного номера; **12** Возможность громкого вызова для данного цифрового телефона; **13** Перевод вызова на место сброса, если аппарат заблокирован; **14** Свойство авторизационного аппарата для функции DISA; **15** Право на транзитные соединения.

Задание:

1.Запустить приложение HiPath Manager E и провести первоначальные настройки.

2.Правильное извлечение и загрузка файла пользовательских настроек системы (KDS-файла).

3. Сконфигурировать абонентов системы и установить их параметры.

Практическая работа 7

Тема: Установка телефонных аппаратов и создание нумерационного плана на АТС

Цель работы: Практически изучить и уметь создавать нумерационный план с помощью программного продукта HiPath Manager E.

Практические навыки:

- безошибочного выполнения команд в программном продукте Siemens HiPath Manager E;

Продолжительность занятия – 2 ч.

Ход работы:



Инициализация станции под Россию с помощью ТА OptiPoint 500

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500.
2. Ввести User name и Password с помощью сервисного меню на ТА OptiPoint 500, инициализировать станцию под Россию в подменю «29».
3. После успешной перезагрузки проверить работоспособность станции и действующего нумерационного плана.

Выставление скорости порта V.24 и IP-адресов с помощью ТА OptiPoint 500

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500.
2. Ввести User name и Password с помощью сервисного меню на ТА OptiPoint 500.
3. С помощью сервисного меню на ТА OptiPoint 500 выставить IP-адрес сети, маску подсети и адрес шлюза, затем выставить скорость порта V.24= 19200 БОТ.
4. Проверить работоспособность скачиванием KDS в программном продукте HiPath Manager E.

Настройка IP-ТА OptiPoint 420 advance и подключение его к сети

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 и OptiPoint 420.
2. Создать IP-client в программном продукте HiPath Manager E:
 - в диалоговом окне Gatekeeper присвоить номер для IP-client;
 - проверить лицензии ComScendo;
 - сконфигурировать IP-транки в диалоговом окне IP tanks.
3. Настроить ТА OptiPoint 420 в сервисном меню, пароль по умолчанию 123456.
4. Перезагрузить сетевую плату HG 1500.
5. Проверить работоспособность IP-client со всеми видами связи.

Практическая работа 8

Тема: Конфигурирование исходящей связи в современных АТС

Цель работы: Изучить на практике механизм для настройки исходящей связи для различных целевых заданий в HiPath Manager E.

Практические навыки:

- настройки исходящей связи и конфигурирования групп;

Продолжительность занятия – 2 ч.

Ход работы:

Механизм **LCR** используется для настройки исходящей связи.

С его помощью определяются префиксы выхода на то или иное направление, способы набора цифр в линию.

Конфигурирование LCR состоит из 3-х шагов:

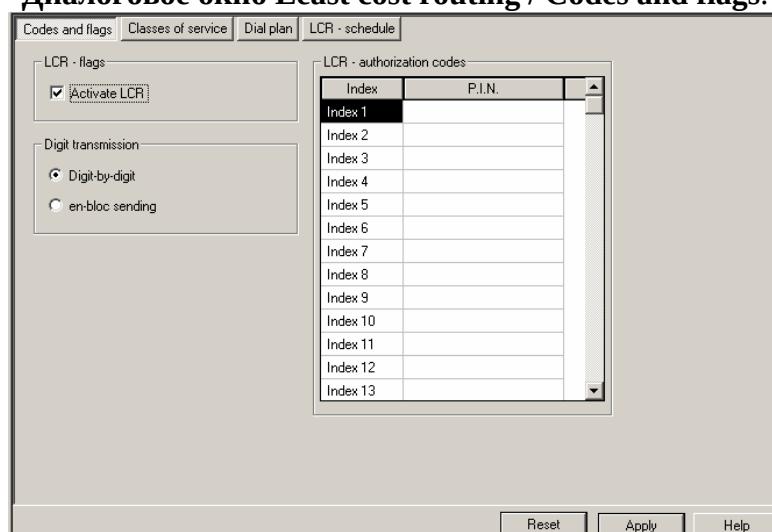
1. Определение соответствий между комбинацией цифр, набираемой абонентами и номером таблицы путей в таблице вкладки **Dial plan**.

2. Заполнение таблиц направлений соответствиями вида **Направление – имя правила набора**. Таблицы направлений содержаться во вкладке **Route table**.

3. Заполнение таблицы правил набора (вкладка **Dialing rules table**).

С помощью диалогового окна **Least cost routing / Codes and flags** активируется функция LCR в системе (переключатель **Activate LCR**), а также определяется тип набора цифр в линию.

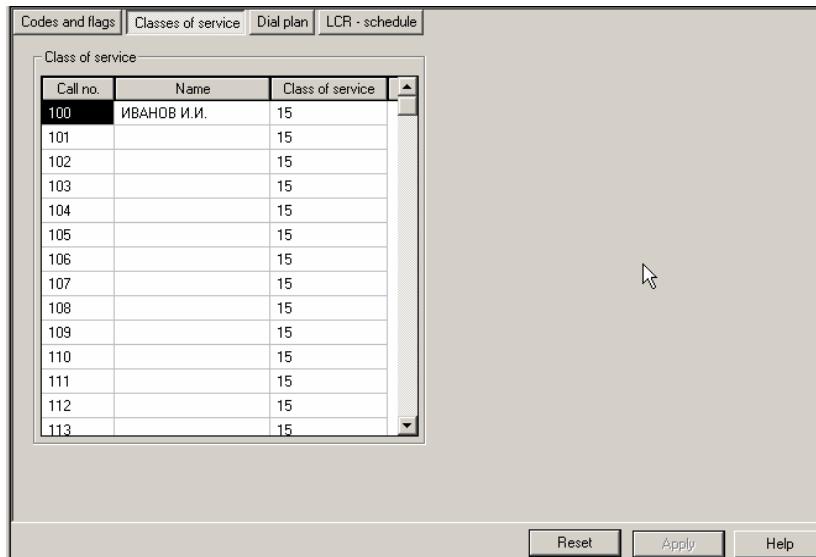
Диалоговое окно Least cost routing / Codes and flags.



Диалог **Least cost routing / Classes of service** позволяет для каждого абонента системы установить класс сервиса – право пользоваться конкретным направлением.

Для пользования линиями направления, класс сервиса, установленный для абонента, должен быть больше или равен значению поля **min COS** таблицы **Route Table** в окне **Dial Plan**, для данного направления (рис.2-18).

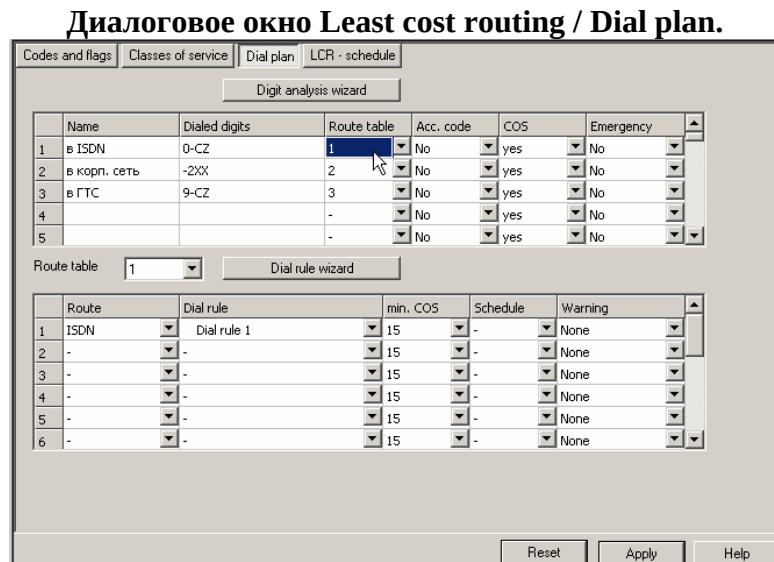
Диалоговое окно Least cost routing / Classes of service



В диалоговом окне **Least cost routing / dial plan** в верхней таблице устанавливается соответствие между комбинацией цифр , набранной пользователем (или пришедшей во входящем Setup) и таблицей **Route table**.

В нижней таблице этого диалогового окна описывается содержимое таблиц **Route table**. Каждая строка в этих таблицах описывает соответствие между направлением **Route** и правилом набора **Dial rule**.

На рисунке, набор, начинающийся на **0** –соответствует 1-й таблице **Route table**, набор, начинающийся на **2** –соответствует 2-й таблице **Route table**, на **9** –соответствует 3-й таблице **Route table**. Для редактирования записей какой либо таблицы **Route table**, необходимо в выпадающем списке выбрать номер таблицы **Route table**. (например 1). Далее, в таблице надо выбрать запись **Dial rule** для редактирования и нажать кнопку **Dial rule wizard**.



На рисунке показано окно конфигурирования правила набора **Dial rule1**.

Имя правила – поле **Edited dial rule**, само правило – поле **Rule format**.

Контролируемые комбинации цифр в **Dial plan** и форматы правил набора в **Dialing rules table** записываются в формульном виде.

например:

9-CZ : **9** – первое поле **CZ** – второе поле **-2XX** : первое поле пусто **2XX** - второе поле
Таблицы, описывающие знаки, применяемые в формулах, примеры.

Dial Plan		Dialing rules table	
знаки	назначение	знаки	назначение

	Разделитель полей			Набрать все в линию, кроме 1-го поля
	любая цифра между 0...9			Набрать цифры (от 1 до 25 цифр).
	любая цифра между 2...9			Набрать в линию поле № n
	симулированный тон набора			Пауза(от 1 до 60 единиц системных пауз)
	Одна или более цифр до конца набора			Переключиться в тоновый режим.
Пользовательский набор	Dial Plan/ Dialed digits	Dial rule wizard Dial Rule format	Набрано в линию	Примечание
91234567	9-CZ	A	1234567	Стандарт для городских линий (префикс выхода - 9)
91234567	9-CZ	E1A	91234567	Добавлен ие первого поля (9)
01234567	0-CZ	D9A	91234567	Добавлен ие цифры (9)
234	-2XX	A	234	Стандарт для корпоративной сети со сквозной нумерацией

Диалоговое окно Dial rule wizard.



Задание:

1. Запустить приложение HiPath Manager E и провести первоначальные настройки.
2. Настроить LCR, определить дальнейшее распределение вызова, настроить системные параметры.

Практическая работа 9

Тема: Исследование процедур классов сервиса и системных параметров в HiPath MANAGER E

Цель работы: Изучить процедуры классов сервиса, полномочия для групп (COS) и сконфигурировать системные параметры в HiPath Manager E.

Практические навыки:

- выставления всех параметров системы;
- выставления всех групп по правам (Классы сервиса);
- показа работы сконфигурированной станции.

Продолжительность занятия – 2 ч.

Ход работы:

Конфигурирование классов сервиса позволяет определять права пользования внешними линиями для различных абонентов.

Процедура включает три этапа:

1. Внесение конкретного абонента в одну из групп прав (**COS group**);
2. Определение полномочий данной группы на использование направлений (групп внешних линий, определенных в п. 6.1)
3. Создание листов разрешений и запретов (при тонкой настройке прав)

Распределение абонентов по группам прав (COS group).

В **Classes of service / COS: station** абоненты системы распределяются по группам прав.

На рисунке:

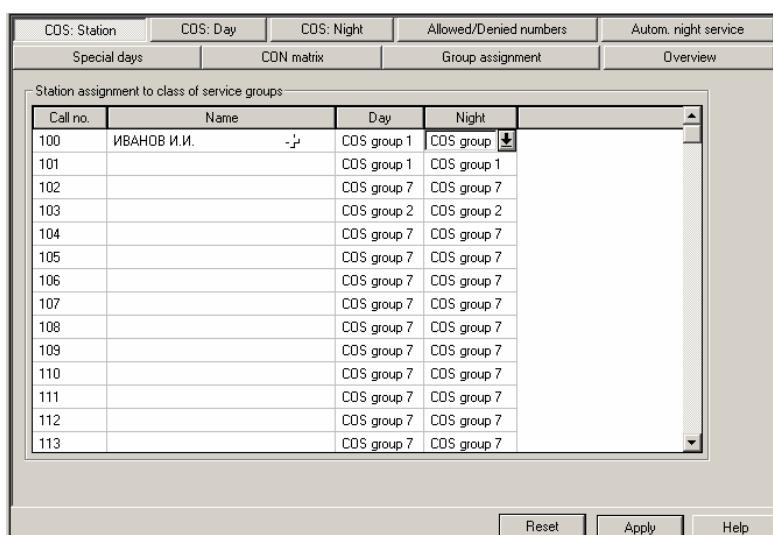
-абоненты №№ 100 и 101 внесены в **COS group 1**

-абонент № 103 внесен в **COS group 2**

-остальные абоненты внесены в **COS group 7**

Один и тот же абонент может быть в разных группах прав для дневного и ночного режимов работы системы.

Диалоговое окно **Classes of service / COS: station**.



Полномочия для групп прав (COS group).

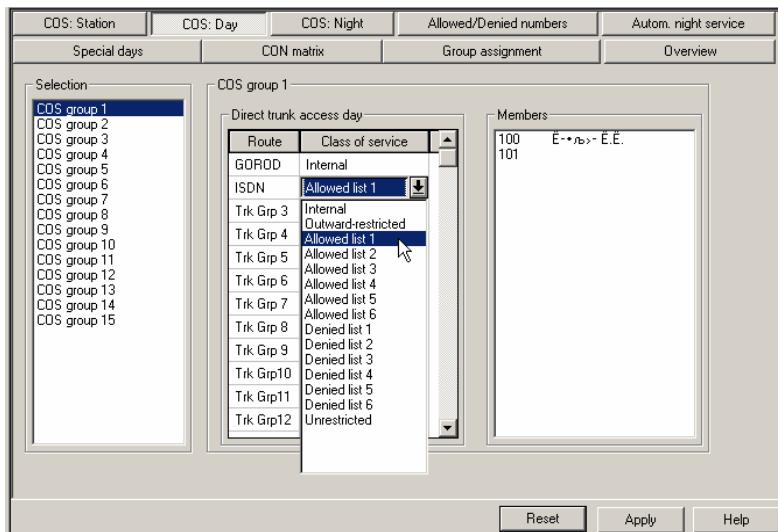
На рисунке показана процедура определения полномочий для группы **COS group 1**: В блоке **Direct Trunk access day** для этой группы: на направление **GOROD** право **Internal** на направление **ISDN** право **Allowed list 1**.

В таблице ниже описаны **назначения прав**.

Право	Назначение
-------	------------

Internal	Запрет входящей и исходящей связи
Outward-restrictive	Запрет исходящей связи
Allowed list1	Разрешены только наборы описанные в Allowed list1
Allowed list2	Разрешены только наборы описанные в Allowed list2
Allowed list3	Разрешены только наборы описанные в Allowed list3
Allowed list4	Разрешены только наборы описанные в Allowed list4
Allowed list5	Разрешены только наборы описанные в Allowed list5
Allowed list6	Разрешены только наборы описанные в Allowed list6
Denied list1	Запрещены только наборы описаные в Denied list1
Denied list2	Запрещены только наборы описаные в Denied list2
Denied list3	Запрещены только наборы описаные в Denied list3
Denied list4	Запрещены только наборы описаные в Denied list4
Denied list5	Запрещены только наборы описаные в Denied list5
Denied list6	Запрещены только наборы описаные в Denied list6
Unrestricted	Пользование направлением без ограничений

Диалоговое окно Classes of service / COS: Day.



Листы разрешений и запретов.

В **Classes of service / Allowed/Denied numbers** формируются листы разрешений и запретов, которые используются в **Classes of service / COS: Day** и **Classes of service / COS: Night**.

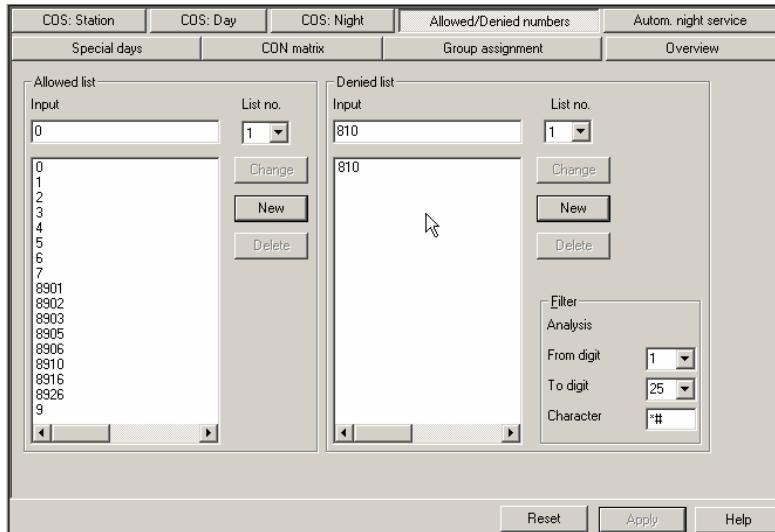
В примере на **рисунке** созданы 2 листа:

Allowed list 1 – позволяет набирать номера, начинающиеся на 0,1,2,3,4,5,6,7,9 и 8901, 8902, 8903, 8905, 8906, 8910, 8916, 8926;

Denied list 1 – запрещает набирать международные номера (810....);

Первый лист разрешений и первый лист запретов могут содержать до **100** элементов, остальные листы разрешений и запретов могут содержать не более **10** элементов

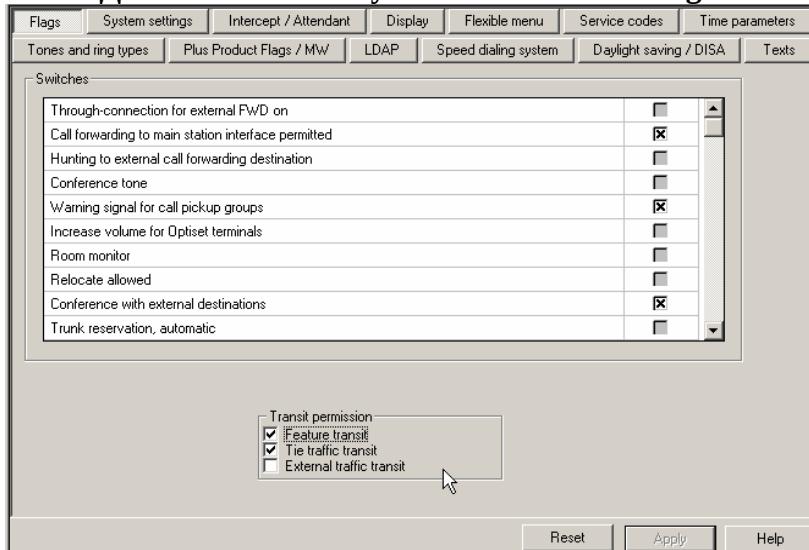
Диалоговое окно Classes of service / Allowed/Denied numbers.



Настройка системных параметров, флаги.

В данном диалоге описываются флаги общесистемных настроек. Наиболее употребляемые из них, описаны в таблице ниже.

Диалоговое окно System Parameters / Flags.



Флаг	Назначение
Call forwarding to main station interface permitted	Разрешение переадресации на аналоговые транки
Conference tone	Тон конференции у участников
Warning signal for call pickup groups	Тон внимания при вызове в группе перехвата
Increase volume for Optiset terminals	Альтернативная звуковая схема на цифровых ТА
Room monitor	Разрешение сервиса прослушивания
Conference with external destinations	Разрешение конференции с внешними целями
Trunk reservation, automatic	Резервирование транка (не работает с LCR)
Simplified dialing	Прямой набор внешних номеров с цифровых ТА (не работает с LCR)
Path optimization	Оптимизация маршрута вызова
DTMF automatic	Переключение транков в DTMF, после установления соединения
Automatic redial	Разрешает Автоматический повтор набора

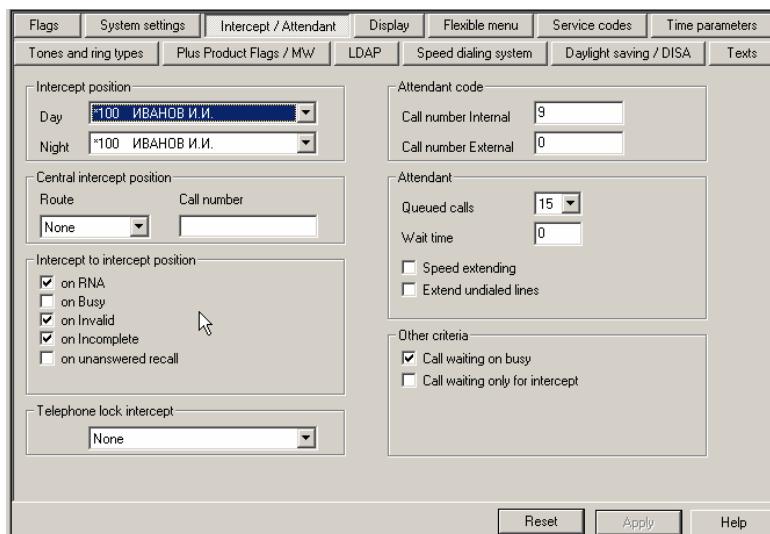
Call Pickup after automatic recall	Разрешает перехват обратного вызова
Configurable CLIP	Разрешает использование CLIP в Setup station

Настройка сброса.

Место сброса – телефонный аппарат/группа, на который распределяются вызовы, согласно определенным критериям.

В поле **Intercept position** описывается внутренний номер места сброса для дневного и ночных режимов работы системы.

Диалоговое окно System Parameters / Intercept/Attendant.



Критерии, распределения вызова на место сброса описывает поле **Intercept to intercept position**. Его значения описываются в таблице ниже.

Блок **Other criteria** содержит переключатели:

Call waiting on busy – разрешение второго вызова для всей системы.

Критерий	Значение
On RNA	При неответе
On Busy	При занятости
On Invalid	При неверном наборе
On Incomplete	При неполном наборе
On unanswered recall	При неотвеченном обратном вызове

Системные установки.

Блоки **Customer name** и **Contact number** могут содержать данные о владельце системы. Содержимое блока **System branding** будет отображено на экранах Optiset/Optipoint терминалов (в правом нижнем углу). Блок **Key click** определяет наличие и громкость озвучивания клавиш Optiset/Optipoint терминалов.

Блок **Hotline** определяет:

-Поле **Hotline** – номер горячей линии (1...6).

-Поле **Destination call number** – цель горячей линии (может быть внешней).

Если используется тип горячей линии «**Off-hook alarm...**», то поле **Off-hook** должно содержать время задержки (после поднятия трубки перед вызовом на место цели горячей линии).

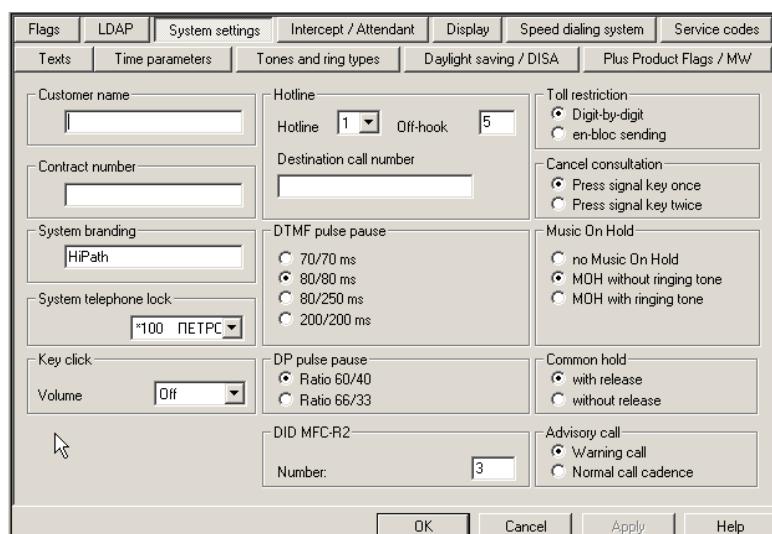
Блок **Music On Hold** содержит 3 радиокнопки, действия которых следующие:

- **no Music On Hold** - музыка на удержании отсутствует.

- **МОН without ringing tone** – при переадресации вызова,зывающему абоненту будет воспроизведется музыка на удержании до тех пор, пока абонент, которому вызов был переведен не поднимет трубку.

- **МОН with ringing tone** - при переадресации вызова,зывающему абоненту будет воспроизведется музыка на удержании до тех пор, пока переадресующий вызов абонент не положит трубку. Если переадресованный вызов так и не был принят, то вызов возвратится к переадресовавшему его абоненту.

Диалоговое окно System Parameters / System settings.



Задание:

1.Запустить приложение HiPath Manager E и провести первоначальные настройки.

2.Правильное извлечение и загрузка файла пользовательских настроек системы (KDS-файла).

3.Сконфигурировать абонентов системы и установить их параметры.

Практическая работа 10

Тема: Поиск минимальных маршрутов исходящей связи на АТС

Цель работы: Изучить на практике механизм поиска минимальных маршрутов исходящей связи для различных целевых заданий в HiPath Manager E.

Практические навыки:

- настройки исходящей связи;
- выставления всех параметров системы;

Продолжительность занятия – 2 ч.

Ход работы:

Настройка исходящей связи Least cost routing в двух направлениях на АТС.

1. Проверить работоспособность АТС HiPath 3000

и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 , OptiPoint 420 и Cordless.

2. Физически подключить аналоговую линию и цифровую линию к АТС через интерфейсы A/B и S2M.

3. Настроить исходящую связь для конфигурирования потока E1 с помощью диалогового окна Trunks и LCR в формульном виде -2xx и 0-cxx.

4. Проверить работоспособность потока E1 между АТС при LCR.

Настройка исходящей связи Least cost routing в двух направлениях на АТС.

1. Проверить работоспособность АТС HiPath 3000

и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 , OptiPoint 420 и Cordless.

2. Физически подключить аналоговую линию и цифровую линию к АТС через интерфейсы A/B и S2M.

3. Настроить исходящую связь для конфигурирования потока E1 с помощью диалогового окна Trunks и LCR в формульном виде -4xx и 9-cxx.

4. Проверить работоспособность потока E1 между АТС при LCR.

Настроить исходящую связь по нескольким направлениям (транки).

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 и OptiPoint 420.

2. Сконфигурировать в Lines/networking / Routes 8 направлений и выставить префиксы выхода. Каждому направлению присвоить имя.

3. Выполнить администрирование направлений, запретив отправку DID для 4 –х абонентов в цифровую сеть.

4. Проверить работоспособность станции.

Практическая работа 11

Тема: Формирование исходящей связи с помощью сложных префиксов на АТС

Цель работы: Изучить и освоить организацию исходящей связи с помощью сложных префиксов.

Практические навыки:

- правильной загрузки всех данных на станции HiPath 3000;
- конфигурации абонентов системы и установки их параметров.

Продолжительность занятия – 2 ч.

Ход работы:

Создать направление с префиксом выхода на городскую АТС - 9

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 и OptiPoint 420.

2. Сконфигурировать 5 направлений и выставить префиксы выхода.

3. Каждому из направлений присвоить имя.

4. Запретить отправку DID 3 абонентов в цифровую сеть (не отправлять DID в виде АОН).

5. После выставления префикса проверить работоспособность направления.

Создать направление с префиксом выхода на городскую АТС - 09

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 и OptiPoint 420.

2. Создать направление с префиксом выхода на городскую АТС – 09, используя вкладку Lines/networking / Routes, выставив префиксы выхода. Организовать 10 направлений. Каждому направлению присвоить имя.

3. Выставить префикс выхода префикс выхода на данное направление

4. Для 2-х направлений, используя переключатель Suppress station number запретить подключение абонента в цифровую сеть (не отправлять DID в виде АОН).
5. После выставления префикса проверить работоспособность направления.

Практическая работа 12

Тема: Создание АОН при исходящей связи разными способами

Цель работы: Практически изучить механизм поиска минимальных маршрутов исходящей связи для различных целевых заданий в HiPath Manager E.

Практические навыки:

- настройки исходящей связи;
- выставления всех параметров системы;

Продолжительность занятия – 2 ч.

Настройка протоколов для подключения цифрового потока E1 с АОН в Least cost routing на АТС

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500, OptiPoint 420 и Cordless.
2. Физически подключить цифровой поток между АТС по интерфейсам S2M.
3. Настроить исходящую связь для конфигурирования потока E1 с помощью диалогового окна Trunks и LCR.
4. Настроить нужные внешние протоколы с помощью диалогового окна Parameter (Trunks) и глубокого кода в экспертном варианте администрирования.
5. Проверить работоспособность потока E1 между АТС при LCR.

Настройка протоколов для подключения цифрового потока E1 с АОН на АТС.

1. Проверить работоспособность АТС HiPath 3000 и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500, OptiPoint 420 и Cordless.
2. Физически подключить цифровой поток между АТС по интерфейсам S2M.
3. Настроить исходящую связь для конфигурирования потока E1 с помощью диалогового окна Trunks и Routs (простейшая исходящая связь).
4. Настроить нужные внешние протоколы с помощью диалогового окна Parameter (Trunks) и глубокого кода в экспертном варианте администрирования.
5. Проверить работоспособность потока E1 между АТС при обычной исходящей связи.

Практическая работа 13

Тема: Сокращённый набор и тарификация с помощью ПО HiPath MANAGER E в HiPath 3000

Цель работы: С помощью программного продукта HiPath Manager E изучить применение сокращённого набора в АТС и настройку тарификации.

Практические навыки:

- конфигурации таблицы быстрого набора;
- правильности заполнения в диалоговых окнах тарификации.

Продолжительность занятия – 2 ч.

Ход работы:

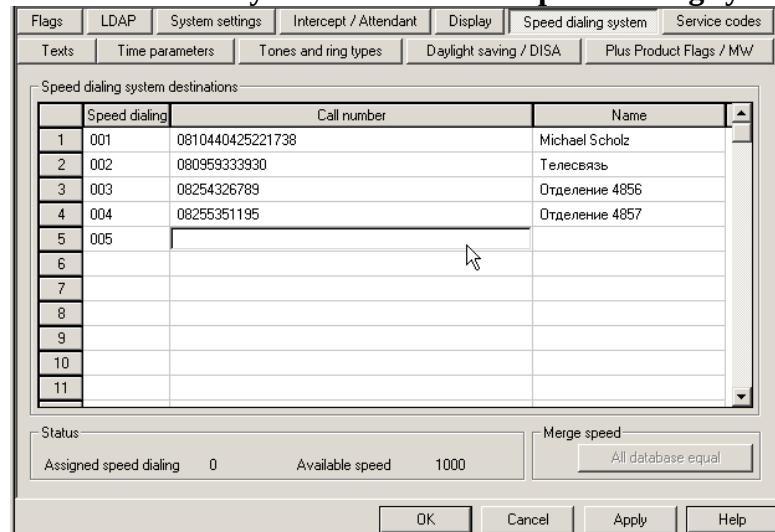
Сокращённый набор

В системах HiPath 3000 предусмотрена общестанционная телефонная книга.

В этой телефонной книге можно внести номера абонентов, организаций и т.п., доступ к набору которых пользователи системы могут получить с помощью кода *7 + № ячейки, содержащей нужный телефонный номер.

Использование общестанционной телефонной книги позволяет существенно облегчить набор часто используемых и/или длинных (напр. Междугородных или международных) телефонных номеров.

Диалоговое окно System Parameters / Speed dialing system



В примере, приведенном на рис., для набора международного номера (строка 1) достаточно набрать на телефонном аппарате код ***7 001**.

Если набор осуществляется с цифрового телефона аппарата (Optiset/Optipoint/OpenStage), то на экране отобразится содержимое поля **Name** соответствующей ячейки.

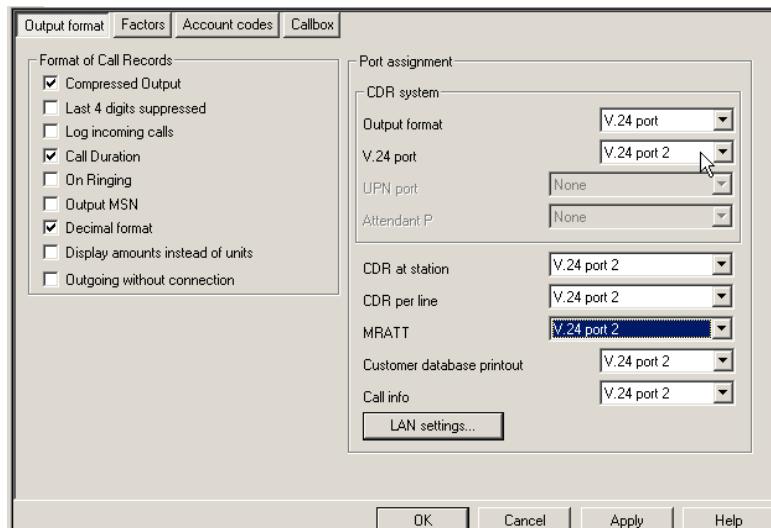
Данные, находящиеся в общестанционной телефонной книге можно предельно просто реплицировать на другие системы (напр. Копировать – вставить).

Тарификация.

В системах HiPath 3000 предусмотрено несколько способов учета длительности исходящих и входящих вызовов:

- вывод тарификационных данных на порт V.24 системы;
- вывод тарификационных данных в файл на TFTP-сервере (этот способ возможен только при наличии в системе модуля HG1500 либо модуля LIM);

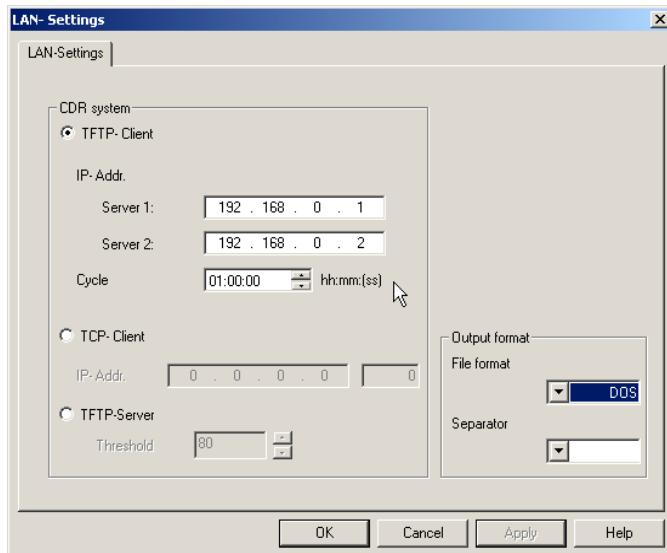
Диалоговое окно Call charges.../Output format



На рис. показаны настройки тарификации для вывода на порт V.24. Для вывода тарификационных данных в файл на TFTP-сервере, поле **Output format** блока **CDR systems**

должно содержать значение «**LAN-TFTP-client**». Также должны быть указаны IP-адреса TFTP-серверов в диалоговом окне **LAN-Settings**, доступ к которому можно получить нажав кнопку **LAN-Settings...**

Диалоговое окно LAN-Settings



Внимание: после настройки выдачи данных система должна быть перезагружена!

Задание:

- 1.Запустить приложение HiPath Manager E и провести первоначальные настройки.
- 2.Сконфигурировать таблицу сокращённого набора и проверить на практике.
- 3.Настроить тарификацию разными способами.

Практическая работа 14

Тема: Создание групп перехвата на АТС и их применение

Цель работы: С помощью программного продукта HiPath Manager E уметь создавать группы перехвата на АТС и их применять.

Практические навыки:

- создания направления с параметрами;
- конфигурирования линий.

Продолжительность занятия – 2 ч.

Ход работы:

Конфигурирование групп перехвата.

Абоненты системы HiPath 3000 могут принимать вызовы, приходящие на другие телефонные аппараты (перехватывать вызовы). Создание групп «перехвата» позволяет членам данной группы перехватывать вызовы внутри группы. Группы «перехвата» конфигурируются в диалоге **Incoming calls/ Call Pickup**.

В системах HiPath 3000 может быть до 32 групп «перехвата». В данном примере абоненты 100 – 104 включены в группу 1. «Перехват» в группе осуществляется с помощью кода *57. В системах HiPath 3000 существует, также, возможность директивного «перехвата» вызова («перехват» вызова **вне** группы перехвата).

Директивный «перехват» осуществляется с помощью кода *59 + № абонента.

Задание:

1. Правильная загрузка всех данных на станции HiPath 3000.
2. Безошибочное выполнение команд в программном продукте Siemens HiPath ManagerE.
3. Выставление всех параметров системы.
4. Правильносозданные направления с параметрами.
5. Показать работу сконфигурированных линий.

Практическая работа 15

Тема: Создание групп поиска на АТС и их применение

Цель работы: С помощью программного продукта HiPath Manager E уметь конфигурировать группы поиска на АТС и их применять.

Практические навыки:

- правильной загрузки всех данных на станции HiPath 3000;
- безошибочного выполнения команд в программном продукте Siemens HiPath Manager E;
- конфигурирования линий.

Продолжительность занятия – 2 ч.

Ход работы:

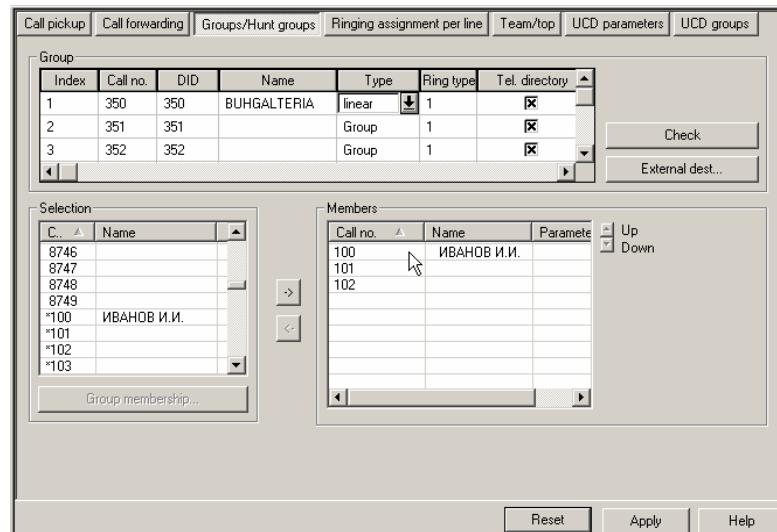
Группы поиска (Hunt groups).

Группы поиска предназначены для осуществления вызовов одновременно на несколько ТА, а также для последовательного, либо циклического «обзвона» группы ТА.

Конфигурирование групп поиска осуществляется в диалоге **Incoming calls / Groups/Hunt groups**.

В приведенном примере сконфигурирована группа №350, членами которой являются абоненты №№100,101,102 (таблица **Members**). Группа имеет имя «BUHGALTERIA». Вызов,

осуществленный в данную группу, будет линейно распределен на аппараты №№100,101,102. (последовательно, сначала на №100, затем на №101,затем на №102).



1.Call.no -Внутренний номер

2.DID -Номер, адресующий группу в цифровой сети

3.Name -Имя группы (необязательно)

4.Type- Тип:

Group – одновременный вызов

Linear – последовательный «обзвон» группы

Cyclic – циклический «обзвон» группы

5.Ring type- Тип вызывного сигнала на ТА группы.

Количество вызывных сигналов на каждом ТА при линейном/циклическом типе группы, определяется номером списка в таблице **Calldest list. – Station Assignment**, присвоенном данной группе и полем **Cycles** в таблице **Calldest list. – Definition** вкладки **Call Forwarding**.

Задание:

1. Правильная загрузка всех данных на станции HiPath 3000.
2. Безошибочное выполнение команд в программном продукте Siemens HiPath ManagerE.
3. Выставление всех параметров системы.
4. Правильно созданные направления с параметрами.
5. Показать работу сконфигурированных линий.

Практическая работа 16

Тема: Создание шеф/секретарских групп и их применение

Цель работы: С помощью программного продукта HiPath Manager E уметь создавать шеф/секретарские группы на АТС и их применять.

Практические навыки:

- выставления всех параметров системы;
- создания направления с параметрами;
- конфигурирования линий.

Продолжительность занятия – 2 ч.

Ход работы:

Функции шеф-секретарь

Данные функции обеспечивают быструю коммуникацию между шефом и секретарем.

- Сигнализация второго вызова на аппарате шефа с телефона секретаря
- Схема замещения (на временное отсутствие)
- Переключение соединения на аппарат секретаря
- Клавиши прямой связи на аппаратах шефа и секретаря
- Второй телефон с параллельной сигнализацией вызова на основной аппарат шефа
- Личная линия для шефа или секретаря

Сконфигурировать секретарскую группу Team/Top group

1. Проверить работоспособность АТС HiPath 3000

и модулей на станции, а также наличие подключённых телефонных аппаратов OptiPoint 500 и OptiPoint 420.

2. Сконфигурировать секретарскую группу на 8 номеров.

3. Загрузить KDS в систему.

4. Проверить работоспособность группы.

Практическая работы № 17

Тема: Загрузка новой версии программного обеспечения на АТС

1. Цель работы:

Освоить и проанализировать работу модулей шлюза VoIP и функциональных возможностей.

2. Подготовка к работе:

2.1. Иметь знания в области ИТ.

2.2. Знать топологию модели взаимодействия открытых систем.

2.3. Иметь наработки в ПО HiPath Manager E.

3. Перечень оборудования:

3.1. ТСПИ со слаботочными системами.

3.2. Станции фирмы Siemens HiPath 3800, HiPath 3500.

3.3. TA OptiPoint XXX, OpenStage XX, Gigaset XXX.

4. Задание:

4.1. Изучить теоретические аспекты маркировки модулей, плат шлюза VoIP .

4.2. Установить и запустить плату HG 1500.

4.3. Проверить правильность загрузки и описать возможности.

5. Указания к выполнению практической работы:

5.1. Теоретическая часть.

Возможные применения HG 1500 v3.0 в составе HiPath 3000

STMI2, HXGM3, HXGS3 и HXGR3 - модули шлюза VoIP (VoIP - Voice over IP, передача голоса поверх протокола IP), которые обеспечивают функциональные возможности HiPath HG1500, версия 3.0 в HiPath 3750/00 (HXGM3), HiPath 3550 и HiPath 3350 (HXGS3) и HiPath 3500, HiPath 3300 (HXGR3):

VoIP в HiPath 3000

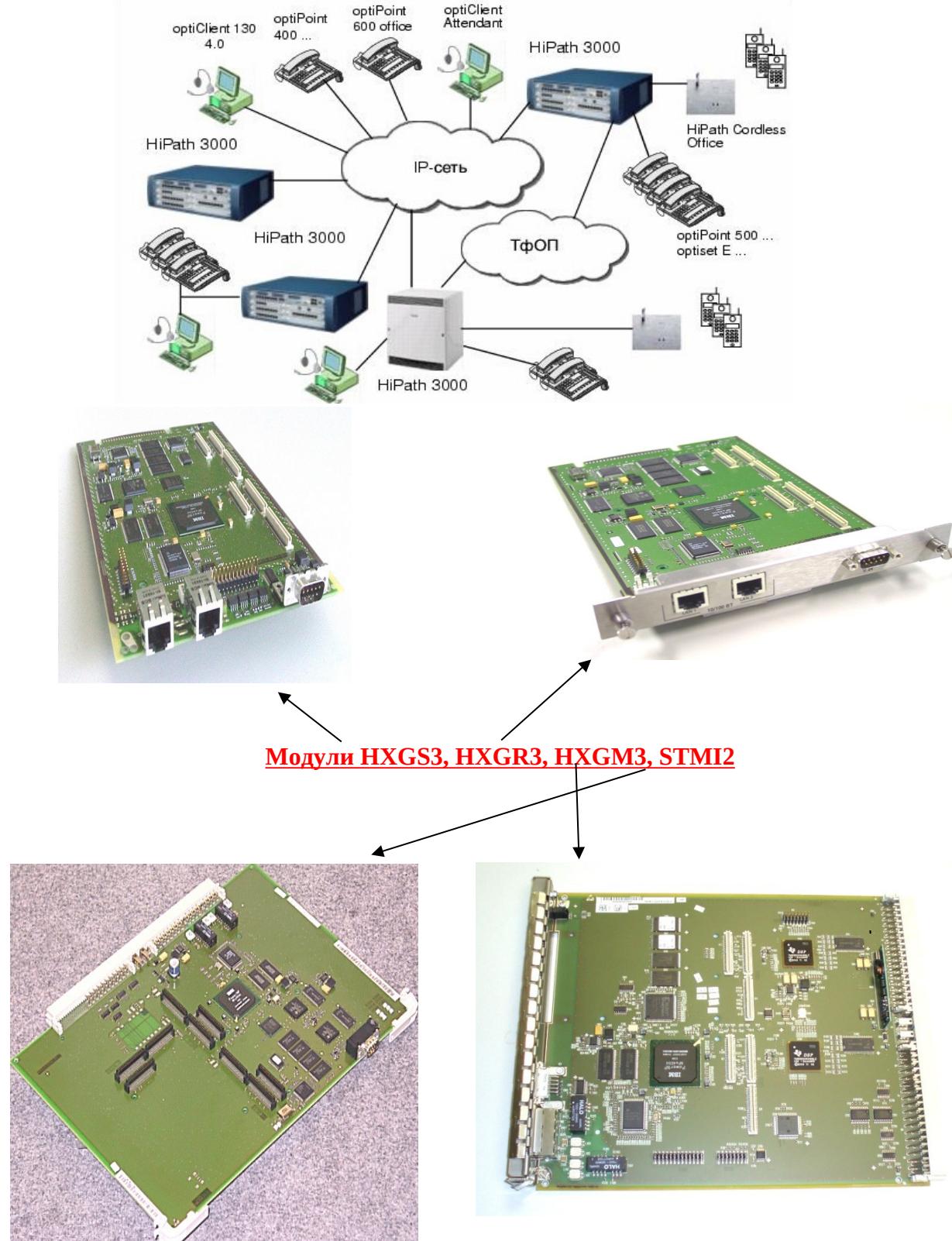
1.Подключение местной LAN к HiPath 3000 и соединение с внешними LAN через интерфейсы ISDN.

2.Поддержка классических функций маршрутизатора ISDN с дополнительными функциональными возможностями медиашлюза для передачи голоса, факсов и данных.

3. Ретрансляция голосовых соединений между сетями, использующими протокол IP (LAN, Инtranet, Интернет), и сетями с коммутацией каналов (ЦСИС (ISDN), ТфОП (PSTN)). С версии 3.0 HiPath HG1500 для конфигурирования вместо HiPath 3000 Manager используется управления на базе Web (WBM). Такой подход позволяет управлять HiPath HG1500 без специального программного обеспечения.

Процедуры начального конфигурирования модулей производится при помощи терминальной программы и прямого подключения к порту V.24 соответствующего модуля.

В системе должен быть установлен Internet Explorer v5.5 и выше, Java plug-in JRE 1.3.1 или выше, MS XML Extension DLL V3.0 SP2 or SP4.



Разъемы для доп. Модулей

Модуль **HXGS3** устанавливается в системы **3550** (max.3) и **3350** (max.1)

Модуль **HXGR3** устанавливается в системы **3500** (max.3) и **3300** (max.1)

Физические интерфейсы LAN1 и LAN2 для модулей HXGM3 реализуются с помощью **LAN-адаптеров**, устанавливаемых в разъемы задней панели систем 37XX, соответствующие установленному модулю HXGM3.

Физические интерфейсы LAN1 и LAN2 для модулей STMI2 , а также интерфейс V.24 расположены на передней панели.

В системе HiPath 3800 может быть установлено до восьми модулей STMI2, однако, при этом должны быть соблюдены следующие условия:

- Не более 4-х модулей STMI2 на бокс системы;

-Слот между двумя модулями STMI2 должен оставаться свободным.

Модуль STMI2 поддерживает **max. 32** одновременных телефонных разговора.

Модуль HXGM3 поддерживает **max. 16** одновременных телефонных разговоров.

Модули HXGS3 и HXGR3 поддерживают **max. 8** одновременных телефонных разговоров.

С помощью дополнительного модуля **PDM1**- можно увеличить количество одновременных телефонных разговоров через модули **HXGM3, HXGS3 и HXGR3** на 8 разговоров.

Модули **HXGS3** и **HXGR3** поддерживают **max. один** доп. модуль **PDM1**, при этом, количество телефонных разговоров через модуль увеличивается до **16**.

Модуль **HXGM3** поддерживает **max. два** доп. модуля PDM1, при этом количество одновременных телефонных разговоров увеличивается до **32**.

Функциональность модуля **STMI2** может быть расширена с помощью доп.модуля **PDMX**. Однако, в данный момент применение модуля **PDMX** не разрешается.

Модуль PDM1 может быть установлен в слот **HGA Slot0** на модулях HXGS3, HXGR3.

Модули PDM1 могут быть установлены в слоты **HGA Slot0 и HGA Slot2** на модуле HXGM3.

Слот **HGA Slot1** зарезервирован для будущих применений.

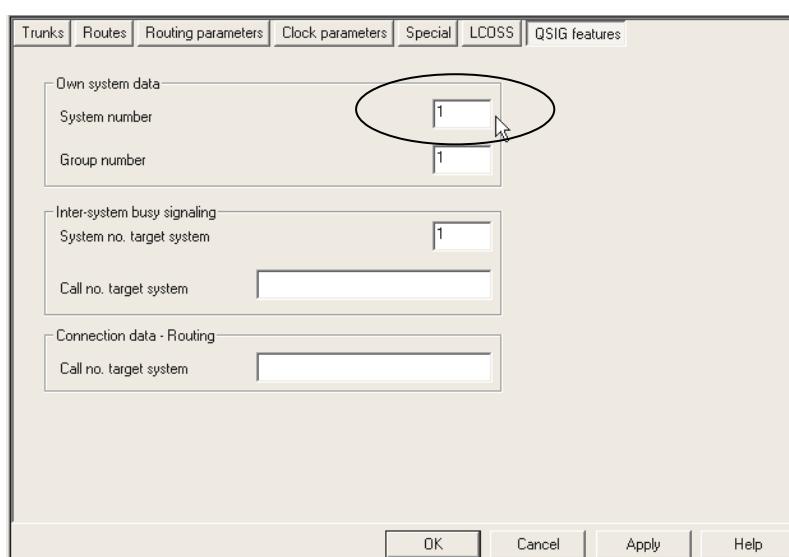
Внимание. Модули HG1500 V5.0 не поддерживают горячую замену.

При установке, извлечении или апгрейде модулей, **система должна быть обесточена**.

5.2. Настройка системы в программе HiPath3000 Manager E.

В **Lines/networking → QSIG futures** в поле **Sistem number** присвоить системе **Node ID** – уникальный в сети номер, однозначно определяющий данную систему.

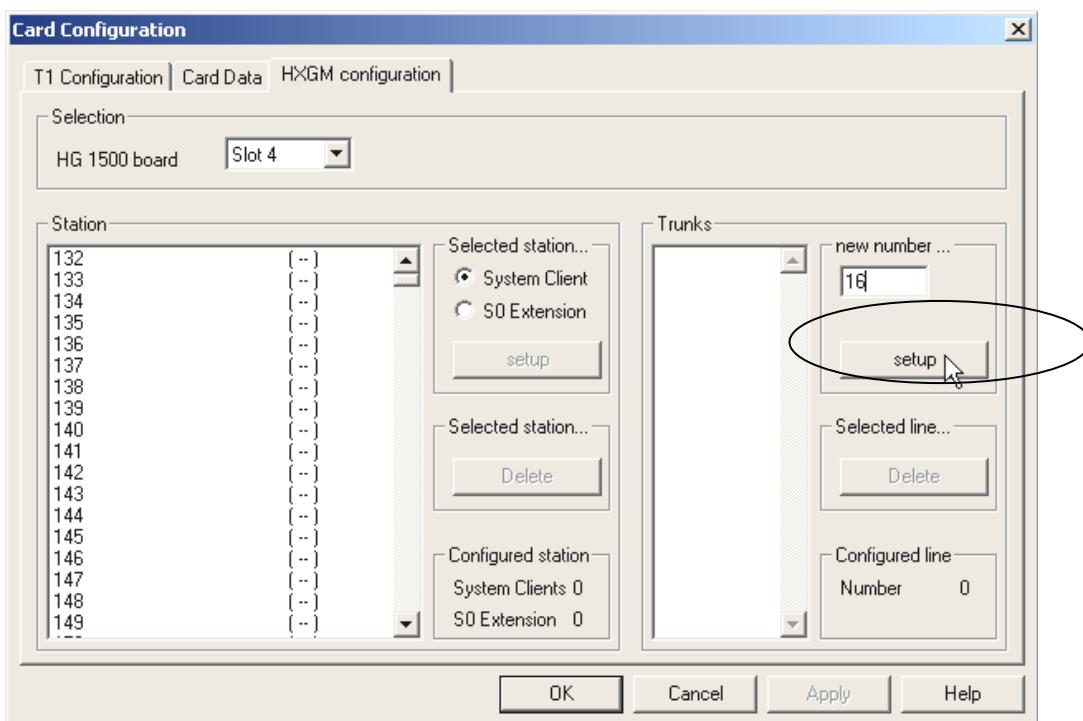
Назначение Node ID



В System-wide → cards нажать кнопку **SW expansion**, затем нажать кнопку **Card Config.** для вызова диалога **Card Configuration**.

В открывшемся диалоге перейти на вкладку **HXGM configuration** и в поле **new number...** внести необходимое число IP-транков, после чего нажать кнопку **Setup**.

Добавление IP-транков.



Соответствующее количество транков появится в поле **Trunks**.

6. Итог выполнения практической работы:

- 1.Правильная загрузка всех данных на станции HiPath 3000.
- 2.Безошибочное выполнение команд в программном продукте Siemens HiPath MenegerE.
- 3.Выставление всех параметров системы.
- 4.Инициализация и первичная настройка HG 1500.

7. Учебно-методическое и информационное обеспечение дисциплины

Комплект учебно-методической документации

- интерактивные программы обучения;
- мультимедийные презентации по темам МДК;
- обучающие программы, эмуляторы, используемые для изучения монтажа, эксплуатации и технического обслуживания телекоммуникационных систем с коммутацией каналов;
- система программированного контроля знаний;
- видеофильмы по темам МДК;
- методические указания по выполнению лабораторных работ (в электронном виде и практикум).

Базы данных, информационно-справочные и поисковые системы

<http://www.twirpx.com/>

<http://www.kafvt.narod.ru/Osia/frameset.htm>

<http://ngnetwork.ru/category/koncepciya-ngn/page/2/>

http://www.informsviaz.ru/inform_tech/617.html

<http://www.siemens.com>

Практическое занятие №18

Тема: Настройка удаленного доступа

Цель работы

Научиться производить настройку VPN-соединения

Оборудование: компьютерный класс

Задание

Аббревиатура VPN расшифровывается как Virtual Private Network – “виртуальная частная сеть”. Суть этой технологии в том, что при подключении к VPN серверу при помощи специального программного обеспечения поверх общедоступной сети в уже установленном соединении организуется зашифрованный канал, обеспечивающий высокую защиту передаваемой по этому каналу информации за счёт применения специальных алгоритмов шифрования.

В общем случае VPN - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую виртуальную (наложенную) сеть, обеспечивающую секретность и целостность передаваемой по ней информации (прозрачно для пользователей).

Использование технологии VPN необходимо там, где требуется защита корпоративной сети от воздействия вирусов, злоумышленников, просто любопытных, а также от других угроз, являющихся результатом ошибок в конфигурировании или администрировании сети.

Виртуальные частные сети (VPN), создаваемые на базе арендаемых и коммутируемых каналов связи сетей общего пользования (и, в первую очередь, Интернет), являются отличной альтернативой изолированным корпоративным сетям, причем, альтернативой, обладающей рядом несомненных преимуществ:

- низкая стоимость арендаемых каналов и коммуникационного оборудования;
- развитая топология сети (широкий географический охват); высокая надежность;
- легкость масштабирования (подключения новых сетей или пользователей); легкость изменения конфигурации;
- контроль событий и действий пользователей.
- Какими свойствами должна обладать VPN?

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе сети общего пользования, в виртуальную частную сеть:

- шифрование
- аутентификация
- контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий. Ниже приведены примеры реализации решений путем применения технологии VPN

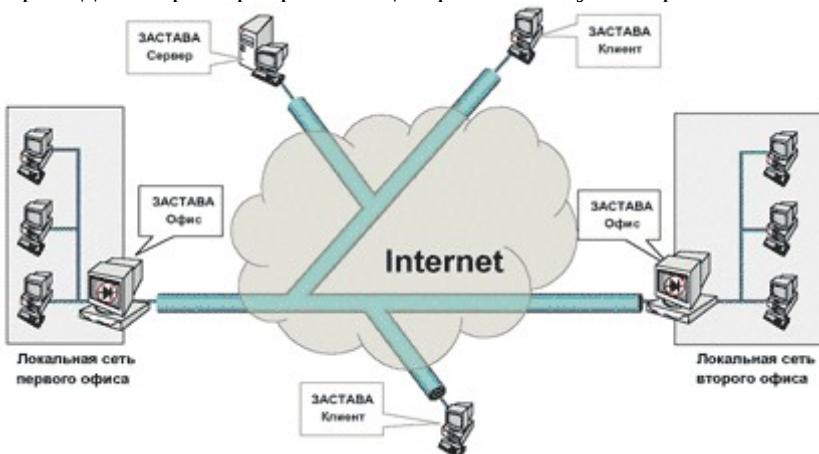


Рис. 1 Пример решения, позволяющий объединить территориально разнесенные ЛВС, удаленный сервер и удаленных клиентов

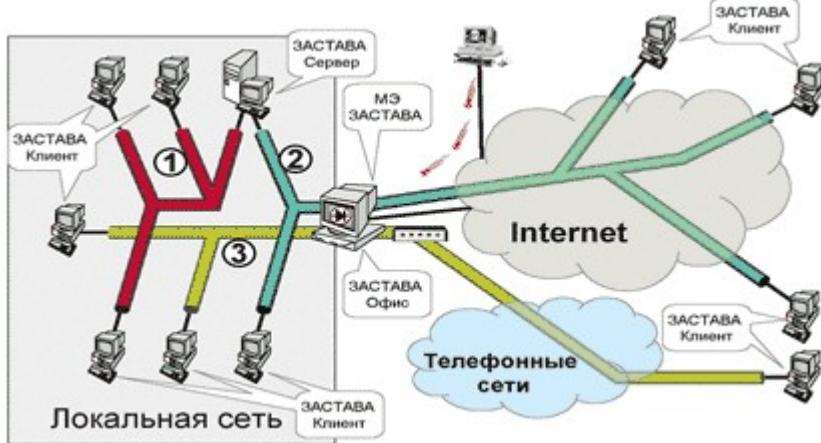


Рис. 2. Более сложный пример создания VPN сегментов

Цветом и, соответственно, цифрами выделены непересекающиеся VPN подсети с различными технологиями доступа к ресурсам. Таким образом, решается не только задача организации защищенных удаленных соединений, но и задача сегментирования ЛВС на информационно непересекающиеся подсети.

Порядок выполнения задания

Настройка VPN-соединения в Windows XP должна выполняться из под учетной записи пользователя, имеющего права администратора. Если вы выполнили вход в Windows как пользователь, не имеющий прав администратора, завершите сеанс этого пользователя и войдите в Windows как администратор (или как пользователь, обладающий правами администратора).

1. Создание VPN-соединения

Убедитесь, что запущены следующие службы Windows XP ("Пуск" - "Панель управления" - "Администрирование" - "Службы"): "Телефония"; "Диспетчер автоподключений удаленного доступа"; "Диспетчер подключения удаленного доступа".

Запустите мастер новых подключений. Для этого нажмите кнопку "Пуск" на панели задач, в открывшемся меню выберите пункт "Все программы" (либо просто "Программы", если вы перенастроили стандартное представление стартового меню), затем "Стандартные", "Связь", "Мастер новых подключений" (рис. 3).

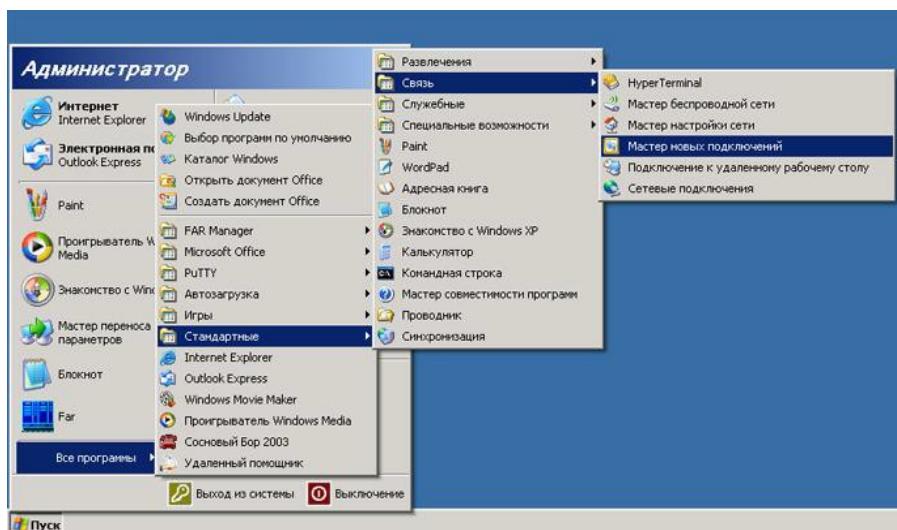
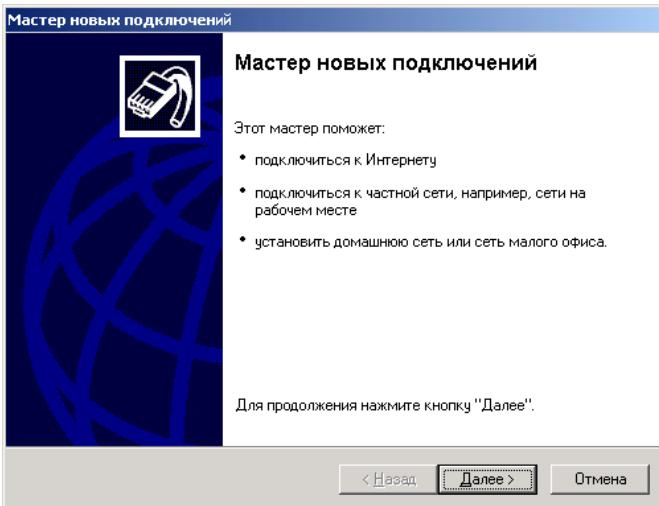
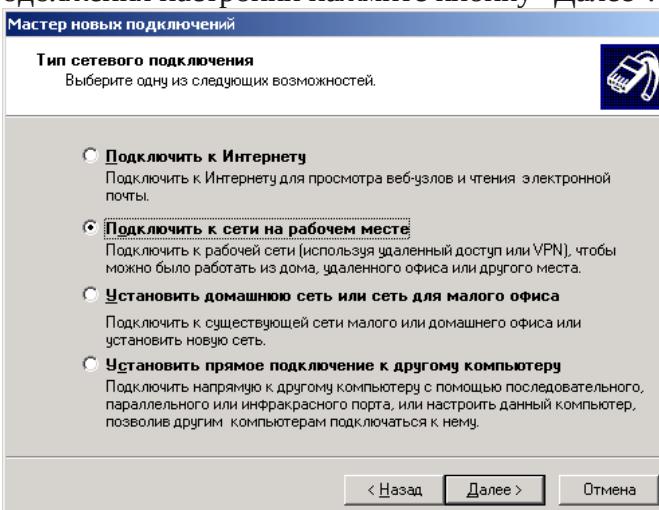


Рис. 3 Запуск программы "Мастер новых подключений"

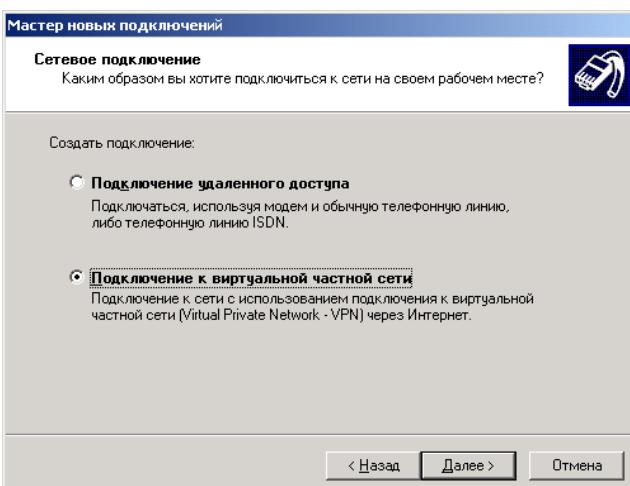
Первое диалоговое окно мастера новых подключений информирует о том, что с его помощью можно сделать. Чтобы приступить к созданию подключения нажмите кнопку "Далее" (рис. 4).



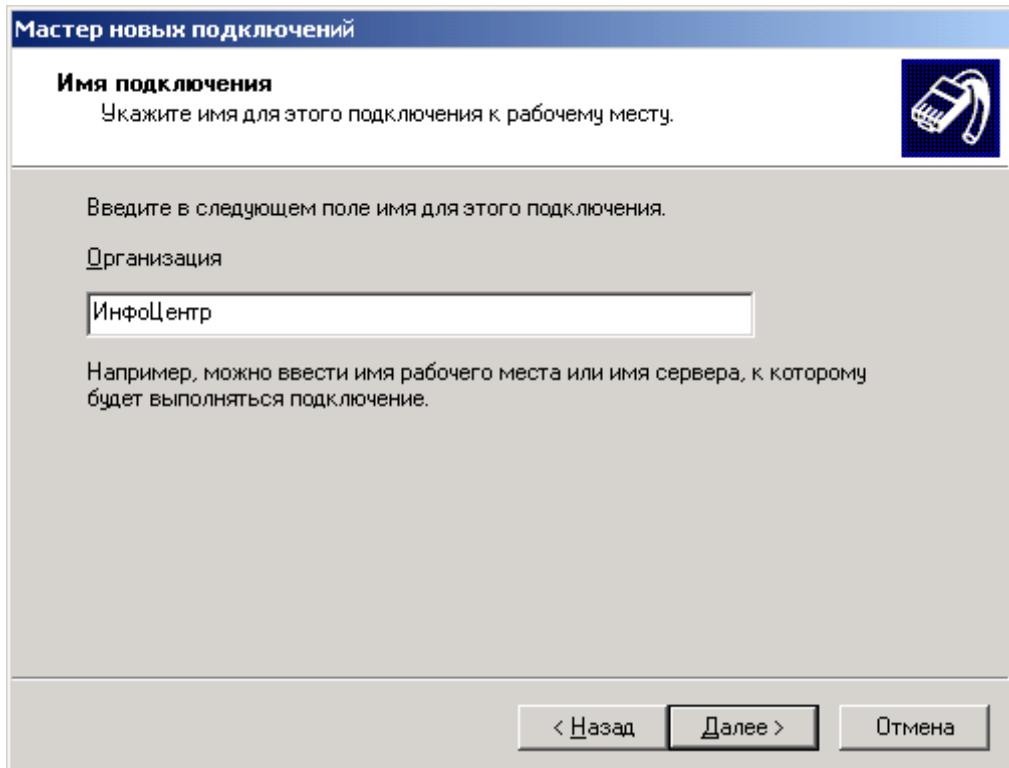
В следующем окне мастера новых подключений нужно выбрать тип сетевого подключения. В нашем случае нужно выбрать пункт "Подключить к сети на рабочем месте". Для продолжения настройки нажмите кнопку "Далее".



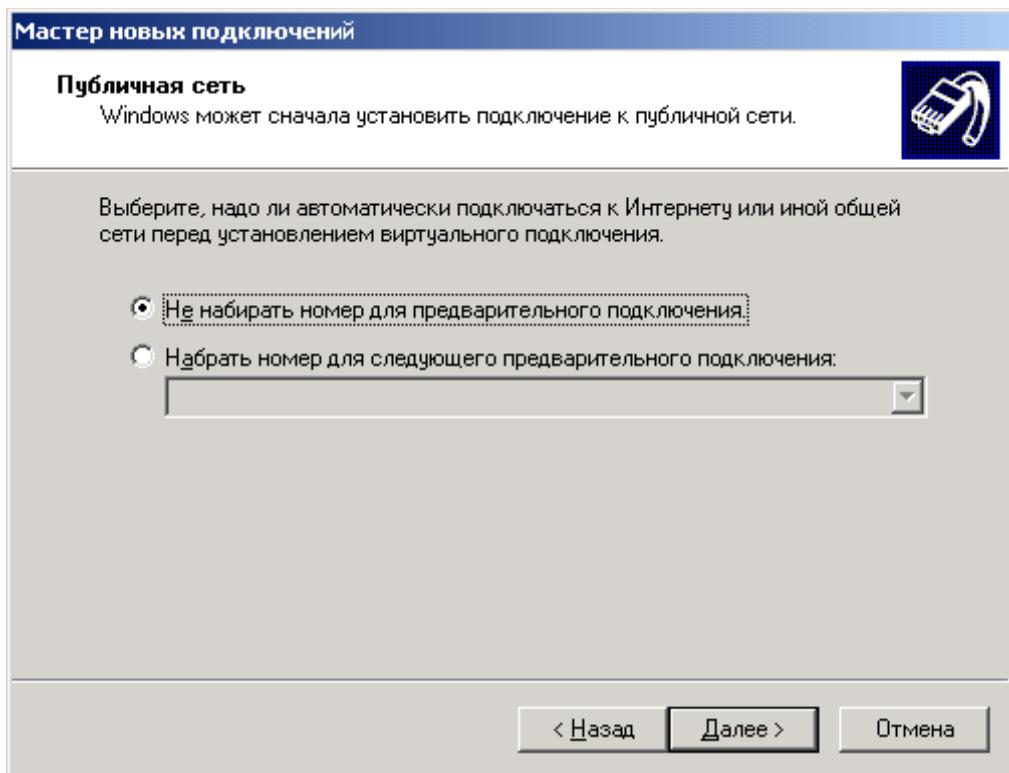
В следующем окне нужно выбрать способ подключения. В качестве способа подключения нужно указать пункт "Подключение к виртуальной частной сети" (рис. 5). Для продолжения настройки нажмите кнопку "Далее".



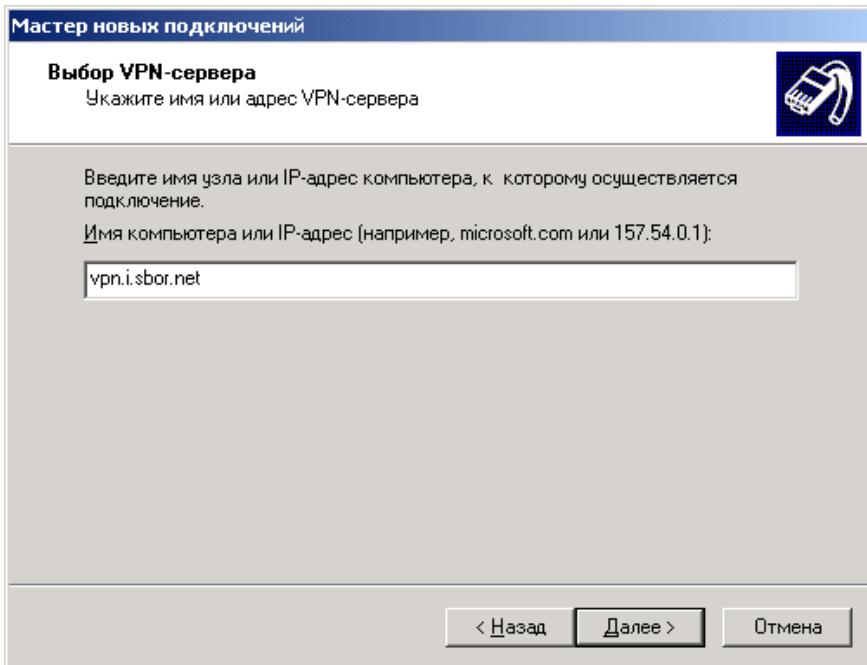
В следующем окне нужно ввести название для создаваемого подключения. Название может быть любым, например, "ИнфоЦентр". Для продолжения настройки нажмите кнопку "Далее".



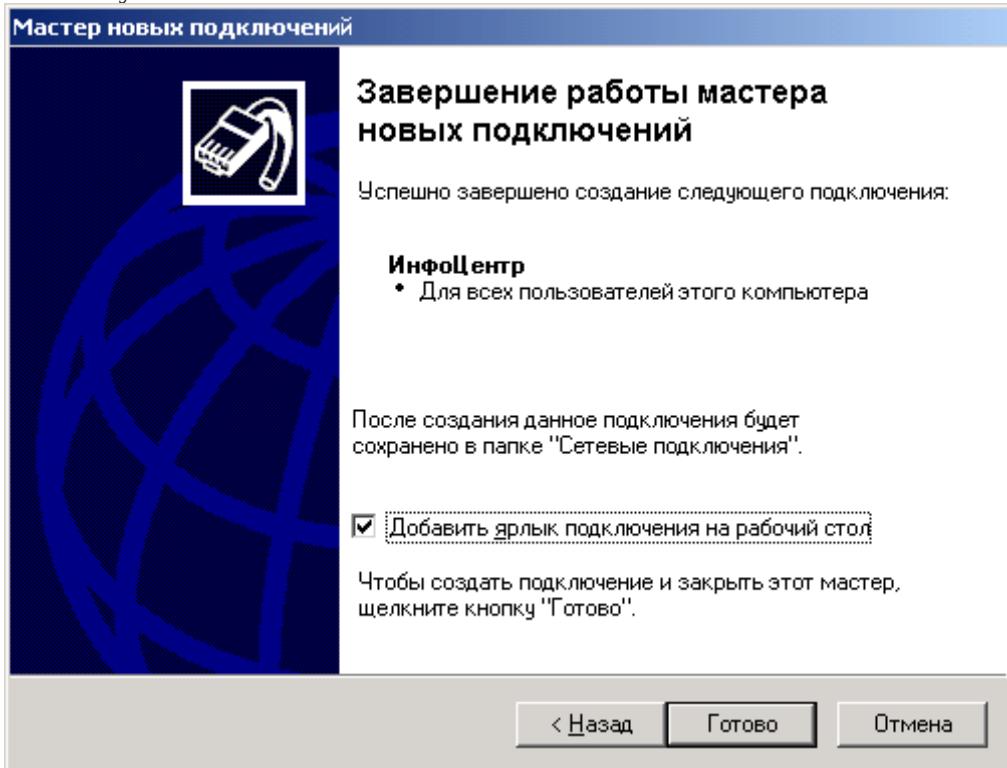
Окно, в котором предлагается выбрать, надо ли перед установкой этого соединения установить другое предварительное подключение, будет выводиться в том случае, если у вас уже создано сетевое подключение для соединения по модему. Если такое окно появилось, то нужно выбрать пункт "Не набирать номер для предварительного подключения" и нажать кнопку "Далее".



В следующем окне мастера новых подключений необходимо ввести имя или IP-адрес VPN-сервера. В качестве имени укажите **vpn.i.sbor.net**. Для продолжения настройки нажмите кнопку "Далее".

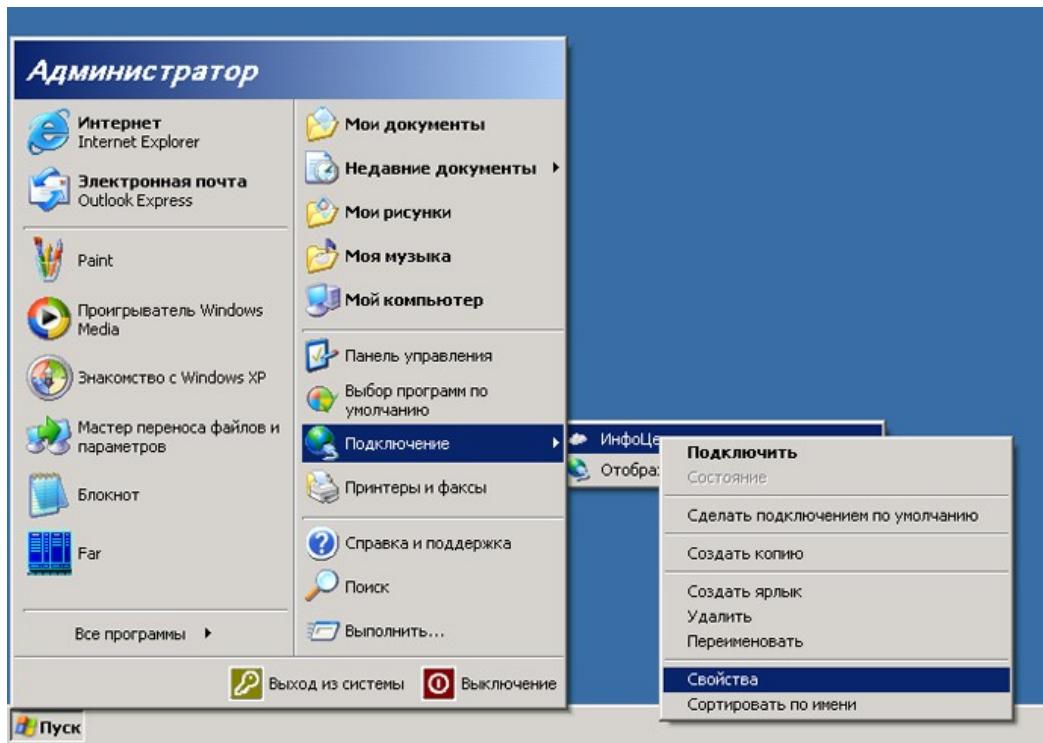


В последнем окне мастера новых подключений можно указать, что нужно создать ярлык на рабочем столе для созданного подключения. Для создания ярлыка необходимо, чтобы был включен соответствующий флажок (рис. 8). Для завершения создания соединения нажмите кнопку "Готово".

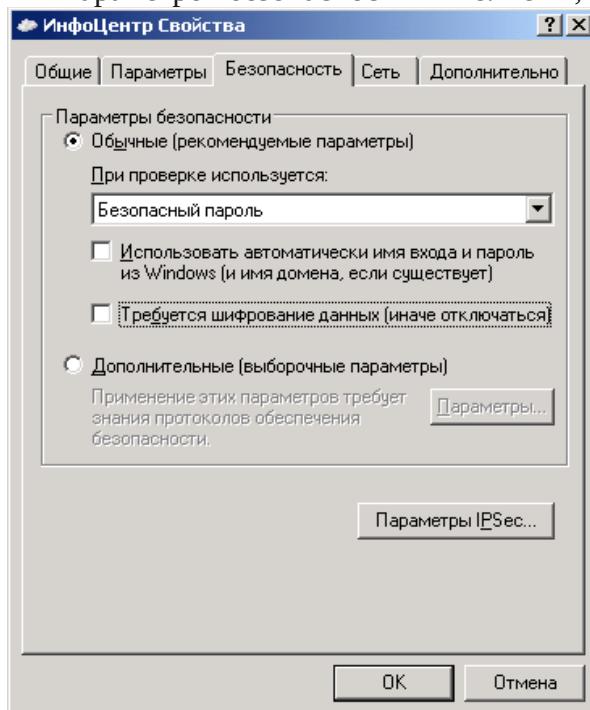


2. Дополнительные настройки

Вызовите свойства VPN-подключения. Для этого нажмите кнопку "Пуск" на панели задач, в открывшемся меню выберите пункт "Подключение". В меню со списком подключений кликните правой кнопкой мыши на созданном подключении и в открывшемся контекстном меню выберите пункт "Свойства"

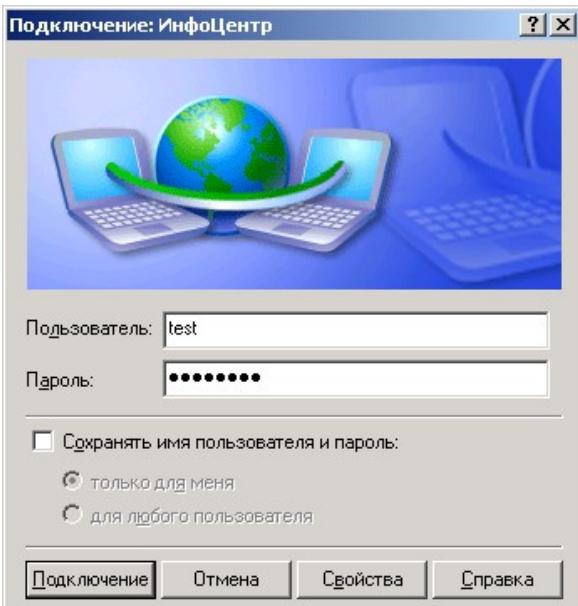


Откроется диалоговое окно с несколькими вкладками. Выберите вкладку "Безопасность" и выключите галочку "Требуется шифрование данных". В настройках проверки пароля должен быть выбран пункт "Безопасный пароль" (рис. 10). После того, как настройки параметров безопасности выполнены, нужно нажать кнопку "OK".

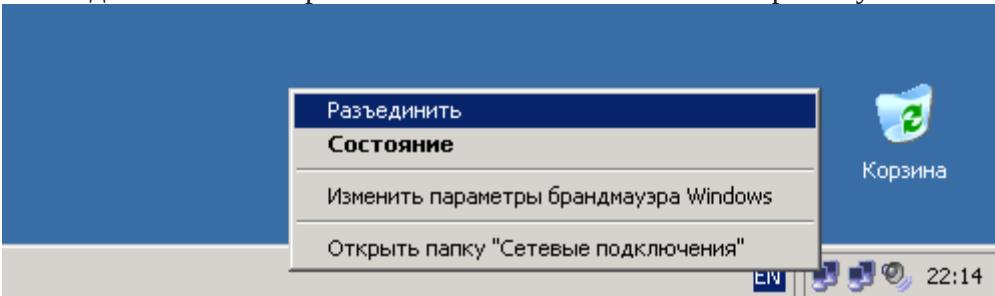


3. Подключение

Для того, чтобы установить VPN-подключение кликните на ярлыке VPN-подключения (предполагается, что при создании подключения включили флажок для создания ярлыка на рабочем столе). Откроется окно для ввода имени пользователя и пароля. В соответствующих полях ввода, введите имя пользователя и пароль для подключения по сети (такие же, как и на авторизацию) и нажмите кнопку "Подключение". После того, как соединение будет установлено, в системном трее (область значков) появится значок соединения.



Если вы желаете отключить VPN-соединение, нужно кликнуть правой кнопкой мыши на значке соединения и в открывшемся контекстном меню выбрать пункт "Разъединить"



5. Настройка маршрутизации

Если внутригородские ресурсы должны быть доступны при установленном VPN-соединении, необходимо задать явные маршруты к IP-сетям 10.0.0.0/8 и 91.203.168.0/27. Делается это следующим образом:

1. Отключите VPN-соединение, если оно у вас подключено.
2. Откройте окно с командной строкой. Для этого нажмите кнопку "Пуск" в панели задач, выберите пункт "Все программы", затем "Стандартные", затем "Командная строка".
3. Наберите команду **ipconfig** и нажмите клавишу "ENTER". В окне будет выведена информация о настройках IP-протокола. Запомните IP-адрес основного шлюза
4. Введите команды: **route -p add 10.0.0.0 mask 255.0.0.0 IP-адрес основного шлюза** **route -p add 91.203.168.0 mask 255.255.255.224 IP-адрес основного шлюза** Вместо **IP-адрес основного шлюза** нужно подставить IP-адрес, который вы запомнили в предыдущем пункте.

После добавления маршрутов, внутригородские ресурсы будут доступны вне зависимости от того, установлено у вас VPN-соединение или нет.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Презентацию с выполненным заданием

Контрольные вопросы

1. Что такое VPN?
2. Каковы достоинства применения этой технологии?
3. Каковы ограничения применения этой технологии?

Практическая работа №19

Тема: Объединение локальных сетей с помощью маршрутизаторов

Цель занятия: изучить принцип работы маршрутизатора на сетевом уровне

Теоретические выкладки

Маршрутизаторы объединяют сегменты LAN на сетевом уровне. Маршрутизация включает в себя два этапа: определение оптимальных маршрутов и передача пакетов по этим маршрутам. Оптимальность маршрута определяется на основе некоторого критерия в качестве которого могут выступать показатели скорости передачи, задержки, стоимости маршрутов. Исходя из численных значений критериев для каждого из известных маршрутов формируется таблица маршрутов. На основе этой таблицы и информации об адресе сетевого уровня, содержащихся в пересылаемом пакете, маршрутизатор осуществляет пересылку пакета по определенному маршруту. Алгоритмы определения оптимальных маршрутов придают маршрутизаторам более высокий "интеллект" по сравнению с мостами.

Это позволяет:

- избегать больших задержек при передаче пакетов, выбирая альтернативные пути;
- динамически изменять маршруты при отказе каналов или больших нагрузках в сети;
- уменьшать стоимость передачи за счет выбора альтернативных путей.

Объединение через межсетевые интерфейсы, называемые также шлюзами (gateway) осуществляется на уровнях 4-7. Применение шлюзов связано с необходимостью осуществлять сетевые взаимодействия в неоднородной среде. Неоднородность заключается в существовании различных стеков протоколов, установленных на станциях между которыми необходимо осуществлять взаимодействие. Наиболее известными стеками протоколов являются SPX/IPX, TCP/IP, ISO. Работа шлюза заключается в преобразовании пакетов одного стека протоколов в другой.

Каждое из перечисленных устройств обеспечивает функциональные возможности, соответствующие своему уровню, а также использует функциональные возможности всех более низких уровней. "Интеллектуальность", а вместе с ней сложность и стоимость межсетевых устройств повышаются с уровнем OSI на котором в них происходит объединение в LAN.

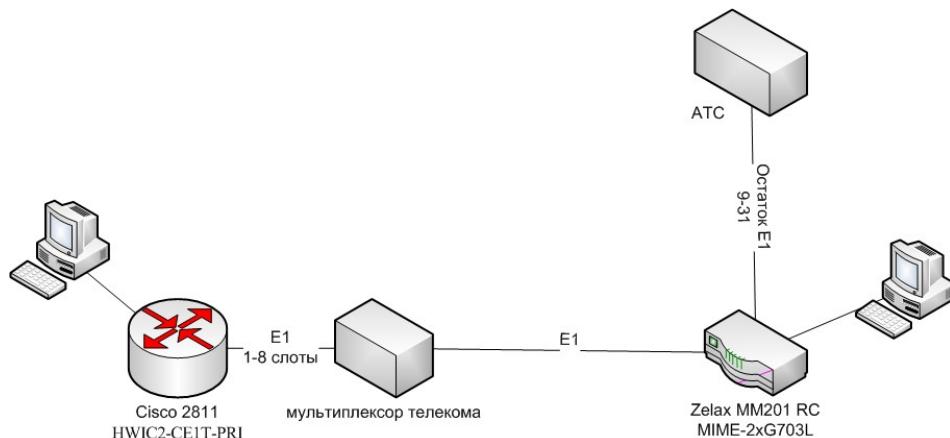
Например:

При построении каналов связи, с учетом технических условий телекома, приходилось использовать оборудование разных производителей.

Так согласно тех.условий на одной стороне пришлось вклиниваться в поток E1 забирать часть слотов и отдавать остаток.

Для этого использовали модульный маршрутизатор MM201RC с модулем MIME-2xG703L фирмы Zelax.

Схема сети и настройка двух маршрутизаторов



При организации Serial канала чаще всего используют протоколы **PPP** или **HDLC**. Но с **HDLC** протоколом проблема: у Cisco свой **HDLC**, у других производителей свой. В связи с тем, что объединяются маршрутизаторы cisco и не cisco будем использовать протокол **PPP**.

Маршрутизатор ит Zelax оказался достаточно дружелюбным устройством, с системой команд похожей на Cisco IOS.

Но тут новая проблема. После поднятия serialных интерфейсов, даже при соединении Zelax с Zelax по протоколу **PPP** интерфейсы переходят в состояние UP, счетчики пакетов увеличиваются, но ничего не работает.

После нескольких экспериментов и переписки с представителями Zelax единственный рабочий вариант получился при создании мостового соединения.

Выкладываю файл конфигураций

Конфигурация маршрутизатора Cisco

bridge

controller	E1	timeslots	0/0/0
channel-group	1		1-8
description			MM201

interface

no	ip	Serial0/0/0:16
no		address
encapsulation		directed-broadcast
no		ppp
bridge-group		keepalive
		1

interface

encapsulation	dot1Q	FastEthernet0/0.202
no	ip	202
no		address
bridge-group		directed-broadcast
		1

interface

ip	address	10.1.1.1	BVI1
no	ip	255.255.255.0	directed-broadcast

bridge

bridge 1 route ip	1	protocol	ieee
--------------------------	----------	-----------------	-------------

Конфигурация маршрутизатора mm201RC

ip			routing
ip	route	0.0.0.0/0	10.1.1.1
bridge			1
controller	E1		1/0
framing			pcm31
channel-group	1	timeslots	1-8
channel-group	2	timeslots	9-31
controller	E1		1/1
framing			pcm31
channel-group	2	timeslots	9-31
connect	vozvrat	E1	1/0:2
network-clock-select		1	E1
			1/0

interface	address	10.1.1.2	BVI1
ip		255.255.255.0	
mac-address		11:11:11:11:11:12	
no		shutdown	
interface			Ethernet0
bridge-group			1
no			shutdown
interface			Serial1/0:1
bridge-group			1
bandwidth		512000	
point-to-point			
encapsulation			ppp
no			
no shutdown			keepalive

Задание: Опишите процесс объединения LAN.

Нюансы

Первое:

При настройке Zelax на BVI1 интерфейсе в зависимости от версии может генерироваться MAC адрес, а может создать с нулями. Проверьте, и если сам не появился допишите, иначе удаленно до маршрутизатора не дастчаться.

Второе:

Определитесь, откуда идет синхронизация потока и пропишите командой network-clock-select 1 E1 1/0

Иначе работа будет идти с ошибками, да и у телекома с АТС проблемы будут.

Не забудьте прописать username и enable password

Практическое занятие №20

Тема: Формирование и настройка транковых групп и направлений

Цель работы. Освоить порядок настройки транковых групп и направлений.

Как создать и настроить trunk порты в Cisco для соединения коммутаторов на примере Cisco 2960+48TC-S

В предыдущей части мы рассмотрели вариант одного коммутатора который имеет разделение на vlan. Представим что появился еще один этаж и на нем свой коммутатор который тоже имеет свои vlan, встает вопрос как подключить два коммутатора. Для этого есть vlan trunk.

Теоретический материал.

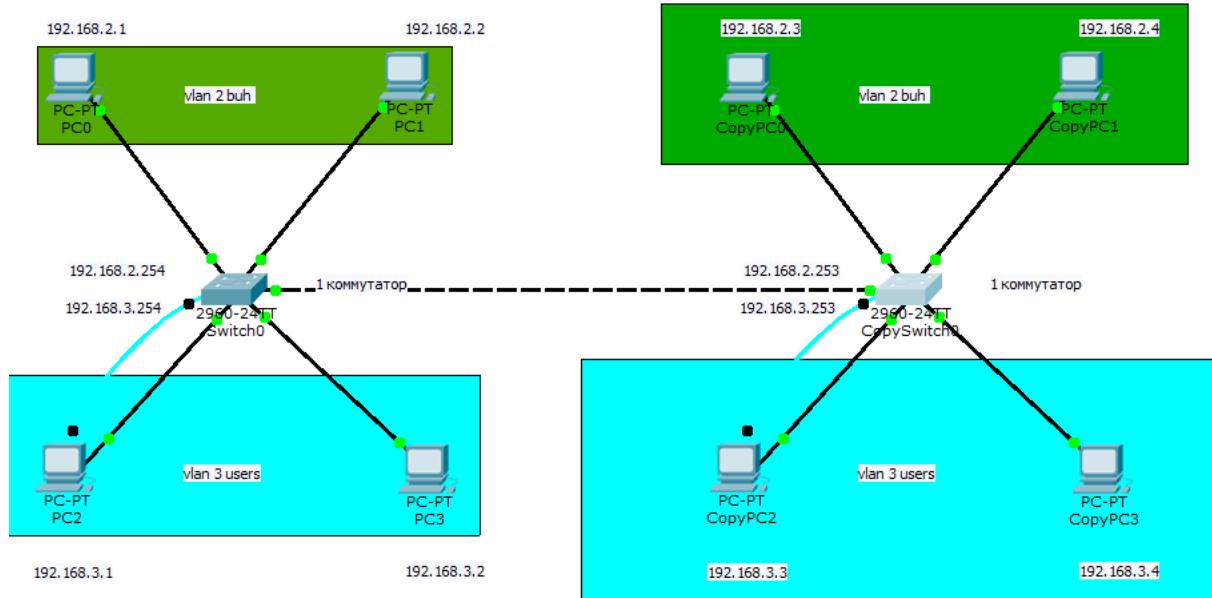
Trunk - сконфигурированное состояние порта коммутатора (в меню команды interface ...), предназначенное для подключения к другому коммутатору. Могут объединяться в Port-channel для увеличения надёжности и быстродействия. На обоих соединяемых таким образом коммутаторах порты должны быть в режиме trunk. Коммутаторы можно иногда соединять друг с другом и портами в режиме access.

Trunk Port (Магистральный порт) - это порт, предназначенный для переноса трафика для всех VLAN, доступных через определенный коммутатор, процесс, известный как транкинг. Магистральные порты помечают кадры уникальными идентифицирующими тегами - тегами 802.1Q или тегами Inter-Switch Link (ISL) - при их перемещении между

коммутаторами. Следовательно, каждый отдельный кадр может быть направлен в назначенный ему VLAN.

Интерфейс Ethernet может функционировать как магистральный порт или как порт доступа, но не оба одновременно. Магистральный порт может иметь более одного VLAN, настроенного на интерфейсе. В результате он может одновременно передавать трафик для многочисленных сетей VLAN. Это большое преимущество, так как для передачи трафика группе VLAN может использоваться один порт коммутатора. Они очень полезны, если пользователь хочет обмениваться трафиком между несколькими коммутаторами, имеющими более одного сконфигурированного vlan.

Схема выглядит так, есть два коммутатора Cisco 2060 находящиеся на разных этажах здания.



Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S20

Соединять будем через гигабитные порты. Идем на первом коммутаторе в режим конфигурирования **config**, t выбираем нужный интерфейс

```

Switch(config)#int
Switch(config)#interface g
Switch(config)#interface gigabitEthernet ?
  <0-9> GigabitEthernet interface number
Switch(config)#interface gigabitEthernet 1/?
  <0-24> GigabitEthernet interface number
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#

```

Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S16

Switch(config)#interface gigabitEthernet 1/1

Ставим нужный режим

Switch(config-if)#switchport mode trunk

```

Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed stat
e to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed stat
e to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
|
```

Ka

к создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S17

Разрешаем нужные vlan в нашем случае 2 и 3

```

Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#
end
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Switch#
```

Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S19

Делаем на втором коммутаторе **тоже самое**.

Проверим пингами соседей по этажам.

```

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
PC>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

Control-C
^C
PC>
```

Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S21

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=5ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=2ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

PC>
```

Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S22

```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)
Link-local IPv6 Address.....: FE80::2E0:F9FF:FECD:6B3B
IP Address.....: 192.168.3.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=0ms TTL=128
Reply from 192.168.3.1: bytes=32 time=0ms TTL=128
Reply from 192.168.3.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
PC>
```

Как создать и настроить vlan в Cisco на примере Cisco 2960+48TC-S23

Следующим шагом идет настройка маршрутизации в cisco, чтобы vlan видели друг друга.

Практическая работа №21

Тема: Соединение двух АТС по цифровым интерфейсам на базе оборудования компании Schmid Telecom



Описание:

В данном решении используются SHDSL-модемы ГМ-2Д1 предназначенные для передачи полного или частичного потока E1 по каналу SHDSL (одной симметричной витой паре). ГМ-2Д1 поддерживает стартовую процедуру коннекта между модемами по SHDSL в соответствии с ITU G.hs (ITU-T G.994.1). Скорости передачи данных для двухпроводного режима SHDSL от 64 кбит/с до 2312 кбит/с.

В данном решении используются SHDSL-модемы ГМ-2Д1, предназначенные для передачи полного или частичного потока E1 по каналу SHDSL (одной симметричной витой паре). ГМ-2Д1 поддерживает стартовую процедуру соединения модемов по протоколу SHDSL в соответствии с ITU G.hs (ITU-T G.994.1). Скорости передачи данных для двухпроводного режима SHDSL от 64 кбит/с до 2312 кбит/с.



Модем ГМ-2Д1 предназначен для передачи одного потока E1 по одной медной витой паре. Одновременно возможна передача асинхронного потока через канал E1.

Ключевые возможности

- благодаря встроенному мультиплексору, модем ГМ-2Д1 может передавать через канал SHDSL как весь поток E1, так и часть тайм-слотов в соответствии с задаваемой пользователем картой их распределения;
- для передачи потока E1 (2048 кбит/с) используется одна медная витая пара;
- обеспечивает передачу потока E1 (2048 кбит/с) на существенно большие расстояния, чем оборудование G.703/G.704 (до 4,5 км по одной витой паре с диаметром жилы 0,4 мм против 2 км при использовании оборудования G.703/G.704);
- асинхронный порт для передачи данных по каналу E1;
- допускает включение тестовых режимов как с локального, так и с удаленного устройства, что в сочетании со встроенным BER-тестером позволяет проверять работоспособность устройств, линии связи и сквозного канала;
- имеет встроенные функции самодиагностики и тестирования, ведут журнал статистики работы устройства;
- обеспечивает полную гальваническую развязку с линией и эффективную электрическую защиту (до 1500 В);
- позволяет загружать встроенное программное обеспечение и управлять режимами работы модемов с любого компьютера через порт RS-232 с использованием экранного меню;
- обеспечивает конфигурирование с удаленного устройства, работающего в соответствии с рекомендациями ITU-T G.991.2, G.994.1
- гарантия 5 лет.

Интерфейс SHDSL:

- характеристики портов SHDSL соответствуют рекомендациям ETSI SDSL (ETSI TS 101 524) и ITU SHDSL (ITU-T G.991.2, G.994.1);
- тип линейного кодирования: TC-PAM16, TC-PAM32, TC-PAM8;
- двухпроводный режим передачи данных по SHDSL-каналу;

- скорость передачи данных — 192...2048 кбит/с.

Цифровые интерфейсы:

- интерфейс E1:
 - импеданс порта E1: 120 Ом (RJ-45) или 75 Ом (BNC, подключение через переходник PE1); характеристики каналов E1 соответствуют рекомендациям G.703, G.704, G.706, G732, G.823;
- RS-232 (V.24/V.28):
 - программируемая скорость передачи данных до 230,4 кбит/с;
 - поддержка программного и аппаратного управления потоком данных;

Управление и контроль работы:

- настройка параметров осуществляется с помощью внешнего терминала, в качестве которого можно использовать персональный или карманный компьютер;
- предусмотрена настройка параметров удаленного модема с локального модема;
- встроенный BER-тестер;
- три тестовых режима.

Питание (в зависимости от модификации):

- универсальное: ~220 В и от постоянного напряжения 20...75 В;
- от сетевого адаптера ~220 / ~9 В.

Конструктивные исполнения (в зависимости от модификации):

- пластмассовый корпус 225×200 × 80 мм;
- для монтажа в корзину Р-510.

Задание.

Изучить принцип соединение двух АТС по цифровым интерфейсам, назначение используемого оборудования.

Практическое занятие №22

Тема: Изучение системы управления сетевым оборудованием. Протокол SNMP

Цель занятия: изучить задачи протокола SNMP.

Оборудование: раздаточный материал.

Основные теоретические сведения

Основная задача при управлении компьютерными сетями – автоматизировать процесс конфигурации и мониторинга параметров сети. На сегодня существует множество моделей и систем сетевого управления. Эта статья должна помочь читателю разобраться во всем этом разнообразии. Обычно, система сетевого управления представляет собой прикладную программу высокого уровня, которая использует один из стандартных протоколов сетевого управления. (SimpleNetworkManagementProtocol (SNMP) или CommonManagementInformationProtocol (CMIP)).

CMIP применяется в телекоммуникационных сетях, где необходимы все доступные возможности управления сетями, в то время как SNMP используется в локальных и корпоративных сетях, где достаточно минимума данных.

Информационная структура большинства компаний представляет собой сложную разнородную сеть, которая состоит из разнообразного программного и аппаратного обеспечения многих производителей, а интеллектуальная система управления сетевым оборудованием способна значительно упростить процесс управления телекоммуникационным оборудованием.

Основными задачами системы управления являются:

1. обеспечение высокой производительности сети;
2. обеспечение удобной среды для управления сетевыми ресурсами;
3. сбор информации о состоянии всех сетевых устройств;
4. анализ и хранение информации о состоянии всех сетевых устройств;
5. прогнозирование возможных сбоев в работе сети.

ПРОТОКОЛЫ УПРАВЛЕНИЯ СЕТЯМИ

Системы управления сетями используют один из стандартных протоколов (SNMP или CMIP).

Система, основанная на протоколе SNMP, включает в себя:

1. протокол взаимодействия агента и менеджера;
2. язык описания моделей MIB и сообщений SNMP — язык абстрактной синтаксической нотации ASN.1

3. ограниченное количество моделей MIB (MIB-I, MIB-II, RMON, ...)

Изначально, протокол SNMP и база SNMPMIB разрабатывались как временное решение для управления маршрутизаторами Интернет. Но решение оказалось настолько простым, эффективным и гибким, что и по сей день, оно находит повсеместное применение при управлении сетевым оборудованием.

С помощью протокола SNMP можно оценить производительность сетевых устройств, количество свободных ресурсов, загруженность и получить множество других полезных характеристик, необходимых для управления сетевыми устройствами. SNMP – протокол типа “запрос-ответ” т.е на каждый запрос от менеджера должен быть передан ответ от агента.

Протокол SNMP обладает достаточно небольшим набором команд:

1. Команда ‘Get-request’ применяется менеджером для получения от агента значения объекта по имени;

2. Команда ‘GetNext-request’ применяется менеджером для получения значения следующего объекта при последовательном обходе MIB;

3. При помощи команды ‘Get-response’ агент SNMP передает менеджеру результаты вышеперечисленных команд;

4. Команда ‘Set’ устанавливает значения объекта;

5. Команда ‘Trap’ сообщает менеджеру о возникновении какой-либо нестандартной ситуации;

6. В SNMPv.2 добавлена команда ‘GetBulk’, при помощи которой менеджер может получить несколько значений переменных за один запрос.

Сама структура MIB имеет стандартизированную структуру, которой придерживаются все фирмы-производители сетевого оборудования. Для специфических параметров сетевого оборудования используются специальные частные (private) поддеревья.

В протоколе SNMP присутствует агент, который обрабатывает данные, полученные из MIB, и передает их менеджеру, на управляющей станции сети. В результате управляющие станции обладают всей информацией, которая им необходима из MIB. главное достоинство протокола SNMP заключается в его простоте и в том, что он поддерживается почти всеми производителями сетевого оборудования.

Из-за своей простоты, протокол SNMP обладает еще и некоторыми недостатками:

1. при опросе происходит загрузка сети сервисной информацией, что ухудшает пропускную способность сети в целом;

2. данные практически не шифруются при передаче;

3. Так как в качестве транспортного протокола используется протокол низкого уровня (UDP), нет возможности подтвердить доставку информации.

В следующей таблице представлены наиболее важные характеристики самых распространенных платформ управления:

HP OpenView Network Node

Manager

IBM Tivoli NetView Sun Solstice

Domain Manager

Определение имени хоста по его адресу через сервер DNS + + +

Возможность модификации присвоенного имени хоста + + +

Распознавание сетевых топологий

Любые сети, работающие по TCP/IP

Распознавание по интерфейсам устройств Ethernet, Token Ring, FDDI, распределенные сети

Поддержка баз данных MicrosoftSQLServer, Oracle, интегрированные DB2, Informix, Oracle, SQL, Sybase, Informix, Oracle, Sybase

Формат отчетов Формат HTML, электронная почта

Формат HTML Консоль Поддерживаемые веб серверы MicrosoftIIS, Apache WebSphere® Application Server, BEA WebLogic Application Server, Apache, Microsoft IIS, Planet Web Server

Поддерживаемые протоколы SNMPv1; SNMPv2, TCP/IP, SNMP, SOAP, SSH, CMIP, SNMP, IPX/DMI, UDP, ICMP, ARP/RARP TCP/IP NC/NFS, IPX, TCP/IP, SunNet OSI, X.25 Start, DCE, Netware

Взаимодействие с майнфреймами

При помощи приложений третьих фирм

Может обращаться к NetView на майнфрейме +

Поддержка ОС HP-UX, Solaris, Windows, Linux AIX, OSF/1, Windows NT Solaris 2.4 или более поздняя версия Solaris 1.1.1 (SunOS™ 4.1.3) Или более поздняя версия

Контрольные вопросы:

1. Достоинства и недостатки SNMP.
2. Основные задачи системы управления.
3. Набор команд протокола SNMP

Практическая работа 23

Тема: Создание аналогового и цифрового направления на АТС

Теоретический материал.

Главная задача цифровой АТС — увеличить возможности системы связи за счет обработки оцифрованных данных. При этом наличие специальных цифровых подключений — важное, но не обязательное условие применения цифровой станции.

Предположим, требуется организовать связь по внешним и внутренним аналоговым линиям, но при этом емкость больше 80 номеров и (или) требуется дополнительный расширенный функционал (то же самое селекторное совещание, например). Цифровых подключений нет, но для обеспечения требуемых параметров нужны более мощные процессорные возможности. Значит, альтернативы цифровой АТС в данном случае нет.

Но ведь в каком-то другом случае сможет потребоваться не только все вышеперечисленное, но еще и, скажем, подключение цифрового потока. Опять потребуется цифровая станция, но уже в другой конфигурации.

Как предусмотреть все это в архитектуре АТС?

Этот вопрос рассмотрим на п



римецифровой IP АТС МАКСИКОМ MXM500Р.

Цифровая IP АТС МАКСИКОМ MXM500 — преимущества традиционной телефонии и новые возможности. Обязательно загляните в описание и спецификации!

Для АТС этой модели установлен универсальный базовый блок на 16 универсальных слотов (платомест). Платы источника питания и процессора устанавливаются в специальные отдельные слоты.

Для MXM500P разработаны и выпускаются несколько типов плат. Среди них — IP плата и плата подключения цифрового потока. Остальные модули рассчитаны на подключение разных комбинаций аналоговых портов СЛ и АЛ. Кроме того, есть специальные платы для подключения аналоговых и цифровых системных телефонных аппаратов.

В результате даже на базе одного блока можно создать множество разных конфигураций. В одном случае это будет АТС для подключения по аналоговым внешним и внутренним линиям, но с богатым набором сервисных функций. В другом — помимо аналоговых подключений появятся цифровые потоки. В третьем — добавится возможность внешней и внутренней IP связи.

Задание. Запрограммировать связь с аналоговой и цифровой линией связи.

Ход работы.

Индивидуальная настройка внешних линий.

Для программирования каждой СЛ доступны следующие установки:

- **Запрет исходящей связи.** Включенная установка запрещает исходящую связь. (Поэтому помещение в группу такой линии смысла не имеет).
- **разрешение автоотключения.** Включенная установка отключит линию по истечении времени T27 (51 мин).
- **режим «Без сервиса».** При включенной установке УАТС не подает в СЛ никаких звуковых сигналов. Всякий сервис полностью отсутствует.

Освобождение такой линии возможно только положением трубки.

Внимание: В режим «Без сервиса» войдет всякая АЛ, соединившаяся с такой СЛ.

- **разрешение тонального набора.** При включенной установке набор в СЛ будет тональным (DTMF). Если набор производится автоматически (из буфера автонабора или из записной книжки), он может меняться при помощи специальных символов, содержащихся в номере (См. Е1.5.).

- **разрешение отбоя входящего вызова.** Включенная установка разрешает УАТС дать сигнал отбоя в городскую линию при невозможности подать входящий звонок (или сигнал «требование внешнего соединения») хотя бы на одну АЛ.

Необходимо знать о последствиях включения этой установки.

Во внешнюю линию сразу будет подан сигнал «отбой» и вызов будет потерян, если следующая строка в таблице не заполнена, а в текущую строку вызов подать нельзя по одной из причин, а именно:

- АЛ заняты и у них включен «Запрет сигналов требования соединения»,
- АЛ заняты и имеют включенным режим "без сервиса".
- АЛ получают ранее поступивший вызов.

Однако если следующая строка заполнена, то вызов сразу будет переведён на неё и не будет потерян.

- **разрешение замещения сигнала.** Только для исходящей связи. При включенной установке вместо сигналов «готовность» или «отбой» от

внешней АТС, УАТС подает свой соответствующий сигнал. Замещение сигнала выключается после начала набора внешнего номера. Замещение сигнала не будет, если для этой СЛ включен тональный набор

Совет: Необходимость включения замещения сигнала возникает в случаях, когда внутри УАТС используется тональный набор и внешние шумы из СЛ мешают распознанию тонального набора, или приводят к ложным срабатываниям тонального приемника станции.

- **Тип линии “Квант”.** Эта установка предназначена для подключения СЛ к станциям, поддерживающим соответствующий протокол занятия низковольтной линии, после чего выполняется задержка Т33 (1 с).

- **Номер блокированной СЛ.** Запрещает станции одновременно использовать оба выхода такой линии для исходящей связи.

Совет: При наличии УАТС блокированные номера одной линии становятся ненужными. Дешевле и удобнее задействовать эту линию как обычную, т.е. завести её напрямую, отказавшись от второго номера. Исключение составляет случай, когда пользователь дорожит этими номерами, например, если оба номера такой линии широко известны как контактные.

- **Буфер автонабора.** Содержит комбинацию цифр и спец. символов, которые будут набраны или обработаны УАТС, прежде чем в линию пойдут цифры, набранные абонентом.

- **Разрешение удержания последней цифры.** Включается для устранения задержки включения разговорного тракта в сторону внешнего абонента на время Т16 (5 с).

- **Цифры выхода на междугороднюю и международную связь.** Нужные цифровые комбинации прописываются в общесистемных установках.

Отчет.

Описать принцип программирования аналогового и цифрового направления на АТС.

Практическая работа 24

Тема: Подключение и конфигурирование IP-клиентов (на примере протоко SIP)

Краткий теоретический материал

Понятия, определения

• **Алиас (абонент)** — совокупность, описывающая в пределах системы телефонный номер, связанный с интерфейсом в рамках определенной виртуальной АТС и различные дополнительные атрибуты (категория, абонентская группа, услуги). Фактически описывает абонента виртуальной АТС, подключенного к определенному порту и обладающего определенным набором специфичных для него параметров.

- **Форкинг (forking)** — привязка нескольких частных контактов к одному публичному контакту.

Ход работы.

Порядок конфигурирования SIP-абонентов

Перед созданием SIP-абонента необходимо:

1. Создать виртуальную АТС, создать контексты маршрутизации;
2. Выделить абонентскую емкость для использования системой;
3. При необходимости настроить LDAP-сервер, если для хранения данных аутентификации пользователя выбран данный режим. По умолчанию в системе выбран другой вариант хранения параметров аутентификации — база DS.

Порядок конфигурирования:

1. Создать SIP-абонента;
2. Выполнить настройку параметров.

Описание общих параметров абонента приведено в [Приложении А. Инструкции Набор параметров алиасов.](#)

Настройка параметров SIP-абонента может быть выполнена индивидуально или через назначение определенного профиля настроек.

Иерархия профилей настроек имеет вид:

1. Domain profile — профиль на уровне виртуальной АТС;
2. Named profiles — абонентские профили;
3. Subscriber settings — индивидуальные настройки абонента.

Для каждой виртуальной АТС может быть настроен только один профиль на уровне виртуальной АТС. Настройка профилей доступна администратору виртуальной АТС и администратору системы ECSS-10.

Значения параметров с меньшей областью действия переопределяют значения параметров профилей с большей областью действия. В приведенной выше иерархии параметры уровня 3 переопределяют параметры уровня 2 и меньших.

На практике рекомендуется задавать значения параметров в наиболее общих профилях, то есть на больших уровнях иерархии. Это позволяет хранить меньше данных, вносить групповые изменения в одном месте.

Настройка абонентов через CLI

Описание команд, используемых при настройке SIP-абонентов, приведено в справочнике команд CLI, раздел [Команды управления конфигурацией абонентов SIP.](#)

Добавление абонента

Для создания SIP-абонента используется команда:

```
/domain/<DOMAIN>/sip/user/declare      <ROUTING_CONTEXT>      <GROUP>
<INTERFACE> [<ALIAS> [<QOP_AUTH> [<LOGIN> [<PASSWORD>]]]]
```

где

<DOMAIN> — имя виртуальной АТС; <ROUTING_CONTEXT> — имя контекста маршрутизации для данного абонента; <GROUP> — название группы пользователей, логическое объединение интерфейсов в определенной виртуальной АТС. Может быть задана существующая или новая группа пользователей;

<INTERFACE> — название декларируемого интерфейса, задается в виде: username@host, где username — номер абонента; host — название SIP-домена регистрации. Список может быть задан диапазоном {a-b} или перечислением {a,b}, где a,b — натуральные числа. Например, интерфейсы 1111@eltex.local, 1112@eltex.local, 1113@eltex.local можно задать в виде 111{1-3}@eltex.local или 111{1,2,3}@eltex.local или {1111,1112,1113}@eltex.local. Может быть задан существующий домен SIP-регистрации или указан новый; <ALIAS> — альтернативный номер абонента, при указании значения "none" альтернативный номер не используется. Параметр нужен для возможности использовать тестовые имена на уровне SIP. Например, нужно прописать в качестве интерфейса SIP-абонента "text.users.name@some.sip.area", но так как в системе ECSS-10 используется телефонная

маршрутизация, текстовое имя в маршрутизации использовать запрещено. В этом случае SIP-абоненту назначается параметр <ALIAS> — цифровой (телефонный) номер; <QOP_AUTHN> — поддержка QOP-аутентификации (повышенный уровень защиты). Опциональный параметр:

- no_qop_authentication — использовать QOP-аутентификацию;
- qop_authentication — не использовать QOP-аутентификацию;

<LOGIN> — имя декларируемого пользователя. Опциональный параметр. Имя пользователя может быть впоследствии добавлено/изменено как терминальными командами, так и на LDAP-сервере:

• login_as_number — в качестве имен пользователей использовать декларируемые номера;

- none — не назначать параметры авторизации при декларации;
- common_login <LOGIN> — общее имя <LOGIN> для всех декларируемых абонентов.

<PASSWORD> — пароль декларируемых пользователей. Не указывается, если в качестве <LOGIN> выбрано "none".

• auto_generation — каждому декларируемому абоненту генерируется персональный пароль. Полученные пароли можно будет посмотреть командами "user info" или "user authentication";

• публичный пароль (символьная строка) — всем декларируемым абонентам будет назначен единый заданный пароль.

Пример

Декларация одного абонента без указания параметров аутентификации, например, планируется указание доверенных IP-адресов (параметр "trusted-ip"):

```
domain/test.domain/sip/user/declare local smg 401@test.domain none no_qop_authentication
```

Настройка параметров абонента

Команды уровня администратора виртуальной АТС

Для изменения индивидуальных значений параметров абонента используются следующие команды:

• Команда для изменения параметров определенного абонентского номера и интерфейса заданной виртуальной АТС:

```
/domain/<DOMAIN>/alias/set <NUMBER> <GROUP> <INTERFACE>
<PROPERTY> <VALUE>
```

• Команда для изменения параметров всех абонентов с определенным интерфейсом заданной виртуальной АТС:

```
/domain/<DOMAIN>/alias/set-for-iface <GROUP> <INTERFACE> <PROPERTY>
<VALUE>
```

• Команда для изменения параметров всех абонентов с определенным абонентским номером заданной виртуальной АТС:

```
/domain/<DOMAIN>/alias/set-for-address <NUMBER> <PROPERTY> <VALUE>
где
```

<DOMAIN> — имя виртуальной АТС;

<NUMBER> — абонентский номер; <GROUP> — имя группы интерфейсов, логическая привязка интерфейсов в определенной виртуальной АТС;

<INTERFACE> — имя интерфейса;

<PROPERTY> — имя изменяемого параметра, список приведен [Приложении А. Набор параметров алиасов](#);

<VALUE> — значение изменяемого параметра, список приведен [Приложении А. Набор параметров алиасов](#).

Для изменения значений параметров профиля виртуальной АТС абонента необходимо выполнить следующую команду:

```
/domain/<DOMAIN>/alias/set-for-domain <PROPERTY> <VALUE>
```

где
<DOMAIN> — имя виртуальной АТС;
<PROPERTY> — имя изменяемого параметра, список приведен [Приложении А. Набор параметров алиасов](#);
<VALUE> — значение изменяемого параметра, список приведен [Приложении А. Набор параметров алиасов](#).

Указанные выше команды используются для настройки общих параметров для всех абонентов системы: SIP-абонентов, абонентов H.248/megaco, виртуальных абонентов.

Для настройки параметров, специфичных только для SIP-абонентов, используется команда:

```
/domain/<DOMAIN>/sip/user/set      <GROUP>      <SIP_URI>      <PROPERTY>
<VALUE>
```

где

<DOMAIN> — имя виртуальной АТС;
<GROUP> — имя группы интерфейсов, логическая привязка интерфейсов в определенной виртуальной АТС;
<SIP_URI> — SIP URI абонента, задается в виде: username@host, где username — номер абонента; host — название SIP-домена;

Список может быть задан диапазоном {a-b} или перечислением {a,b}, где a,b — натуральные числа.

Пример. Интерфейсы [1111@eltex.local](#), [1112@eltex.local](#), [1113@eltex.local](#) можно задать в виде [111{1-3}@eltex.local](#) или [111{1,2,3}@eltex.local](#) или [{1111,1112,1113}@eltex.local](#).

<PARAMETER> — имя изменяемого параметра, список приведен [Приложении Б. Набор параметров интерфейса SIP](#);

<VALUE> — значение изменяемого параметра, список приведен [Приложении Б. Набор параметров интерфейса SIP](#).

Команды уровня администратора системы

Для изменения значений индивидуальных параметров абонента необходимо выполнить следующую команду:

```
/cluster/storage/<CLUSTER>/alias/set-for-address      <DOMAIN>      <NUMBER>
<PROPERTY> <VALUE>
```

Свойство будет назначено всем одинаковым номерам во всех виртуальных АТС.

Для изменения значений параметров профиля на уровне виртуальной АТС необходимо выполнить следующую команду:

```
/cluster/storage/<CLUSTER>/alias/set <DOMAIN> <PROPERTY> <VALUE>
```

где

<CLUSTER> — имя кластера хранения долговременных данных (DS). По умолчанию в системе присутствует кластера хранения долговременных данных с именем "ds1";
<NUMBER> — абонентский номер;

<DOMAIN> — имя виртуальной АТС (домена);

<PROPERTY> — имя изменяемого параметра, список приведен в [Приложении А. Набор параметров алиасов](#);

<VALUE> — значение изменяемого параметра, список приведен в [Приложении А. Набор параметров алиасов](#).

Удаление SIP-абонента

Для удаления SIP-абонента используется команда:

Команда удаляет одновременно интерфейс и алиас.

```
/domain/<DOMAIN>/sip/user/remove <GROUP> <SIP_URI> [--force]
```

где

<DOMAIN> — имя виртуальной АТС;

<GROUP> — имя группы интерфейсов, логическая привязка интерфейсов в определенной виртуальной АТС;

<SIP_URI> — SIP URI абонента, задается в виде: username@host, где username – номер абонента; host – название SIP-домена;

Список может быть задан диапазоном {a-b} или перечислением {a,b}, где a,b – натуральные числа.

Пример. Интерфейсы 1111@eltex.local, 1112@eltex.local, 1113@eltex.local можно задать в виде 111{1-3}@eltex.local или 111{1,2,3}@eltex.local или {1111,1112,1113}@eltex.local.

[--force] — удаление без дополнительного подтверждения, optionalный параметр.

Настройка SIP-абонентов через web-конфигуратор

Для создания SIP-абонентов используется приложение "Карточка абонента" ("Subscriber card").

Описание приложения приведено в разделе Карточка абонента (Subscriber card).

Для управления профилями абонентов используется приложение "Профили алиасов" ("Alias profiles").

Описание приложения приведено в разделе Профили абонентов (Alias profiles).

Создание SIP-абонента

Перед конфигурированием абонентской емкости необходимо настроить SIP транспорт см. Настройка ip-set.

Для добавления SIP-абонента нажмите кнопку "Добавить SIP пользователя" ("Add sip user") и заполните следующие поля:

Создать SIP пользователя

Имя интерфейса:	123 @ sorm
Владелец интерфейсов:	sip1
Контекст:	default_routing
Группа интерфейсов:	sip.ab
Модификация номеров:	default_modifiers
Аlias как пользователь:	<input checked="" type="checkbox"/>
Альтернативный alias:	
Профиль услуг:	
Авторизация:	<input checked="" type="radio"/> none <input type="radio"/> always <input type="radio"/> register
Логин:	
<input type="checkbox"/> Использовать номер в качестве логина	
Пароль:	
<input type="checkbox"/> Сгенерировать пароль	
<input type="button" value="Ok"/> <input type="button" value="Отмена"/>	

- Владелец интерфейсов (Interface owner) — владелец интерфейса — системная нода (адаптер);

- Контекст (Context) — название контекста маршрутизации;

- Группа интерфейсов (Interface group) — группа, в которую входит интерфейс. Задается администратором системы для удобства группировки абонентов по определенным параметрам.

- *Имя интерфейса (Interface)* — номер, закрепляемый за абонентом. Задается администратором системы. Номер не должен повторяться внутри одной ВАТС;

- о Список абонентов может быть задан диапазоном {a-b} или перечислением {a,b}, где a,b — натуральные числа;

- Пример. Список абонентов с номерами 755,765,775 можно указать в виде 7{5-7}5 или 7{5,6,7}5 или {755,765,775};

- *Модификация номеров (Modifier)* — выбрать правило модификации номера;

- *Алиас как пользователь (Alias as user)* — использовать алиас, с тем же номером, что и SIP-номер;

- *Альтернативный алиас (Alternative alias)* — использовать альтернативный номер у алиаса абонента;

- *Профиль услуг (SS profile)* — системный или доменный профиль услуг;

- *Авторизация (Auth)* — требование авторизации у абонента:

- о *none* — авторизация не требуется;

- о *always* — авторизация требуется как при регистрации, так и при запросах со стороны абонента;

- о *register* — авторизация требуется при регистрации.

- При выборе значений "*always*" и "*register*" нужно указать:

- *Логин (Login)* — имя пользователя для авторизации;

- *Использовать номер в качестве логина (Login as number)* — при установленном флаге в качестве имени пользователя использовать номер абонента, иначе — имя пользователя, установленное в поле "Логин" ("Login");

- *Пароль (Password)* — пароль пользователя для авторизации. Если поле оставить пустым, то пароль будет генерироваться автоматически;

- *Авторизация qop (Authorization qop)* — при установленном флаге использовать расширенную QoP-авторизацию, иначе — не использовать.

Нажмите кнопку "*Ok*" для добавления абонента(ов) в систему либо "*Отмена*" ("*Cancel*") для выхода из диалогового окна без добавления абонента(ов) в систему.

Настройка параметров SIP-абонента

Для настройки параметров, приведенных ниже, необходимо выделить нужного абонента, после чего приступать к настройке.

Настройка основных параметров для абонента

Во вкладке "*Основные*" ("*General*") выполняется настройка основных параметров для абонента.

Основные		Номера		Другие		SIP		Модификации SIP		Дополнительные услуги	
nai:		p	subscriberNumber								
npi:		p	isdnTelephony								
ni:		p	private								
screening:		p	networkProvided								
apri:	.										
категория:		p	ordinarySubscriber (10)								
активная:	.		true								
cdr группа:	.										
тип доступа:	d	access_type0									
режим:	.										
группа доступа:	p	all									
отображаемое имя:	.										
support encoding:	.	utf8									
почта:	.										
джаббер идентификатор:	.										
PIN-код:	g	1111									
media-profile:	d	default									
media-profile-outgoing:	.										
тип терминала:	.	smart									
профиль:	.	user_default									
расположение:	.										
Язык:	.										

Обновить

Сохранить

Отмена

- *nai* — идентификатор типа адреса, принимает значения: subscriberNumber, unknown, nationalNumber, internationNumber;
- *npi* — индикатор плана нумерации, принимает значения: isdnTelephony, dataNumberingPlan, telexNumberingPlan;
- *ni* — индикатор номера, принимает значения:
 - o emergency — экстренные службы;
 - o intercity — абоненты междугородной сети;
 - o international — абоненты международной сети;
 - o local — абоненты местной сети;
 - o private — локальные абоненты АТС;
 - o zone — абоненты зоновой сети;
- *screening* — индикатор контроля номера вызывающего абонента, принимает значения: userProvidedNotVerified, userProvidedVerifiedAndPassed, userProvidedVerifiedAndFailed, networkProvided;
- *apri* — индикатор ограничения предоставления номера вызывающего абонента: presentationAllowed, presentationRestricted, addressNotAvailable;

- *категория (category)* — категория вызывающего абонента, принимает значения: unknownAtThisTime, operatorFrench, operatorEnglish, operatorGerman, operatorRussian, operatorSpanish, reserved, ordinarySubscriber, subscriberWithPriority, dataCall, testCall, spare, payphone, category0, hotelsSubscriber, freeSubscriber, paidSubscriber, localSubscriber, localTaksofon, autoCallI, semiautoCallI, autoCallII, semiautoCallII, autoCallIII, semiautoCallIII, autoCallIV, semiautoCallIV;
- *статус (active)* — состояние абонента, принимает значения:
 - о *true* — активен;
 - о *false* — не активен;
- *cdr группа (cdr group)* — имя CDR-группы (используется для группировки cdr-записей);
- *тип доступа (access type)* — тип доступа для абонента (долговременные ограничения, которые вводятся при подключении абонента);
 - *режим (regime)* — режим обслуживания для абонента (временные ограничения);
 - *группа доступа (access group)* — имя группы доступа;
 - *отображаемое имя (display name)* — отображаемое имя на дисплее для абонента;
 - *support encoding* — тип кодировки, используемый для отображения имени абонента;
 - *почта (email)* — электронная почта для абонента;
 - *джаббер идентификатор (jabber id)* — идентификационный номер Jabber для абонента;
 - *PIN-код* — PIN-код для управления услугами с телефонного аппарата абонента;
 - *media-profile* — выбранный на домене медиа-профиль для входящей связи, по умолчанию устанавливается профиль default;
 - *media-profile-outgoing* — выбранный на домене медиа-профиль для исходящей связи связи, по умолчанию устанавливается значение undefined. При значении undefined для исходящей связи применяется тот же профиль, что и для входящей связи;
 - *тип терминала (terminal type)* — basic/smart;
 - *профиль (profile)* — профиль, назначаемый абоненту. Настройка профилей выполняется в приложении "Профили алиасов"("Alias profiles") в каталоге "named profiles";
 - *расположение (placement)* — территориальное расположение номера;
 - **Язык** — языковая локаль абонента.
 - о *Русский*
 - о *Английский*
 - о *Немецкий*
 - о *Испанский*
 - о *Французский*

Для обновления информации нажмите кнопку "Обновить" ("Refresh"). Для сохранения изменений в системе нажмите кнопку "Сохранить" ("Save"). Для отмены изменений нажмите кнопку "Отмена" ("Cancel").

Настройка дополнительных параметров для SIP-абонентов

Вкладка "SIP" будет доступна только при выборе SIP-абонента. Во вкладке "SIP" выполняются настройки, специфичные для SIP-абонентов.

Основные	Номера	Другие	SIP	Модификации SIP	Дополнительные услуги
Имя		Значение			
alarm_enable		false			
aliases_list		111			
auto_answer_version		default			
auto_answer_template					
auth_qop		false			
contact					
digest		true			
dtmf_relay		false			
fork_mode		all-contacts			
last_via		SIP/2.0/UDP 192.168.116.181 branch=z9hG4bK-17616-12-7			
login		111			
my_from		192.168.116.132			
nat_traversal		false			
password		123			
referred_by_as_cgrp		false			
reg_expire_min		90			
reg_expire_max		3600			
req100rel		false			
rfc4028_control		force			
routing_context		default_routing			
modificator					
sip_domain		192.168.116.132			
symbol_hash_as_is		false			
remote_ctr_indication		rpi			
original_cdpn_to		true			
category_to_sip		default			
tel_uri_in_diversion		false			
trusted_ip		false			
display_encoding		default			
user_agent					

Обновить

Сохранить

Отмена

Описание параметров приведено в [Приложении Б. Набор параметров интерфейса SIP](#).

Для обновления информации нажмите кнопку "Обновить" ("Refresh"). Для сохранения изменений в системе нажмите кнопку "Сохранить" ("Save"). Для отмены изменений нажмите кнопку "Отмена" ("Cancel").

Удаление абонента

Для удаления абонента в таблице абонентов установите флаг(и) напротив удаляемого(ых) абонента(ов) и нажмите кнопку "Удалить" ("Delete"). Подтвердите действие нажатием кнопки "Да".

Карточка абонента > arko > 100 [100@arko]

Номер			
<input type="checkbox"/>	0001		
<input type="checkbox"/>	0005		
<input checked="" type="checkbox"/>	100		
<input type="checkbox"/>	1001		
<input type="checkbox"/>	1002		
<input type="checkbox"/>	1003		
<input type="checkbox"/>	101		
<input type="checkbox"/>	102		
<input type="checkbox"/>	103		
<input type="checkbox"/>	111		
<input type="checkbox"/>	112		
<input type="checkbox"/>	1234		
<input type="checkbox"/>	1410		
<input type="checkbox"/>	1411		
<input type="checkbox"/>	1412		
<input type="checkbox"/>	1413		
<input type="checkbox"/>	1482		
<input type="checkbox"/>	4321		
<input type="checkbox"/>	5555		

Основные **Номера** **Другие** **SIP** **Модификации SIP** **Дополн.**

nai: p subscriberNumber
 npi: p isdnTelephony
 ni: p private
 screening: p networkProvided
 apri:
 категория: p ordinarySubscriber (10)
 активная: . true
 cdr группа: .
 тип доступа: d access_type0
 режим: .
 группа доступа: p all
 отображаемое имя:
support encoding: . utf8
 почта:
 джаббер:
 идентификатор: PIN-код: g 1111

Добавить **Удалить** **Обновить** Сохранить

Аутентификация абонентов

В системе ECSS-10 всегда требуется аутентификация абонентов.

Избежать требования аутентификации абонентов можно настройкой следующих параметров:

- **trusted-IP** — список доверенных IP-адресов, с которых разрешено получение запросов. Существует два режима запросов: strict (жесткий) — запросы разрешены только с этого адреса (адресов), nostrict — запросы разрешены с разных адресов. В случае strict-запроса аутентификация будет требоваться при включенном параметре *digest*. В случае nostrict-запросов вне зависимости от параметра *digest* аутентификация требуется с IP-адресов, не являющихся доверенными, с доверенных пускаем сразу.

Настройка выполняется командой `domain/<DOMAIN>/sip/user/set <GROUP> <INTERFACE> trusted-ip <IP-addr>`

Запрещено указывать адрес SBC или NAT как доверенный адрес.

Случай, когда можно отказаться от требования аутентификации:

- Офисные абоненты подключены к абонентскому шлюзу (например, TAU-32M.IP, TAU-72.IP), но при этом абонентам разрешена регистрация из внешней сети (например, форкинг с мобильным терминалом, с домашним телефоном). Если указать "доверенный IP" (параметр "trusted-IP"), то при регистрации и звонках с офисных шлюзов не будет требоваться аутентификация. Звонки из внешней сети будут требовать аутентификацию.

В данном случае не рекомендуется указание единого логина и пароля для всех абонентов, подключенных к офисному шлюзу.

- Офисные абоненты подключены к абонентскому шлюзу (например, TAU-32M.IP, TAU-72.IP). При этом все абоненты считаются стационарными без возможности форкинга контактов. Если указать «фиксированный IP» (параметр "trusted-ip"), то при регистрации и звонках с офисных шлюзов не будет требоваться аутентификация. При этом на шлюзах можно отключить регистрацию на сервере.

Альтернативным вариантом является указание единого логина и пароль для всех абонентов, подключенных к шлюзу.

Если пользователи регистрируются из внешней сети, всегда должна требоваться аутентификация.

Регистрация нескольких контактов SIP-абонента (forking)

Общее описание

Если у абонента есть несколько терминалов, например, стационарный телефон и мобильный телефон, то он может все свои терминалы (разные SIP-контакты) зарегистрировать под одним публичным номером. Публичный номер будет известен другим абонентам, и по публичному номеру будут поступать входящие вызовы. Привязка нескольких частных контактов к одному публичному называется **форкингом (forking)**.

На уровне SIP-адаптера форкинг работает в рамках одного абонентского интерфейса. Один абонент может под одним аккаунтом зарегистрировать несколько контактов (одной регистрацией или несколькими).

Принцип работы

Если есть несколько зарегистрированных контактов, то входящий вызов в зависимости от выбранного режима поступает одновременно или последовательно на все контакты. Переход на следующий контакт/контакты выполняется по получению неуспешного ответа или истечении тайм-аута (таймер "find-me").

Ответы 3xx воспринимаются как неуспешные, если в списке есть другие контакты. То есть работа форкинга приоритетней услуг переадресации.

Исходящие звонки разрешены с любого контакта в любом режиме. Абонент считается занятым, если по какому-либо контакту есть соединение или идет установка соединения, то есть работа интерфейса с несколькими зарегистрированными контактами в системе ничем не отличается от работы интерфейса с одним контактом.

Пример зарегистрированного абонента с несколькими контактами:

```
ecss-root@[ecss_mycelium@alex]:# domain/d.408/sip/user/info sip.test 900000@sip.test
```

```
1 users information read ...
```

```
[*****] 6ms
```

```
Executed on the pa_sip@alex
```

User	Is active	Group	Login	Registration	
Extended information					
-----+-----+-----+					
+-----+-----+-----					
900000@sip.test true <sip:900000@192.168.23.166:5064>;expires=65 sip.test q=1.0;					
<sip:900000@192.168.23.166:5062;transport=udp>;expires=9003 q=0.8;					
----- ----- ----- ----- ----- -----					

Режим форкинга

Выбор режима работы форкинга выполняется для абонента или группы абонентов следующей командой:

```
domain/<DOMAIN>/sip/user/set <GROUP> <SIP_URI> fork-mode <MODE>
<ALLOW-REPEAT-IP> <PREVIOUS-CONTINUE>
```

где

<DOMAIN> — имя виртуальной АТС;
<GROUP> — имя группы интерфейсов, логическая привязка интерфейсов в определенной виртуальной АТС;
<SIP_URI> — SIP URI абонента, задается в виде: username@host, где username — имя/номер абонента; host — домен регистрации;
Список может быть задан диапазоном {a-b} или перечислением {a,b}, где a,b — натуральные числа.

Пример. Интерфейсы 1111@eltex.local, 1112@eltex.local, 1113@eltex.local можно задать в виде 111{1-3}@eltex.local или 111{1,2,3}@eltex.local или {1111,1112,1113}@eltex.local.
<MODE> — режим форкинга:

- all-contacts — запрос на установление соединения (INVITE) отправляется одновременно на все зарегистрированные контакты. С первым ответившим контактом устанавливается диалог, вызовы на остальные контакты завершаются;

- find-me-one-by-one — последовательный перебор контактов по списку. Если контакт не отвечает по истечении таймера "find-me" (контакту отправляется CANCEL) или приходит неуспешный ответ, запрос перенаправляется на следующий контакт;

- find-me-with-q — последовательный перебор с учетом приоритета. Сначала выполняется запрос на все контакты самого старшего приоритета, затем на контакты со следующим приоритетом и так далее. Если в списке контакты только одного приоритета, то работа аналогична режиму "all-contacts". Если все имеют разный приоритет, то аналогично режиму "find-me-one-by-one";

- disable — отключение форкинга. Запрос на установление соединения (INVITE) будет отправляться только на первый контакт в списке, наличие остальных контактов игнорируется. Совершать вызовы разрешено со всех зарегистрированных контактов.

<ALLOW-REPEAT-IP> — будет ли перезаписываться старый контакт новым, если изменился только порт:

- allow-repeat-ip — существующий контакт будет сохраняться;
- disallow-repeat-ip — существующий контакт будет перезаписываться;

Примечание: параметр обязателен для всех режимов, кроме операции отключения (disable)

<PREVIOUS-CONTINUE> — свойство режимов find-me (для all-contacts не применяется):

- previous-continue — при переходе к следующему контакту (группе контактов с одним приоритетом) вызов предыдущего (предыдущих) продолжается;

- previous-stop — при переходе к следующему контакту (группе контактов с одним приоритетом) вызов предыдущего (предыдущих) отменяется

Примечание: параметр обязателен для режимов find-me-one-by-one и find-me-with-q

Список контактов формируется при регистрации в порядке убывания приоритета (параметр контакта "q"), равнозначные — в порядке получения регистраций. Если в регистрации приоритет контакта не указан, то он принимается равным 1. Значения приоритетов — число от 0 (низкий) до 1 (высокий).

Назначить приоритет контакту на уровне системы нельзя, приоритет контакта указывает пользователь в запросе регистрации.

Таймер "find-me"

Таймер "find-me" определяет интервал времени, в течение которого контакт должен ответить на поступивший вызов, по истечении таймера вызов передается следующему контакту SIP-аккаунта. Значение устанавливается в секундах, по умолчанию 5 секунд.

Команда для изменения значения таймера "find-me":
domain/<DOMAIN>/timers/sip/set find-me <VALUE>
где
<DOMAIN> — имя виртуальной АТС;
<VALUE> — значение таймера "find-me".

Пример:

```
admin@[mycelium@ecss1]:# domain/d.408/timers/sip/set find-me 5
```

Property "find_me" successfully changed from:

7

to

5.

...

```
admin@[mycelium@ecss1]:# domain/d.408/timers/sip/info
```

Property	Domain	Value
find_me	d.408	5

...

SIP-профили

Общее описание

Многие SIP-клиенты имеют особенности реализации.

Основная масса касается поддержки того или иного стандарта или спецификации. Также оператор сам может контролировать включение/выключение некоей функции (например, контроль сессии по RFC 4028).

Есть еще ограничения встречной стороны, которые противоречат или жестко ограничивают текущую реализацию взаимодействия адаптер-клиент:

- нотификации BLF о ходе параллельных соединений на наблюдаемом клиенте;
- осуществление исходящих звонков только через ноду адаптера, принявшую запрос регистрации
- реализация авто ответа, которая поддержана в рамках трех спецификаций, которые в свою очередь могут иметь разные опции.

Для преодоления данных ограничений реализованы профили SIP-клиентов, которые включают в себя особенности производителя.

Назначение профилей может осуществляться следующим образом:

- непосредственное назначение в свойствах SIP-абонента. Данный режим актуален когда нет полноценной детекции клиента;
- автоматическое определение при регистрации (по User-Agent).

Настройка профиля

При создании профиля задается его имя и набор параметров (один и более из имеющихся).

Сейчас поддерживаются три рабочих параметра и шаблон авто-определения:

- *auto-answer_version* — реализация авто ответа;
- *concurrency_blf* — нотификации о параллельных диалогах. Значения true/false (по умолчанию — false).

Под параллельными нотификациями имеются ввиду нотификации о параллельных звонках с одного абонента.

Реализована очередь нотификаций. Работает следующим образом — пока есть события по одному диалогу, другие события слаться не будут, они будут откладываться в очередь. Когда же текущий диалог завершится, то они будут разосланы в текущем состоянии.

Начиная с версии 3.11.0 этот режим может быть выбран профилем SIP-клиента. Абоненту назначается соответствующий профиль, либо он определяется автоматически (настройка `client_profile = auto`). Параметры профиля:

- `concurrency_blf = true` — разрешены параллельные нотификации, очередь не работает.
 - `concurrency_blf = false` — запрещены параллельные нотификации, очередь работает.
- Этот режим используется "по умолчанию"
- `node_control` — ограничение исходящих вызовов нодой-регистратором, то есть привязка к ноде адаптера, на который пришла регистрация. Значения `true|false` (по умолчанию — `false`);
 - `templates` — шаблон имени, содержащийся в заголовке User-Agent запроса регистрации;
 - `extended_blf` — поддержка события Endpoint States для BLF. Значение `true|false`(по умолчанию — `false`).

Команды управления профилями

Ниже приведены команды CoCon для управления SIP-профилями

В данном разделе приводится описание команд управления команды настройки профиля абонентов SIP.

Общее описание работы SIP-профилей приведено в разделе [SIP-профили](#).

<DOMAIN> - имя виртуальной АТС.

clean

Команда предназначена для сброса параметров профиля абонента SIP в значение по умолчанию. При необходимости можно сбросить все параметры профиля. Сам профиль удален при этом не будет.

В команде допустим ключ `--force`, при котором предупреждение будет пропущено. Актуально, например, при работе через скрипт. По "tab" не подставляется!

Путь команды:

/domain/<DOMAIN>/sip/user/profile/clean

Синтаксис:

clean PROFILE_ID [--force]

Параметры:

<PROFILE_ID> - существующий или новый ID профиля;

[--force] - удаление без дополнительного подтверждения.

Пример:

```
admin@mycelium1@ecss1:/$ domain/biysk.local/sip/user/profile/clean vp12
```

```
[clean] Set parameters to default value
```

```
continue: yes/no ?> domain/biysk.local/sip/user/profile/clean vp12
```

```
Executed on the sip1@ecss2
```

Profile ID	Profile set
vp12	auto-answer-version = default concurrency_blf = false direct_early_update = false extended_blf = false force_fork_release = false node_control = false remote_party_id_enable = false templates = -

[exec at: 12.03.2021 15:33:44, exec time: 12s 473ms, nodes: sip1@ecss2 v.3.14.8.26]

del

Команда предназначена для удаления профиля абонента SIP.

В команде допустим ключ --force , при котором предупреждение будет пропущено. Актуально, например, при работе через скрипт. По "tab" не подставляется!

Путь команды:

/domain/<DOMAIN>/sip/user/profile/del

Синтаксис:

del PROFILE_ID [--force]

Параметры:

<PROFILE_ID> - существующий или новый ID профиля;
[--force] - удаление без дополнительного подтверждения.

Пример:

```
admin@mycelium1@ecss1:$ domain/biysk.local/sip/user/profile/del vp12
[del] Remove profiles. Undo will be impossible
continue: yes/no ?> yes
Executed on the sip1@ecss1
ok
```

[exec at: 12.03.2021 15:33:57, exec time: 1s 858ms, nodes: sip1@ecss1 v.3.14.8.26] info
Команда предназначена для просмотра информации о профиле абонента SIP.

Путь команды:

/domain/<DOMAIN>/sip/user/profile/info

Синтаксис:

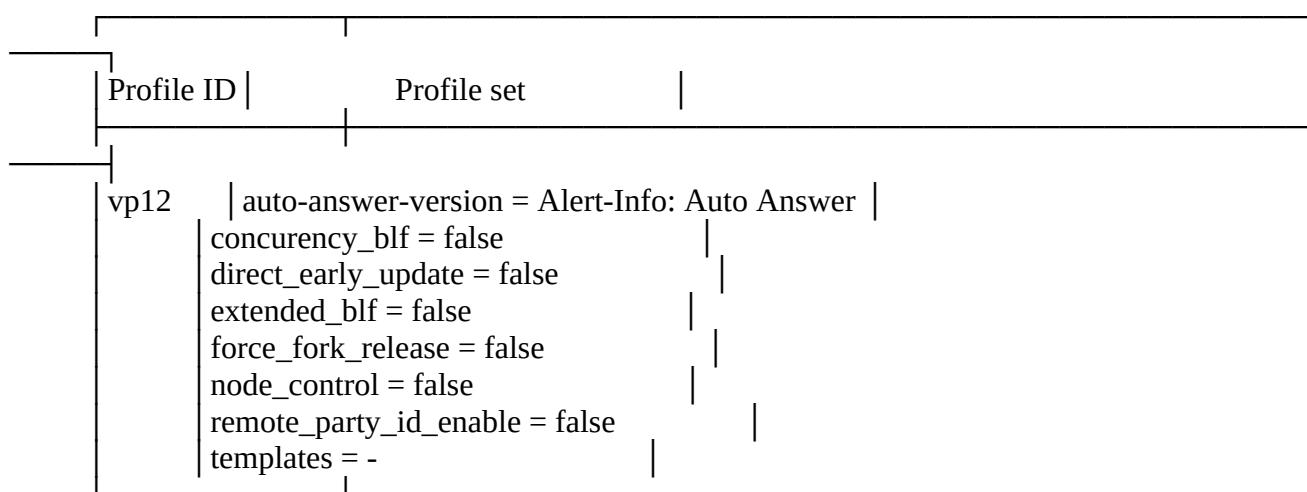
info PROFILE_ID

Параметры:

<PROFILE_ID> - существующий или новый ID профиля.

Пример:

```
admin@mycelium1@ecss1:$ domain/biysk.local/sip/user/profile/info vp12
Executed on the sip1@ecss1
```



[exec at: 12.03.2021 15:32:49, exec time: 5ms, nodes: sip1@ecss1 v.3.14.8.26]

list

Команда предназначена для просмотра списка профилей абонента SIP. Возвращает список имеющихся профилей, включая шаблон авто определения.

Путь команды:

/domain/<DOMAIN>/sip/user/profile/list

Синтаксис:

list

Параметры:

Команда не содержит аргументов.

Пример:

```
admin@mycelium1@ecss1:$ domain/biysk.local/sip/user/profile/list  
Executed on the sip1@ecss2
```

Profile ID	User-Agent template
vp12	

[exec at: 12.03.2021 15:33:17, exec time: 13ms, nodes: sip1@ecss2 v.3.14.8.26] preset

Команда предназначена для активации заранее сконфигурированного профиля.

Путь команды:

```
/domain/<DOMAIN>/sip/user/profile/preset
```

Синтаксис:

```
preset PROFILE_ID
```

Параметры:

PROFILE_ID - идентификатор существующего профиля.

Пример:

```
admin@mycelium1@ecss1:$ domain/biysk.local/sip/user/profile/preset coral
```

Executed on the sip1@ecss1

New profile 'coral' was created

[exec at: 15.03.2021 15:32:38, exec time: 10ms, nodes: sip1@ecss1 v.3.14.8.34]set

Команда позволяет задать параметры профиля SIP-клиента. Если ID не существует, то команда задает новый профиль.

При первой настройке профиль с указанным именем будет создан автоматически. Указывать одновременно можно один и более параметров через запятую. Шаблон агента вводится в кавычках, если содержит пробелы.

Внимание! Вхождение шаблона проверяется без учета регистра, но с учетом количества указанных пробелов!

Результат команды:

new - создан новый профиль с указанными именем и параметрами (неуказанные параметры принимают значения "по умолчанию");

exists - указаны уже установленные параметры существующему профилю;

change - параметр (параметры) существующего профиля изменены.

Путь команды:

```
/domain/<DOMAIN>/sip/user/profile/set
```

Синтаксис:

```
set PROFILE_ID KEY = VALUE[,...]
```

Параметры:

<PROFILE_ID> - существующий или новый ID профиля; <KEY> - название параметра, который разрешен:

- auto_answer_version - реализация авто ответа.;
- concurrency_blf - нотификации о параллельных диалогах. Значения true|false (по умолчанию - false);
- node_control - ограничение исходящих вызовов нодой-регистратором. Значения true|false (по умолчанию - false);
- templates - шаблон имени, содержащийся в заголовке User-Agent запроса регистрации;
- blf_xml_pretty_print - возможность форматирования xml в NOTIFY BLF. Значения true|false (по умолчанию - false).
-

Пример:

```
admin@mycelium1@ecss1:$ domain/biysk.local/sip/user/profile/set vp12 auto-answer-version  
alert-info template: "Auto Answer"
```

Executed on the sip1@ecss1

New profile 'vp12' was created

[exec at: 12.03.2021 15:32:30, exec time: 11ms, nodes: sip1@ecss1 v.3.14.8.26]

Настройки профиля для SIP-абонента

Как уже было указано выше профиль может назначаться как в автоматическом режиме так и непосредственно присвоением нужного.

Назначение режима

Текущее значение режима

```
admin@mycelium1@ecss1:/$ domain/biysk.local/sip/user/info loc.gr 240470@biysk.local --  
show-password
```

1 make users list ...

```
[*****] **** [*****]
```

131mks

1 users information read ...

```
[*****] 11ms
```

Executed on the sip1@ecss2

User	240470@biysk.local
internal iface name	064bc964febde57
isActive	false
group	loc.gr
authentication	240470:eGhohxie (ds) use qop: true
contacts definition	Contacts list is empty
declared by	admin at 28.01.2021 16:08:31
alarm_enable	false
aliases activities	240470:true
allow	INVITE, ACK, BYE, CANCEL, OPTIONS, PRACK, MESSAGE, SUBSCRIBE, NOTIFY, REFER, UPD ATE, INFO
allow events	none
auto-answer-version	Alert-Info: Auto Answer (default by domain)
category_to_sip	default
client-profile	none
compact-form	default (default)
digest	true
display-name-encoding	default
dtnf-duration	100
dtnf-relay	false
fork-mode	all-contacts, allow repeated IP: true
last via	SIP/2.0/UDP 192.168.2.26:5060;received=192.168.2.26;rport=5060
my_from	biysk.local
nat_traversal	false
options_control	disable
original-cdpn-to	true
published presence	none
referred-by-as-cgpn	false
register-expire-max	3600
register-expire-min	90

host-to-invite	registered-domain
registrator	node: sip1@ecss1 port: udp 192.168.2.62:5060
regs_time	18.02.2021 14:44:30
remote-ctr-indication	rpi
req100rel	false
rfc-4028-control	force
routing.context	ctx_from_local
sip-domain	biysk.local
sip-modifications	[]
supported	[req100rel]
symbol_hash_as_is	false
sip-transit	[]
trusted-ip	unassigned
user agent	RG-1404GF-W/1.11.0 SN/VI25002012 sofia-sip/1.12.10

[exec at: 12.03.2021 14:48:25, exec time: 26ms, nodes: sip1@ecss2 v.3.14.8.26]

При назначении автоматического режима, кроме самого значения режима будет указан профиль, который был определен. Если регистрации не было или авто определение было не успешно, будет указано: auto(None)

Отчет.

Цель работы и полученный результат

Литература

1. Приложение А (ссылка) www.multicom.ru Руководство по эксплуатации.

Практическая работа 25

Тема: Соединение двух АТС по IP-маршрутизации

Теоретический материал:

Типы серверов

Ключевые слова: сервер, сеть, аппаратное обеспечение, порт, доступ, dynamic, host, configuration, protocol, IP, Интернет, функция, DNS, почтовый сервер, письмо, запись, очередь, FTP, файл, packet, tracer, HTTP, DHCP, email, топология, Web, сайт, Зона DNS, маршрутизация, routing, определение, маршрутизатор, локальные сети, таблица, стандартный протокол, запрос, адрес, компьютер, интерфейс, администратор, шлюз, пул, TST, параметр, маска, хост, список

Как правило, *сервер* отдает в сеть свои ресурсы, а клиент эти ресурсы использует. Также, на серверах устанавливаются специализированное программное и *аппаратное обеспечение*. На одном компьютере может работать одновременно несколько программ-серверов. Сервисы серверов часто определяют их название:

Cisco HTTP (WEB) сервер – позволяет создавать простейшие веб-странички и проверять прохождение пакетов на 80-ый *порт* сервера. Эти серверы предоставляют *доступ* к веб-страницам и сопутствующим ресурсам, например, картинкам.

DHCP сервер – позволяет организовывать пулы сетевых настроек для автоматического конфигурирования сетевых интерфейсов. *Dynamic Host Configuration Protocol* обеспечивает автоматическое распределение IP -адресов между компьютерами в сети. Такая технология широко применяется в локальных сетях с общим выходом в *Интернет*.

DNS сервер – позволяет организовать службу разрешения доменных имён. Функция DNS -сервера заключается в преобразовании доменных имен серверов в IP -адреса.

Cisco EMAIL – почтовый сервер, для проверки почтовых правил. Электронное письмо нельзя послать непосредственно получателю – сначала оно попадает на сервер, на котором зарегистрирована учетная запись отправителя. Тот, в свою очередь, отправляет "посылку" серверу получателя, с которого последний и забирает сообщение.

FTP – файловый сервер. В его задачи входит хранение файлов и обеспечение доступа к ним клиентских ПК, например, по протоколу *FTP*. Ресурсы файла -сервера могут быть либо открыты для всех компьютеров в сети, либо защищены системой идентификации и правами доступа.

Итак, эмулятор сетевой среды Cisco *Packet Tracer* позволяет проводить настройку таких сетевых сервисов. В конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи (ResourceRecords) в прямой зоне DNS.

Новый термин

Зона DNS — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на сервере доменных имен (DNS-сервере). В зоне прямого просмотра на запрос доменного имени идет ответ в виде IP адреса. В зоне обратного просмотра по IP мы узнаем доменное имя ПК.

Ход работы.

1. Настройка IP адреса, адрес шлюза и адрес DNS сервера от DHCP сервера R0.

Сначала в ресурсной записи типа A Record свяжите доменное имя компьютера **server1.yandex.ru** с его IP адресом **10.0.0.1** и нажмите на кнопку **Add** (добавить) и активируйте переключатель **On** – рис. 6.9.

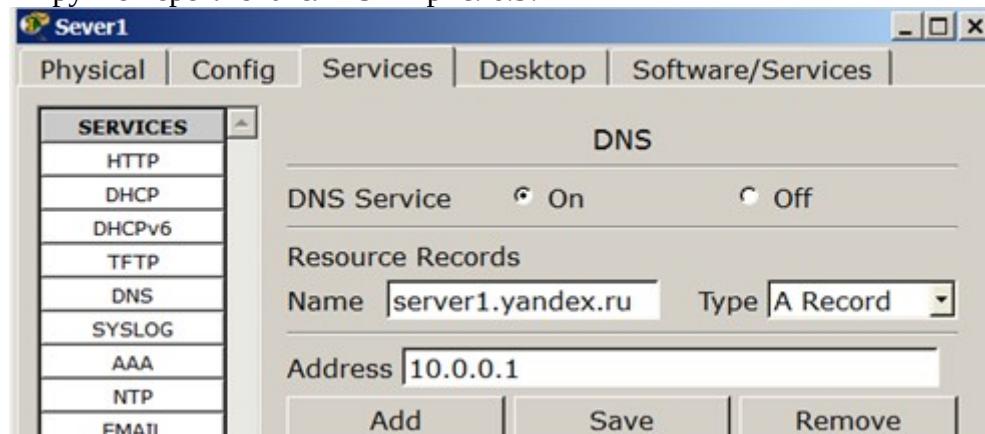


Рис. 6.9. Ввод ресурсной записи типа A Record

Далее в ресурсной записи типа CNAME свяжите название сайта с сервером и нажмите на кнопку Add (добавить) – рис. 6.10.

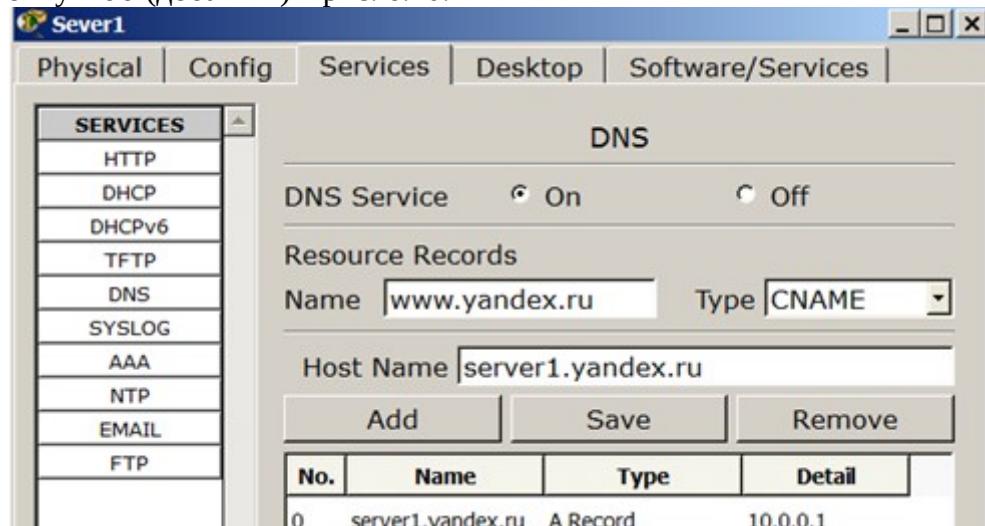


Рис. 6.10. Ввод ресурсной записи типа CNAME

В результате должно получиться следующее (рис. 6.11).

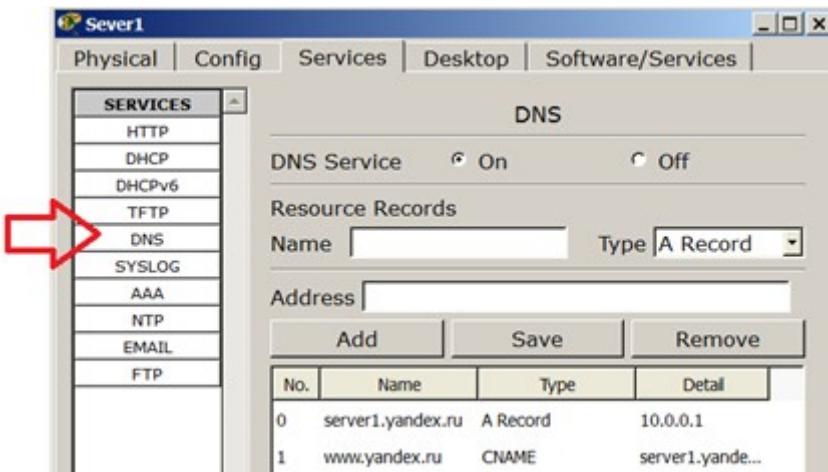


Рис. 6.11. Служба DNS в прямой зоне

Теперь настроим службу HTTP. В конфигурации Server1 войдите на вкладку HTTP и создайте стартовую страницу сайта (рис. 6.12).

```
<html>
<center><font size='+2' color='green'>Web Server</font></center>
www.yandex.ru
<p>
Hello!<br/>I am Server1
</html>
```

Рис. 6.12. Стартовая страница сайта

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки правильности работы прямой зоны DNS сервера введите команду SERVER>nslookup. Если все правильно настроено, то вы получите отклик на запрос с указанием доменного имени DNS сервера в сети и его IP адреса (рис. 6.13).

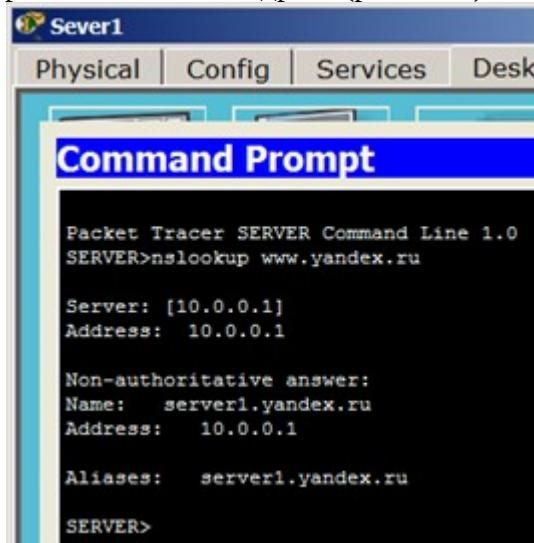


Рис. 6.13. Служба DNS в прямой зоне DNS на Server1 настроена правильно

Примечание

Команда **nslookup** служит для определения ip-адреса по доменному имени (и наоборот).

Настройка службы DHCP на Server2

Войдите в конфигурацию Server2 и на вкладке DHCP настройте службу DHCP. Для этого наберите новые значения пула, установите переключатель **On** и нажмите на кнопку **Save** (Сохранить) - рис. 6.14.

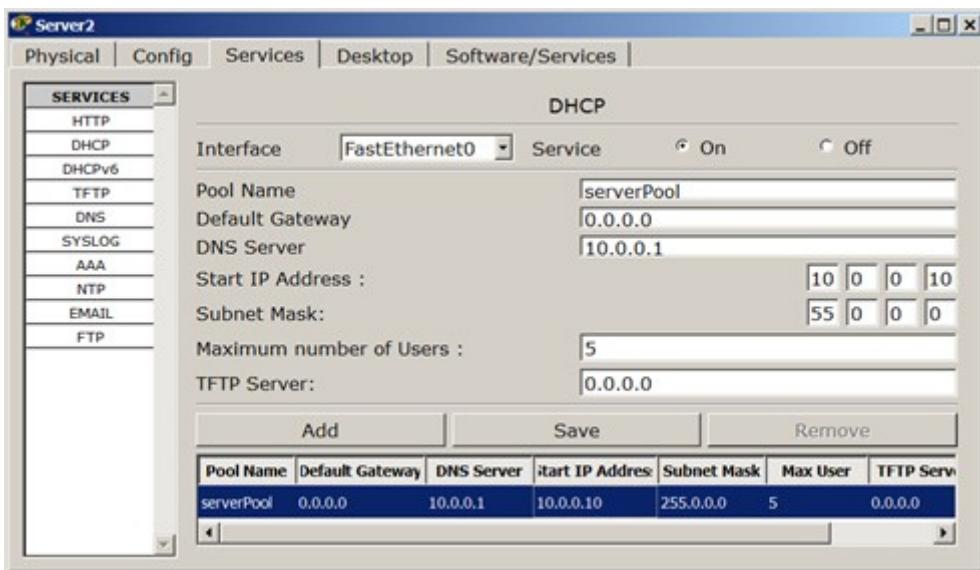


Рис. 6.14. Настройка DHCPсервера.

Проверка работы клиентов

Войдите в конфигурации хоста PC1и PC2 и в командной строке сконфигурируйте протокол TCP/IP. Для этого командой PC>ipconfig /release сбросьте (очистите) старые параметры IP адреса (рис. 6.15).

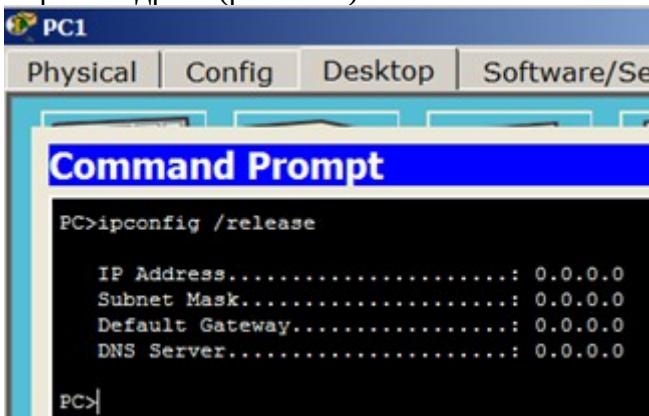


Рис. 6.15. Удаление конфигурации IP-адресов для всех адаптеров

Примечание

Команда **ipconfig /release** отправляет сообщение **DHCP RELEASE** серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан). Этот ключ отключает протокол

приведена на рис. 6.19. С помощью настроек ПК, представленных на рисунке, мы указываем хосту, что он должен получать IP адрес, адрес основного шлюза и адрес DNS сервера от DHCP сервера.

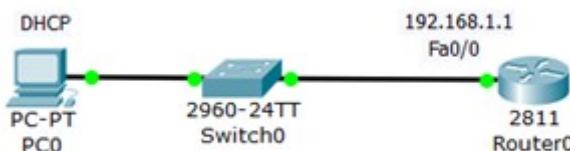


Рис. 6.19. Схема сети

Произведем настройку R0:

Router (config)#ipdhcpool TST создаем пул IP адресов для DHCP сервера с именем TST

Router (dhcp-config)#network 192.168.1.0 255.255.255.0 указываем из какой сети мы будем раздавать IP адреса (первый параметр - адрес данной сети, а второй параметр ее маска)

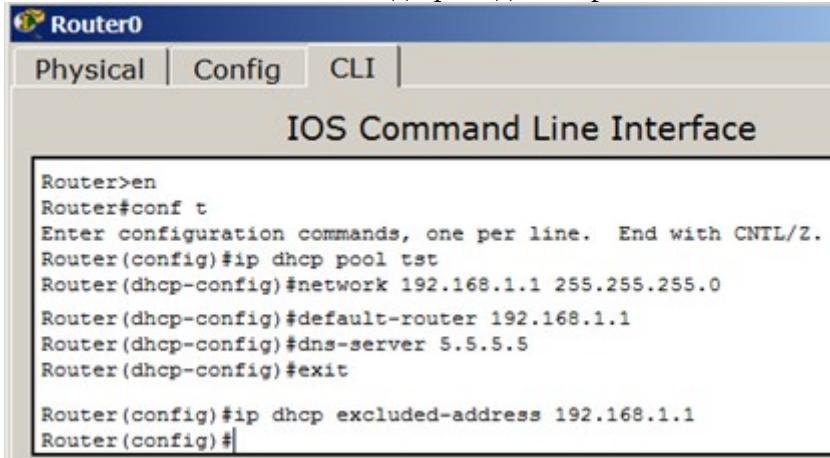
Router (dhcp-config)#default-router 192.168.1.1 указываем адрес основного шлюза, который будет рассыпать в сообщениях *DHCP*

Router (dhcp-config)#dns-server 5.5.5.5 указываем адрес *DNS* сервера, который так же будет рассыпаться хостам в сообщениях *DHCP*

Router (dhcp-config)#exit

Router (config)#ip dhcp excluded-address 192.168.1.1 этот хост исключен из пула, то есть, ни один из хостов сети не получит от *DHCP* сервера этот адрес.

Полный листинг этих команд приведен на рис. 6.20.



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool tst
Router(dhcp-config)#network 192.168.1.1 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 5.5.5.5
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#[
```

Рис. 6.20. Команды для конфигурирования R0

Проверим результат получения динамических параметров для PC0 (рис. 6.21).

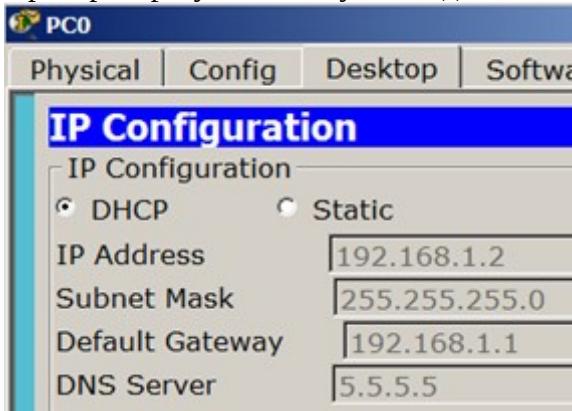
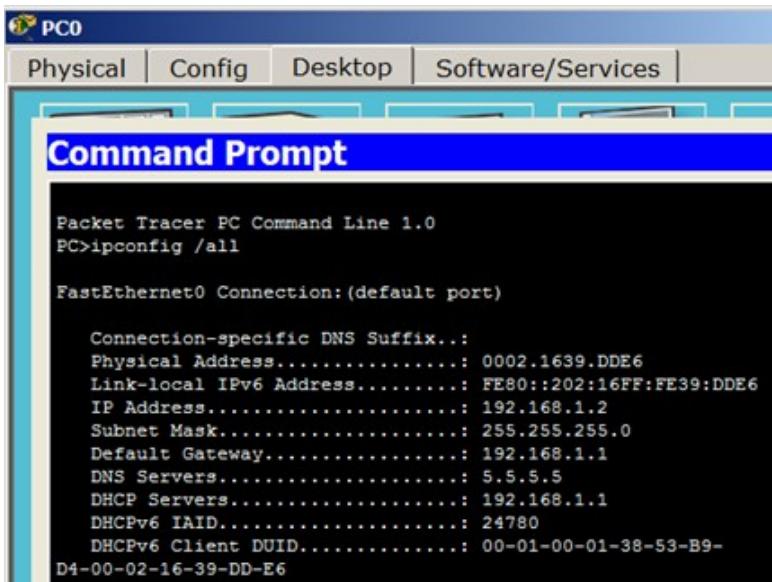


Рис. 6.21. DHCP работает

Проверим работоспособность *DHCP* сервера на хосте PC0 командой **ipconfig /all** (рис. 6.22).



```
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0002.1639.DDE6
Link-local IPv6 Address....: FE80::202:16FF:FE39:DDE6
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 5.5.5.5
DHCP Servers.....: 192.168.1.1
DHCPv6 IAID.....: 24780
DHCPv6 Client DUID.....: 00-01-00-01-38-53-B9-
D4-00-02-16-39-DD-E6
```

Рис. 6.22. Хост получил настройки от *DHCP* сервера

Хост успешно получил IP адрес, адрес шлюза и адрес DNS сервера от DHCP сервера R0.

2. Настройки интерфейса маршрутизатора в качестве DHCP клиента

Схема сети показана на рис. 6.23.

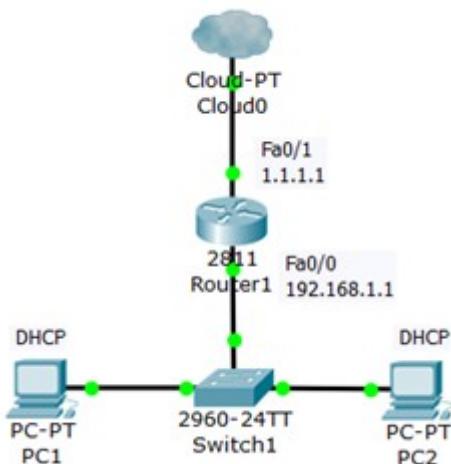


Рис. 6.23. Схема сети

Конфигурируем интерфейс Fa0/0 для R1 (рис. 6.24).

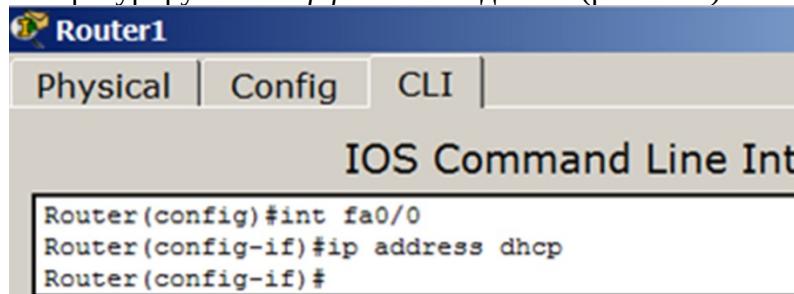


Рис. 6.24. Конфигурируем интерфейс маршрутизатора

Наблюдаем результат (рис. 6.25).

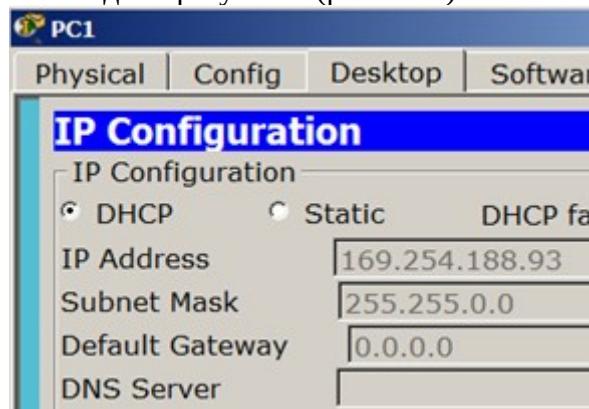


Рис. 6.25. DHCP не работает

После настройки интерфейса роутера на получение настроек по DHCP, DHCP клиент на PC1 перестал получать IP - адрес – IP из диапазона 169.254.x.x/16 назначается автоматически самим ПК при проблемах с получением адреса по DHCP. Интерфейс роутера IP - адрес так же не получит т.к. в данной подсети нет DHCP серверов. Описанные выше схемы представлены в виде одного файла - task-6-3.pkt.

Практическая работа 6-2-2. DHCP сервис на маршрутизаторе 2811

В этом примере мы будем конфигурировать маршрутизатор 2811, а именно, настраивать на нем DHCP сервер, который будет выдавать по DHCP адреса из сети 192.168.1.0 (рис. 6.26). PC1 и PC2 буду получать настройки динамически, а для сервера желательно иметь постоянный адрес, т.е., когда он задан статически.

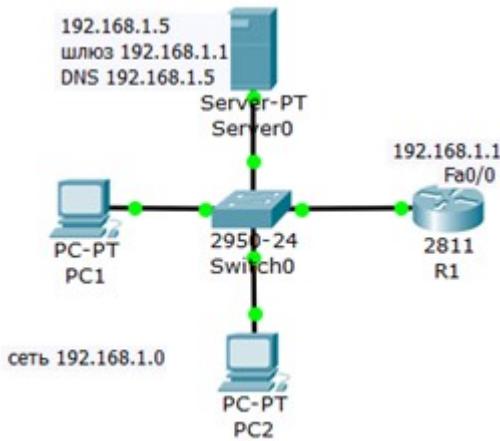


Рис. 6.26. Схема сети

Примечание

Как устройство с постоянным адресом здесь можно включить еще и принтер.

Резервируем 10 адресов

```
R1 (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Примечание

Этой командой мы обязали маршрутизатор R1 не выдавать адреса с 192.168.1.1 по 192.168.1.10 потому, что адрес 192.168.1.1 будет использоваться самим маршрутизатором как шлюз, а остальные адреса мы зарезервируем под различные хосты этой сети.

```
R1 (config)#ip dhcp pool POOL1R1 (dhcp-config)#network 192.168.1.0 255.255.255.0R1 (dhcp-config)#default-router 192.168.1.1R1 (dhcp-config)#domain-name my-domain.comR1 (dhcp-config)#dns-server 192.168.1.5
```

Примечание

Согласно этим настройкам выдавать адреса из сети 192.168.1.0 (кроме тех, что мы исключили) будет маршрутизатор R1 через шлюз 192.168.1.1.

Настраиваем интерфейс маршрутизатора

```
R1 (config)#interface fa0/0R1 (config-if)#ip address 192.168.1.1 255.255.255.0R1 (config-if)#no shutdownR1 (config-if)#exitR1(config)#exitR1#
```

Примечание

Команда **noshut** (сокращение от **no shutdown**) используется для того, чтобы бы интерфейс был активным. Обратная команда – **shut**, выключит интерфейс.

Проверка результата

Теперь оба ПК получили настройки и командой R1#show ip dhcp binding можно посмотреть на список выданных роутером адресов (рис. 6.27).

Консоль IOS Command Line Interface (CLI) на маршрутизаторе R1. Видны вкладки Physical, Config, CLI и вывод команды show ip dhcp binding, который показывает выданные адреса:

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.11	000A.F337.2447	--	
192.168.1.12	0060.3E33.BC81	--	

Рис. 6.27. Адреса выдаются автоматически, начиная с адреса 192.168.1.11

Итак, мы видим, что протокол *DHCP* позволяет производить автоматическую настройку сети на всех компьютерах (рис. 6.28).

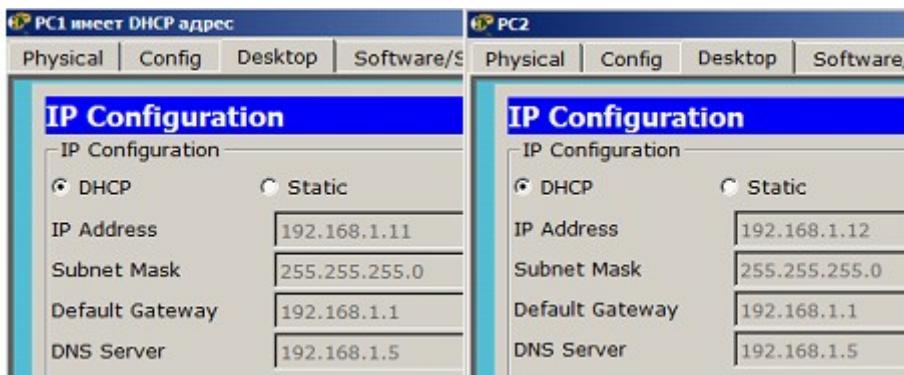
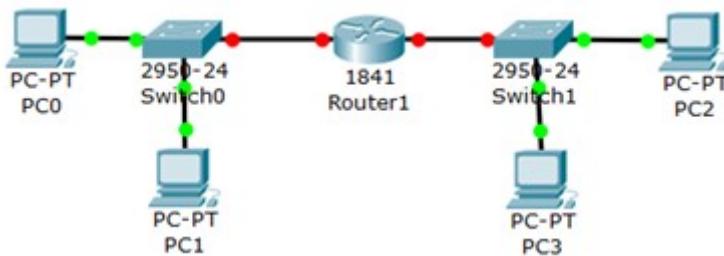


Рис. 6.28. PC1 и PC2 получают IP адреса от DHCP сервера

Рабочая сеть данного задания прилагается виде файла - task-6-4.pkt.



Задание.

Студент должен:

1. Выполнить весь пример по настройке связи двух сетей
2. Покажите преподавателю Шаг 1. Настройку ПК
3. Покажите преподавателю Шаг 2. Настройку роутера (маршрутизатора)
4. Покажите преподавателю Шаг 3. Проверку связи сетей
5. Какой протокол следит за тем, чтобы в сети не было повторения IP адресов? (ARP)
6. Как шлюз по умолчанию для узлов сети связан с портами маршрутизатора?

В процессе выполнения задания необходимо:

1. Задать IP адреса сетевым интерфейсам маршрутизаторов, интерфейсам управления коммутаторов и сетевым интерфейсам локальных компьютеров;
2. Установить связь на физическом и канальном уровнях между соседними маршрутизаторами по последовательному сетевому интерфейсу;
3. Добиться возможности пересылки данных по протоколу IP между соседними объектами сети (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2, и т.д.);
4. Настроить на маршрутизаторе R2 статические маршруты к сетям локальных компьютеров C1, C3
5. Настроить на маршрутизаторах R1, R3 маршруты "по умолчанию" к сетям локальных компьютеров C2-C3 и C1-C2 соответственно;
6. Добиться возможности пересылки данных по протоколу IP между любыми объектами сети (ping);
7. Переключившись в "Режим симуляции" рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой), пояснить роль протокола ARP в этом процессе.

Литература.

1. [Документация ECSS-10, версия 3.14.10](#)

Практическая работа 26

Тема: Соединение двух АТС по IP-маршрутизации и цифровому потоку

Теоретический материал

Специальные термины и понятия

Маршрутизатором (шлюзом), называется узел сети с несколькими IP-интерфейсами (содержащими свой MAC-адрес и IP-адрес), подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю. Как уже отмечалось, **динамическая маршрутизация** — это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами.

Маршрутизатор будет обновлять сведения о каждой подключенной к нему сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется **статическая маршрутизация**, обновить таблицы маршрутизации на всех устройствах придется системному администратору.

Статическая маршрутизация позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого **маршрута по умолчанию** — default (0.0.0.0), который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default.

Схема у нас будет следующая: два коммутатора 2950-24, два ПК в сети 192.168.10.0 с маской 255.255.255.0. Сервер и компьютер в сети 192.168.20.0 с маской 255.255.255.0. Сеть между маршрутизаторами (марки 1841) 192.168.1.0 с маской 255.255.255.252. Компьютеры из сети 192.168.10.0 должны достичься к DNSсерверу в сети 192.168.20.0 (рис. 7.12).

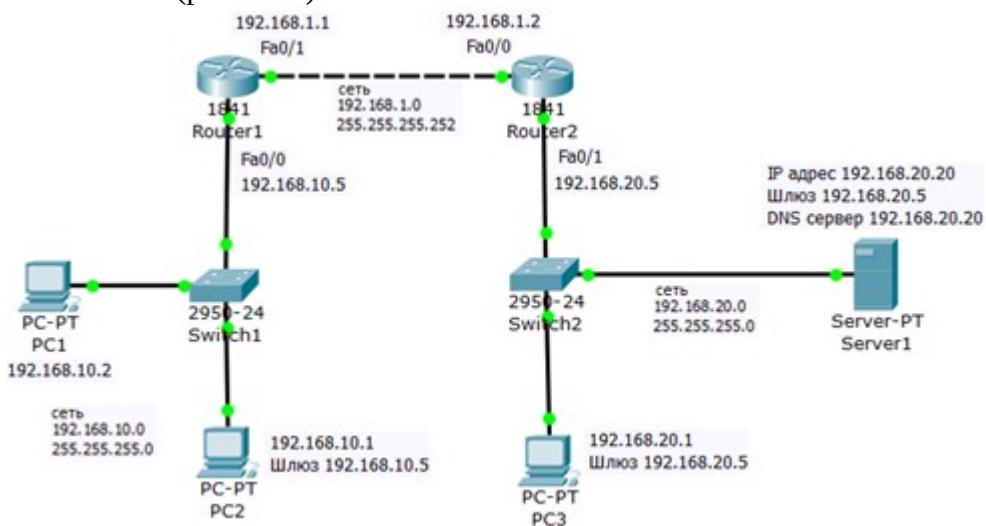


Рис. 7.12. Постановка задачи

Сеть у нас не сложная, ПК в ней немного, поэтому будем использовать не динамическую, а статическую маршрутизацию.

Настройки сетевых интерфейсов роутеров

Будем настраивать связь роутеров через порты Fa0/1 для R1 и Fa0/0 для R2. Настраиваем Router1 исходя из постановки задачи о том, что сеть между маршрутизаторами 192.168.1.0 с маской 255.255.255.252. Поэтому порту Fa0/1 присвоим IP адрес 192.168.1.1 (рис. 7.13).

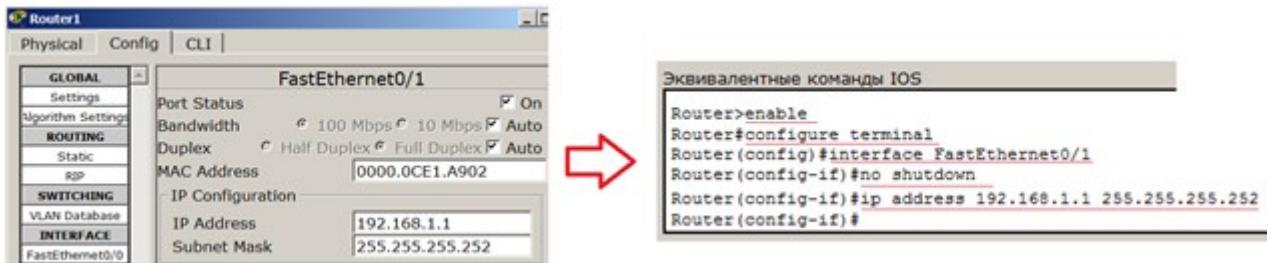


Рис. 7.13. Настраиваем порт 0/1 для маршрутизатора R1

Важно

При конфигурировании через webинтерфейс обязательно установите флајок **On** (Вкл.), что эквивалентно команде **nosh**.

Примечание

Как вариант, все параметры маршрутизатор можно настроить из командной строки на вкладке CLI следующими командами: **enable** (включаем привилегированный режим), **configterminal** (входим в режим конфигурации), **interface fastethernet0/1** (настраиваем интерфейс 100 мбEthernet 0/1), **ipaddress 192.168.1.1 255.255.255.252** (прописываем ip адрес интерфейса и маску сети маршрутизатора), **noshutdown** (включаем интерфейс - по умолчанию все выключено), **exit** (выходим из режима конфигурирования интерфейса), **end** (закончили редактирование), **write** (сохранили конфигурацию).

Аналогично настраиваем Router2 исходя из постановки задачи о том, что сеть между маршрутизаторами 192.168.1.0 с маской 255.255.255.252. Порту Fa0/0 присвоим IP адрес 192.168.1.2 (рис. 7.14).

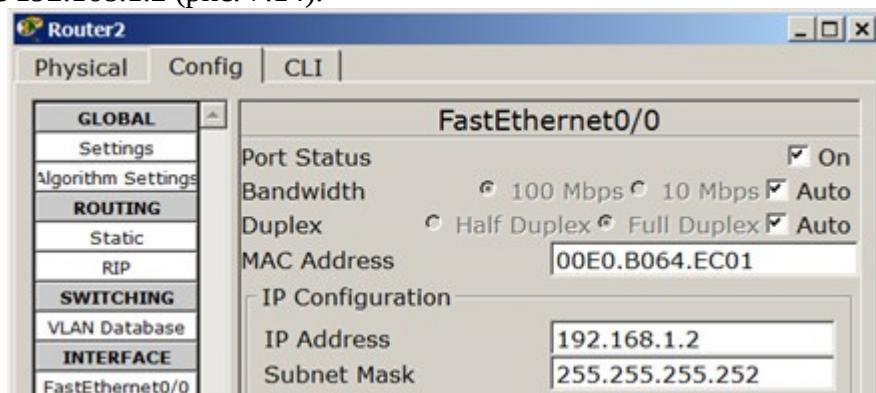


Рис. 7.14. Конфигурируем R2

Примечание

При конфигурировании роутера из командной строки можно использовать сокращенную форму записи команд: **en** (включаем расширенный режим), **conf t** (входим в режим конфигурации), **int fa0/0** (настраиваем интерфейс 100 мб.Ethernet 0/0), **Ip addr192.168.1.2 255.255.255.252** (прописываем ip адрес интерфейса и маску сети), **Noshut** (включаем интерфейс - по умолчанию он выключен), **exit** (выходим из режима конфигурирования интерфейса), **end** (заканчиваем редактирование), **wr** (сохраняем конфигурацию).

В итоге после настройки маршрутизаторов на портах загораются зеленые маркеры, то есть, связь между ними есть. Сеть между маршрутизаторами работает, но маршрутизации пока нет, то есть, из одной сети в другую попасть нельзя.

Настройка связи маршрутизаторов с подсетями (настройка шлюзов)

Настроим порт Fa0/0 маршрутизатора R1 на работу с сетью 192.168.10.0 (рис. 7.15).

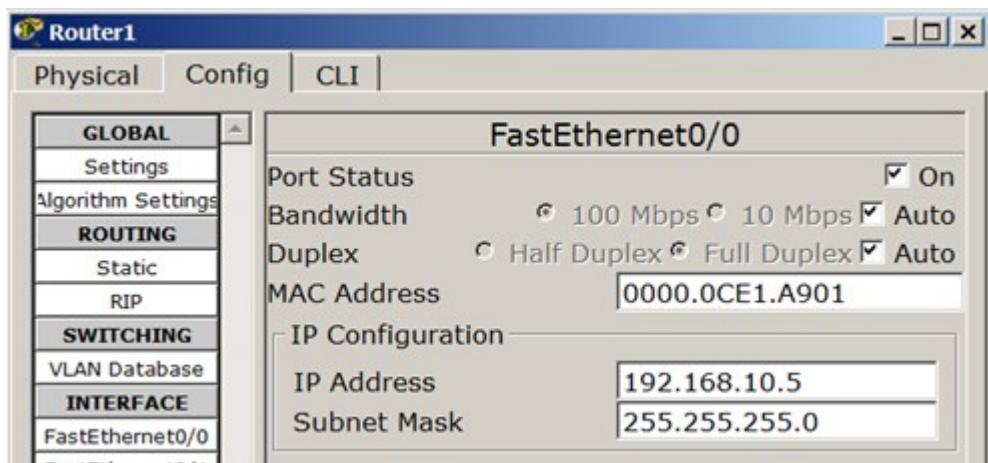


Рис. 7.15. Настроим портFa0/0 маршрутизатораR1 на работу с сетью 192.168.10.0

Аналогично порт Fa0/1 маршрутизатора R2 настроим на работу с сетью 192.168.20.0 (рис. 7.16).

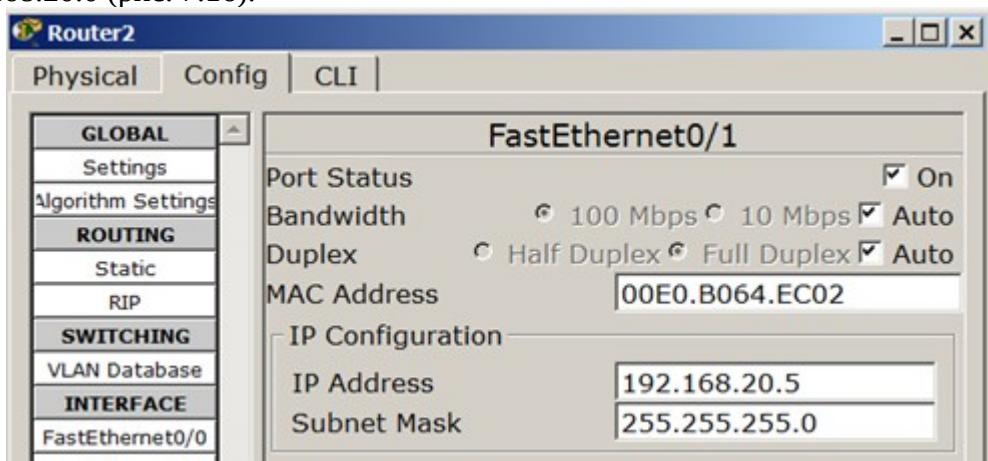


Рис. 7.16. Порт Fa0/1 маршрутизатораR2 настроим на работу с сетью 192.168.20.0

Как теперь видно по маркерам – сеть поднялась (Up), то есть все индикаторы горят зеленым цветом.

Настройка PC1 и PC2

Продолжим работу и настроим компьютеры в сети 192.168.10.0, то есть, нужно задать IP компьютеров, маску сети и основной шлюз. По исходным условиям задачи у нас слева пара компьютеров в сети 192.168.10.0 с маской 255.255.255.0 (рис. 7.17).

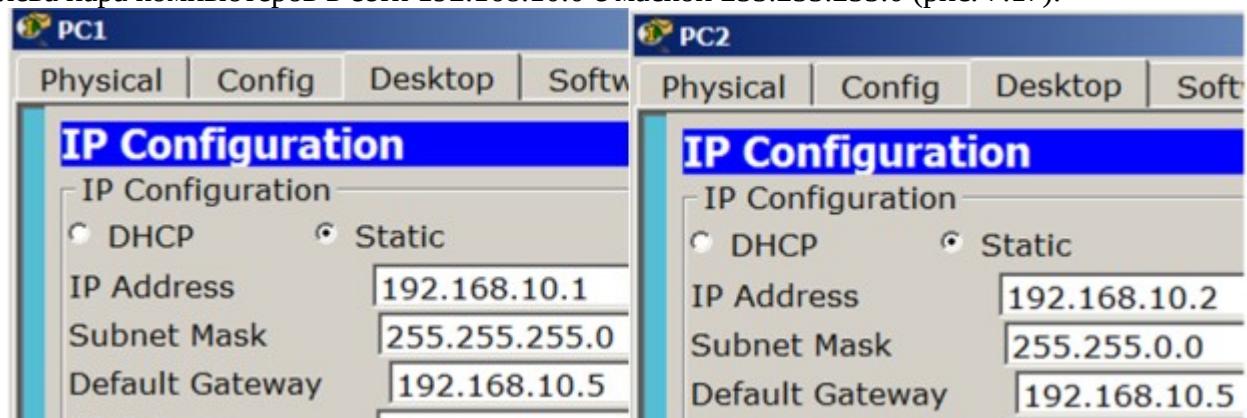


Рис. 7.17. Настраиваем PC1 и PC2

Новый термин

Основной шлюз (DefaultGateway) – это адрес, куда компьютер отправляет пакет, если не знает, куда его отправить. Например, при попытке узла Б отправить данные узлу А. в отсутствие конкретного адреса к узлу А, узел Б направляет трафик TCP/IP, предназначенный для узла А, своему основному шлюзу.

Настройка сервера и PC3

Далее нужно настроить PC3 и сервер в сети 192.168.20.0 (рис. 7.18 и рис. 7.19).

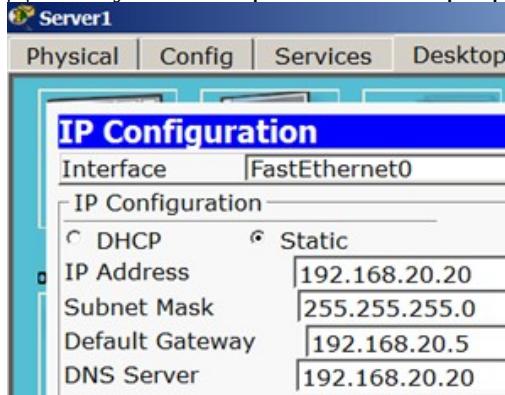


Рис. 7.18. Настройка сервера

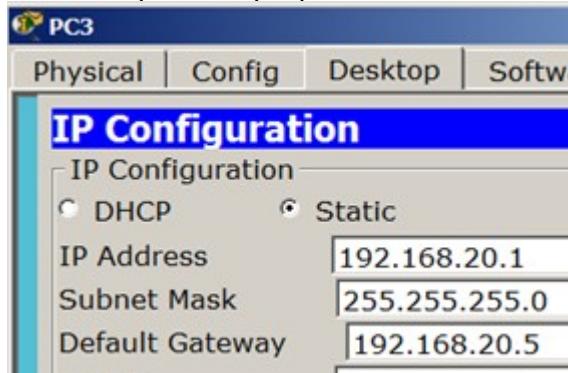


Рис. 7.19. Настраиваем PC2

Далее мы изучим статическую маршрутизацию в локальных сетях, рассмотрев этот вопрос на двух практических примерах.

Схема сети для настройки статической маршрутизации приведена на рис. 7.25.

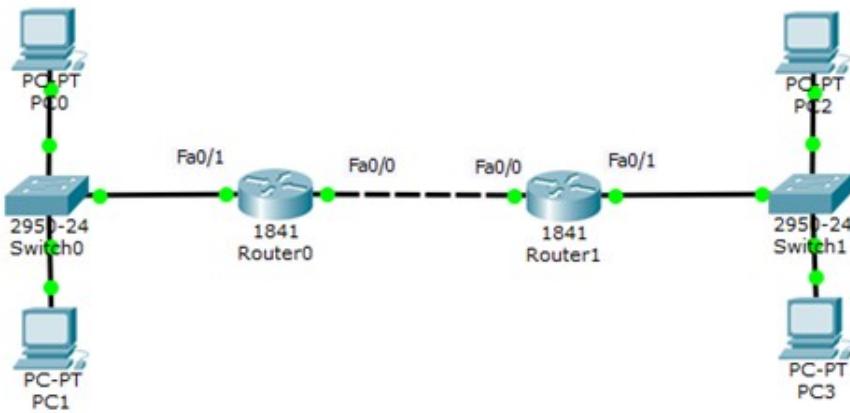


Рис. 7.25. Схема сети

Если сейчас командой `showiproute` посмотреть таблицу маршрутизации на R0 и R1, то увидим следующее (рис. 7.26 и рис. 7.27).

```

Router#sh ip route
Gateway of last resort is not set

C      10.0.0.0/8 is directly connected, FastEthernet0/1
C      192.168.1.0/24 is directly connected, FastEthernet0/0
Router#

```

Рис. 7.26. Таблица маршрутизации на 1-ммаршрутизаторе

```

Router>en
Router#sh ip route
Gateway of last resort is not set

C      10.0.0.0/8 is directly connected, FastEthernet0/1
C      192.168.1.0/24 is directly connected, FastEthernet0/0
Router#

```

Рис. 7.27. Таблица маршрутизации на 2-ммаршрутизаторе

Мы видим, что в данный момент в нашей таблице есть только сети, подключенные напрямую. R0 не знает сеть 10.1.2.0, а R1 не знает сеть 10.1.1.0. Поэтому, чтобы настроить маршрутизацию, следует добавим эти маршруты в таблицы маршрутизаторов:

R0 (config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2 R1 (config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

Теперь снова выведем таблицы маршрутизации наших устройств (рис. 7.28).

```

Router#sh ip route
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.0.0.0/8 is directly connected, FastEthernet0/1
S      10.1.2.0/24 [1/0] via 192.168.1.2
C      192.168.1.0/24 is directly connected, FastEthernet0/0
Router#

Router#sh ip route
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.0.0.0/8 is directly connected, FastEthernet0/1
S      10.1.1.0/24 [1/0] via 192.168.1.1
C      192.168.1.0/24 is directly connected, FastEthernet0/0
Router#

```

Рис. 7.28. Маршрутизация настроена

Теперь 1-й маршрутизатор знает, что пакеты, направляемые в подсеть 10.1.2.0 можно переслать маршрутизатору с ip адресом 192.168.1.2, а 2-й маршрутизатор знает, что пакеты, направляемые в подсеть 10.1.1.0 можно переслать маршрутизатору с ip адресом 192.168.1.1. Проверяем связь ПК из разных сетей (рис. 7.29).

```

PC0
Physical | Config | Desktop | Software/Services |
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 10.1.2.3

Pinging 10.1.2.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.1.2.3: bytes=32 time=1ms TTL=126
Reply from 10.1.2.3: bytes=32 time=0ms TTL=126

Ping statistics for 10.1.2.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Рис. 7.29. Статическая маршрутизация настроена – PC0 может общаться с PC3

Описанная сеть на двух маршрутизаторах (файл task-7-3.pkt) прилагается.

Статическая маршрутизация для пяти сетей и роутеров с тремя портами

В этом примере мы соберем и настроим следующую схему сети (рис. 7.30).

Схема сети

На данной схеме имеется пять сетей: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. В качестве шлюза по умолчанию у каждого компьютера указан интерфейс маршрутизатора, к которому он подключен. Маска у всех ПК одна - 255.255.255.0. Маска маршрутизаторов для каждого порта своя: Fa0/0 - 255.255.255.0, Fa0/1 - 255.255.0.0, Fa1/0 - 255.255.255.252.

На данной схеме имеется пять сетей: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. В качестве шлюза по умолчанию у каждого компьютера указан интерфейс маршрутизатора, к которому он подключен. Маска у всех ПК одна - 255.255.255.0. Маска маршрутизаторов для каждого порта своя: Fa0/0 - 255.255.255.0, Fa0/1 - 255.255.0.0, Fa1/0 - 255.255.255.252.

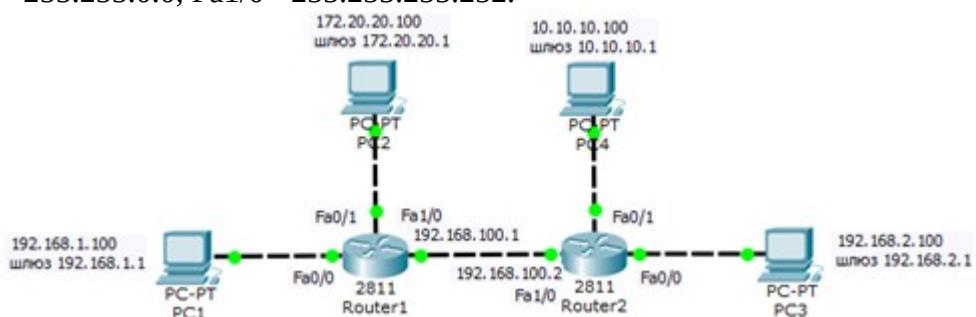


Рис. 7.30. Связь сетей посредством маршрутизаторов

Далее соединим маршрутизаторы между собой нам потребуется добавить к маршрутизатору интерфейсную плату NM-1FE-TX (NM – Networkmodule, 1FE – содержит один порт FastEthernet, TX – поддерживает 10/100MBase-TX). Чтобы это сделать перейдите к окну конфигурации маршрутизатора0, выключите его, щелкнув на кнопке питания. После этого перетяните интерфейсную плату NM-1FE-TX в разъем маршрутизатора (рис. 7.31). После того как карта добавлена, еще раз щелкните по

тумблеру маршрутизатора, чтобы включить его. Повторите аналогичные действия со вторым маршрутизатором.



Рис. 7.31. Вставляем интерфейсную плату в маршрутизатор

Задание.

Нам требуется произвести необходимые настройки для того, чтобы все ПК могли общаться друг с другом, то есть, необходимо обеспечить доступность компьютеров из разных сетей между собой.

В настоящий момент если мы отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2, то ICMP пакет слева дойдет до этого маршрутизатора, но при отправке ICMP пакетов в обратном направлении с адреса 192.168.100.2 на адрес 192.168.1.100 возникнет проблема. Дело в том, что маршрутизатор R2 не имеет в своей таблице маршрутизации информации о сети 172.20.20.0, так как шлюз по умолчанию мы еще не прописывали и маршрутизатор R2 не знает, куда отправлять ответы на запрос. В небольших сетях самым простым способом настроить маршрутизацию, является добавление маршрута по умолчанию. Для того чтобы это сделать выполните на маршрутизаторе R1 в режиме конфигурирования следующие команды (рис. 7.32).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
[OK]
Router#
```

Рис. 7.32. Настройка маршрута по умолчанию на R1

Примечание

В этих командах первая группа цифр 0.0.0.0 обозначают IP адрес сети назначения, следующая группа цифр 0.0.0.0 обозначает её маску, а последние цифры – 192.168.100.2 это IP адрес интерфейса, на который необходимо передать пакеты, чтобы попасть в данную сеть. Если мы указываем в качестве адреса сети 0.0.0.0 с маской 0.0.0.0, то

данный маршрут становится маршрутом по умолчанию, и все пакеты, адреса назначения которых, прямо не указаны в таблице маршрутизации будут отправлены на него.

На правом маршрутизаторе R2 поступаем аналогично (рис. 7.33).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.100.1
Router(config)#end
Router#
*SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
[OK]
Router#
```

Рис. 7.33. Настройка маршрута по умолчанию на R2

Отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2 и посмотрим, что изменилось (рис. 7.34).

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Рис. 7.34. С компьютера PC1 с IP адресом 192.168.1.100 успешно пингуем интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2

Описанная выше, полностью рабочая сеть (файл task-7-4.pkt) прилагается.

Форма отчета.

Резюме

Допустим, мы хотим пропинговать с компьютера PC1 с адресом 192.168.1.100 (из левой сети) компьютер PC4 с IP адресом 10.10.10.100 (из правой сети). В качестве шлюза по умолчанию на компьютере с адресом 192.168.1.100 установлен адрес 192.168.1.1интерфейса Fa0/0 маршрутизатора R1. Сначала компьютер будет искать в своей таблице маршрутизации адрес 10.10.10.100, а после того, как он его не найдет, ICMP пакеты будут отправлены на адрес по умолчанию, то есть на интерфейс маршрутизатора R1 с адресом 192.168.1.1 (порт Fa0/0). Получив пакет, маршрутизатор R1 просмотрит адрес его назначения – 10.10.10.100 и также попытается обнаружить его в своей таблице маршрутизации. Когда он не обнаружит и его, пакет будет отправлен на

интерфейс Fa1/0, с адресом 192.168.100.2 маршрутизатора R2. Маршрутизатор R2 попробует обнаружить в своей таблице маршрутизации маршрут к адресу 10.10.10.100. Когда это не увенчается успехом, маршрутизатор будет искать маршрут к сети 10.0.0.0. Информация о данной сети содержится в таблице маршрутизации, и маршрутизатор знает, что для того чтобы попасть в данную сеть необходимо отправить пакеты на интерфейс FastEthernet0/1, непосредственно к которому подключена данная сеть. Так как в нашем примере вся сеть 10.0.0.0, представляется из себя всего 1 компьютер, то пакеты сразу же попадают в место назначения, то есть, на компьютер с IP адресом 10.10.10.100. При отсылке ответных ICMP пакетов, все происходит аналогичным образом. Однако, не всегда можно обойтись указанием только маршрутов по умолчанию. В более сложных сетевых конфигурациях может потребоваться прописывать маршрут для каждой из сетей в отдельности. Это будет непросто. Поэтому в больших сетях обычно используют не статическую, а динамическую маршрутизацию.

Практическая работа 27

Тема: Конфигурирование нумерационного плана при соединении двух АТС

Теоретический материал

Ключевые слова: маршрутизация, динамическая маршрутизация, RIP, OSPF, протокол маршрутизации, метрика, маршрут, UDP, сеть, алгоритм, адрес, безопасность, маршрутизатор, вектор, NEXT, hop, EIGRP, надежность, базы данных, связь, значение, OPEN, path, First, LSA, стоимость, деление, канал передачи данных, SPF, маска, accesslist, доступ, Интернет, прямой, префикс

Маршрутизация - процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. **Динамическая маршрутизация** может быть осуществлена с использованием одного и более протоколов (RIP v2, OSPF и др.).

Новый термин

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP).

Каждый протокол маршрутизации использует свою систему оценки маршрутов (метрику). Маршрут к сетям назначения строится на основе таких критериев как

- - количество ретрансляционных переходов
- - пропускная способность канала связи
- - задержки передачи данных и др.

Маршрутизаторы обмениваются друг с другом информацией о маршрутах с помощью служебных пакетов по протоколу UDP. Такой обмен информации увеличивает наличие дополнительного трафика в сети и нагрузку на эту сеть. Возможна также ситуация, при которой таблицы маршрутизации на роутерах не успевают согласоваться между собой, что может повлечь появление ошибочных маршрутов и потерю данных.

Протоколы маршрутизации делятся на три типа:

- Дистанционно векторные протоколы (RIP)
- Протоколы с отслеживанием состояния каналов (OSPF)
- Смешанные протоколы (EIGRP)
- И др.

Протокол RIP

RIP — протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути алгоритм Беллмана-Форда. Алгоритм маршрутизации RIP - один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст адрес. Максимальное количество

"хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (*метрика* 15). Ограничение в 15 хопов не дает применять *RIP* в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышенна *безопасность* за счет введения дополнительной маршрутной информации. Принцип дистанционно-векторного протокола: каждый *маршрутизатор*, использующий протокол *RIP* периодически широковещательно рассыпает своим соседям специальный пакет- *вектор*, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. *Маршрутизатор* получивший такой *вектор*, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет *вектор* информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный *вектормаршрутизатор* рассыпает всем своим соседям.

Маршрутизатор выбирает из нескольких альтернативных маршрутов *маршрут* с наименьшим значением метрики, а *маршрутизатор*, передавший информацию о таком маршруте помечается как следующий (*next hop*). Протокол непригоден для работы в больших сетях, так как засоряет сеть интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами *EIGRP* и *OSPF*.

Протокол *EIGRP* более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол *OSPF*. Также *EIGRP* имеет более продвинутый алгоритм вычисления метрики. В формуле вычисления метрики есть возможность учитывать загруженность и надежность интерфейсов на пути пакета. Недостатком протокола *EIGRP* является его ограниченность в его использовании только на оборудовании компании Cisco.

Протокол OSPF

Алгоритм работы протокола динамической маршрутизации *OSPF* основан на использовании всеми маршрутизаторами единой базы данных, описывающей, с какими сетями связан каждый *маршрутизатор*. Описывая каждую связь, маршрутизаторы связывают с ней метрику – значение, характеризующее "качество" канала связи. Это позволяет маршрутизаторам *OSPF* (в отличие от *RIP*, где все каналы равнозначны) учитывать реальную пропускную способность канала и выявлять наилучшие маршруты. Важной особенностью протокола *OSPF* является то, что используется групповая, а не широковещательная рассыпка (как в *RIP*), то есть, нагрузка каналов меньше.

OSPF (*Open Shortest Path First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала link-state (*LSA*). Основан на алгоритме для поиска кратчайшего пути. Отслеживание состояния канала требует отправки объявлений о состоянии канала (*LSA*) на активные интерфейсы всех доступных маршрутизаторов зоны. В этих объявлениях содержится описание всех каналов маршрутизатора и стоимость каждого канала. *LSA* сообщения отправляются, только если произошли какие-либо изменения в сети, но раз в 30 минут *LSA* сообщения отправляются в принудительном порядке. Протокол реализует деление автономной системы на зоны (*areas*). Использование зон позволяет снизить нагрузку на сеть и процессоры маршрутизаторов и уменьшить размер таблиц маршрутизации.

Описание работы протокола:

Все маршрутизаторы обмениваются специальными Hello-пакетами через все интерфейсы, на которых активирован протокол *OSPF*. Таким образом, определяются маршрутизаторы-соседи, разделяющие общий канал передачи данных. В дальнейшем hello-пакеты посыпаются с интервалом раз в 30 секунд. Маршрутизаторы пытаются перейти в состояние соседства со своими соседями. Переход в данное состояние определяется типом маршрутизаторов и типом сети, по которой происходит обмен hello-

пакетами, по зонному признаку. Пара маршрутизаторов в состоянии соседства синхронизирует между собой базу данных состояния каналов.

Каждый маршрутизатор посылает объявление о состоянии канала своим соседям, а каждый получивший такое объявление записывает информацию в базу данных состояния каналов и рассыпает копию объявления другим своим соседям. При рассылке объявлений по зоне, все маршрутизаторы строят идентичную базу данных состояния каналов. Каждый маршрутизатор использует алгоритм SPF для вычисления графа (дерева кратчайшего пути) без петель. Каждый маршрутизатор строит собственную маршрутизацию, основываясь на построенном дереве кратчайшего пути.

Конфигурирование протокола EIGRP

Ход работы.

Схема сети изображена на рис. 8.14.

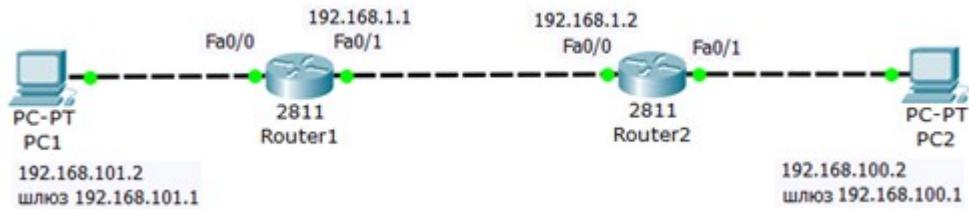


Рис. 8.14. Схема для конфигурации протокола EIGRP

Настройка протокола *EIGRP* очень похожа на настройку протокола *RIP*.

Программирование R1

Конфигурируем R1 (рис. 8.15).

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.101.1
Router(config-router)#exit
Router(config)#

```

Рис. 8.15. Конфигурирование R1

Программирование R2

Конфигурируем R2 (рис. 8.16).

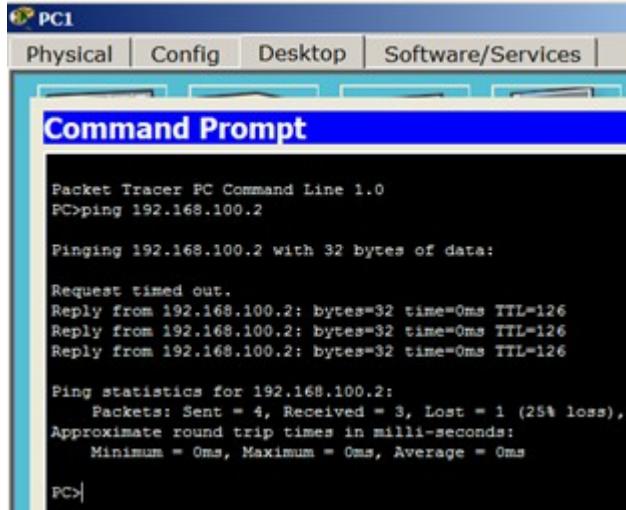
```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.100.1
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

```

Рис. 8.16. Конфигурирование R2

Проверка работы сети

Проверяем работу маршрутизаторов (рис. 8.17).



Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.100.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>

Рис. 8.17. Результат проверки работоспособности сети

Рабочая сеть данного примера представлена файлом task-8-3.pkt.

Задание 2.

Теоретический материал.

Прямая и обратная маска

В оборудовании **Cisco** иногда приходится использовать обратную маску, то есть не привычную нам **255.255.255.0** (Subnetmask — **прямая маска**), а **0.0.0.255** (Wildcardmask — **обратная маска**). Обратная маска используется в листах допуска (*accesslist*) и при описании сетей в протоколе **OSPF**. Прямая маска используется во всех остальных случаях. Отличие масок заключается также в том, что прямая маска оперирует сетями, а обратная — хостами. С помощью обратной маски вы можете, например, выделить во всех подсетях хости с конкретным адресом и разрешить им *доступ в Интернет*. Так, как чаще всего в локальных сетях используют адреса типа 192.168.1.0 с маской 255.255.255.0, то самая распространенная Wildcardmask (шаблонная маска или обратная маска, или инверсная маска) — маска 0.0.0.255.

Новый термин

Шаблонная маска (wildcardmask) — маска, указывающая на количество хостов сети. Является дополнением для маски подсети. Вычисляется по формуле для каждого из октетов маски подсети как 255-маска_подсети. Например, для сети 192.168.1.0 и маской подсети 255.255.255.242 шаблонная маска будет выглядеть как 0.0.0.13. Шаблонная маска используется в настройке некоторых протоколов маршрутизации, а также является удобным параметром ограничений в списках доступа.

Расчёт Wildcardmask

Существует связь, между обратной и прямой маской: в сумме эти маски по каждому разряду должны составлять 255. Пусть наша сеть 192.168.32.0 /28. Рассчитает wildcardmask: префикс /28 это 255.255.255.240 или 11111111.11111111.11111111.11110000. Для wildcardmask нам нужны только нули, то есть, 11110000 переводим в десятичное число и считаем: $128/64/32/16/8/4/2/1$ это будет $8+4+2+1=15$, т.е. наша wildcardmask будет равна 0.0.0.15.

Выполнить самостоятельно

Дана прямая маска **255.255.255.248**. Выполните расчет и докажите, что обратная равна **0.0.0.7**.

Пример конфигурирования протокола OSPF для 4-х устройств

Соберите схему, изображенную на рис. 8.18.

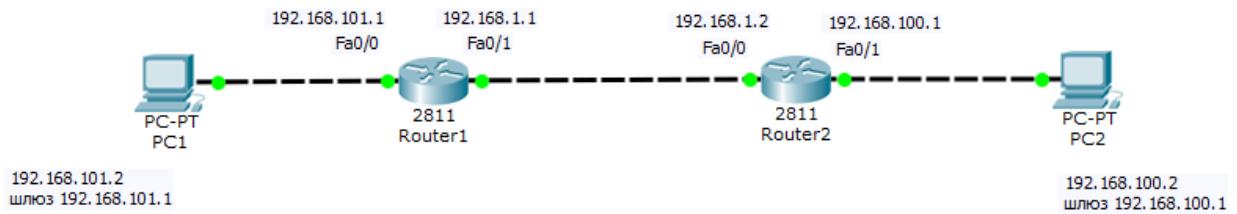


Рис. 8.18. Схема для конфигурации протокола OSPF

Настройка роутеров

Выполним конфигурирование R1 (рис. 8.19).

Router#router ospf 1
Router(config-router)#network 192.168.101.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit

Рис. 8.19. Настройка R1

Теперь выполним настройки R2 (рис. 8.20).

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.100.1 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#

Рис. 8.20. Настройка R2

Совет

Если вам потребуется в СРТ сбросить настройки роутера, то следует выключить его тумблер питания, а затем снова включить.

Проверка результата

Для проверки маршрутизации пропингуем ПК из разных сетей (рис. 8.21).

PC>ping 192.168.101.2
Pinging 192.168.101.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.101.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>

```

Рис. 8.21. Результат проверки работоспособности OSPF

Рабочая сеть данного примера представлена  файлом task-8-4.pkt.

Практическая работа 28

Тема: Конфигурация специфических функций АТС (голосовая почта, автосекретарь и др.)

Цель работы: научиться настраивать систему голосовой почты с записью сообщения и его воспроизведением.

Теоретические данные:

Голосовая почта – это электронная система для регистрации, сохранения и перенаправления телефонных голосовых сообщений (иногда – для розыска и оповещения пользователей).

В настоящее время под голосовой почтой понимают два вида сервисов, предоставляемых операторами и почтовыми серверами:

1. возможность для абонента телефонной сети оставить адресату голосовое сообщение, которое тот сможет прослушать позже;
2. возможность прослушать по телефону хранящиеся на сервере электронной почты сообщения.

Система голосовой почты предназначена для предоставления дополнительных услуг связи абонентам АТС (мини-АТС) и позволяет производить запись сообщений для абонентов при занятости телефонного номера или не ответе. В свободное время абонент может позвонить на номер голосовой почты и прослушать поступившие ему сообщения.

Одной из самых популярных (или, возможно, непопулярных) функций любой современной системы телефонной связи является голосовая почта. Естественно, Asterisk обладает достаточно гибкой системой голосовой почты. Среди ее возможностей можно упомянуть:

Неограниченные по размеру защищенные паролем ящики голосовой почты, в каждом из которых содержатся почтовые папки для организации сообщений голосовой почты.

- Различные приветствия для состояний «занято» и «недоступен».

- Возможность связывать телефоны с несколькими почтовыми ящиками, а почтовые ящики – с несколькими телефонами.
- Уведомление о поступлении сообщения голосовой почты по электронной почте с возможностью прикрепления сообщения голосовой почты в виде звукового файла.
- Индикатор ожидающих сообщений (мигающий световой индикатор или прерывистый тональный сигнал) во многих типах телефонов.
- Каталог ящиков голосовой почты служащих компаний.

Внутри каждого контекста голосовой почты определяются разные почтовые ящики. Для описания почтового ящика используется следующий синтаксис: почтовыйящик => пароль,имя[,email[,email_пейджера[,опции]]]

Поясним назначение каждой части описания почтового ящика:

Почтовыйящик – это номер почтового ящика. Обычно он соответствует добавочному номеру ассоциированного с ним телефонного аппарата.

Status – принимает значение Disable (выключено)/Enable (включено). Служить для активации голосовой почты абонента и деактивации.

Secret – числовой пароль, который будет использоваться владельцем почтового ящика для доступа к своей голосовой почте.

Email – это адрес электронной почты владельца ящика голосовой почты. Asterisk может посыпать уведомления о получении голосовой почты (включая само сообщение голосовой почты) на заданный ящик электронной почты.

Pager Email Address

Это электронный адрес пейджера или мобильного телефона владельца ящика голосовой почты. Asterisk может посыпать короткое сообщение, уведомляющее о получении голосовой почты, на заданный адрес электронной почты.

Настройка всех сервисных функций АТС

Абонентский сервис – это функция в IP-АТС Агат СУ, которая

позволяет организовывать профили для каналов в тех или иных режимах. То есть если нам необходимо настроить какое-либо переадресации или режим временной недоступности (DMD), голосовую почту и т.д., то мы переходим в раздел «Абонентский сервис».

1. Изучите раздел абонентского сервиса и настройте для разных абонентов разные сервисные функции, по их назначению исходя из варианта, согласно рисунку 9. Также создайте групповой профиль для нескольких абонентов сразу, исходя из рисунков 10-12.

2.

Имя профиля	Канал	Контакт	Пользователь (логин)	Назначен в каналах	Приоритет	Активен
отдел кадров	Менеджер	---		0	0	<i>По расписанию</i>
отдел продаж	7890	---		0	0	<i>Всегда</i>
техпо	7891	---	sip_local	0	0	<i>Всегда</i>

Рис. 40. Абонентский сервис

Каналы

admin
выход

Список каналов

Фильтр | Окно

Имя канала	Расположение	Номер в НП	Маршрутизация	Контакт	Профили АБС	Запись	Приоритет записи	Тип канала
<input checked="" type="checkbox"/> 12345	192.168.193.241	12345	Номерной план		отдел кадров / (0)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 12346	192.168.193.241	12346	Номерной план		отдел кадров / (1)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 12347		12347	Номерной план		отдел кадров / (1)	Нет	0	SIP-абонент
<input type="checkbox"/> Менеджер		11421	Номерной план					
<input type="checkbox"/> Начальник отдела	---	11422	Номерной план					
<input type="checkbox"/> Продажа		11419	Номерной план					
<input type="checkbox"/> ТехПо	---	11420	Номерной план					

ДЕЙСТВИЯ

Сохранить и выйти из редактирования

Сохранение и возврат в разговор

Прослушивание данного канала:

Рис. 41. Привязка каналов к групповому профилю

Каналы

Список каналов

Фильтр | Окно

Имя канала	Расположение	Номер в НП	Маршрутизация	Контакт	Профили АБС	Запись	Приоритет записи	Тип канала
<input checked="" type="checkbox"/> 12345		12345	Отдел Кадров		отдел кадров / (0)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 12346		12346	Отдел Кадров		отдел кадров / (1)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 12347		12347	Номерной план		отдел кадров / (1)	Нет	0	SIP-абонент

Список каналов

Фильтр | Окно

Имя канала	Расположение	Номер в НП	Маршрутизация	Контакт	Профили АБС	Запись	Приоритет записи	Тип канала
<input checked="" type="checkbox"/> 114		114	Отдел Кадров		отдел кадров / (0)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 115		115	Отдел Кадров		отдел кадров / (0)	Да	0	SIP-абонент
<input checked="" type="checkbox"/> 116		116	Номерной план		отдел кадров / (0)	Нет	0	SIP-абонент

Рис. 42. Результат настроек

The screenshot shows a configuration interface for the 'Abonent' service. On the left, there's a table of profiles assigned to channels. A specific row for 'отдел кадров' (HR department) is selected. To the right, a modal window titled 'КАНАЛЫ, НА КОТОРЫЕ НАЗНАЧЕН ПРОФИЛЬ' (Channels assigned to the profile) lists three channels: 12345, 12346, and 12347.

Имя профиля	Канал	Пользователь (логин)	Назначен в каналах	Приоритет	Активность
отдел кадров	---		3	2	Всегда вкл
отдел продаж	12346 sip_local		0	0	Всегда вкл
техно	12347 sip_local		0	0	По расписанию

^ КАНАЛЫ, НА КОТОРЫЕ НАЗНАЧЕН ПРОФИЛЬ

Имя канала	Номер в НП	Контакт
12345	12345	
12346	12346	
12347	12347	

Рис. 43. Результат настроек

2. Используйте раздел «Списки контактов», для создания черных (BNL) и белых (WNL) списков, и их применения в абонентском сервисе (Рисунок 13). Они позволяют создавать исключение и/или разрешение на определенный список контактов.

The screenshot shows the 'Списки контактов' (Contact Lists) section. It displays two lists: 'белый список' (white list) containing 3 entries and 'черный список' (black list) containing 4 entries. To the right, a detailed view of the 'белый список' is shown, with fields for 'Тип списка' (Type of list), 'Доступен для:' (Available for), and 'Имя Данных' (Name of Data).

Имя списка	Тип списка	Доступ	Записей	Комментарий	Имя данных 1	Имя данных 2	Имя данных 3
белый	Белый список	Все пользователи	3		200	400	600
черный	Черный список	Все пользователи	4		200	400	600

Рис. 44. Списки контактов

Часть 4. Создание и настройка звукового меню ivr

Звуковое меню IVR позволяет в автоматическом режиме принимать звонки и адресовать их на те или иные направления в зависимости от команд пользователя или его бездействия.

1. Для начала добавьте дополнительные звуковые файлы, для их использования в IVR, согласно рисунку 14. Звуковые файлы загружаются в "Менеджер звуковых файлов", после их загрузки нажмите кнопку "Сохранить медиа".

The screenshot shows the 'Менеджер звуковых файлов' (Sound File Manager) interface. It displays a file browser window showing audio files like 'HelloMusic.wav' and 'MainQueuePrompt.wav'. The main interface has sections for 'МЕДИАФАЙЛЫ ДЛЯ ЗАГРУЗКИ' (Media files for upload) and 'ДОСТУПНЫЕ МЕДИАФАЙЛЫ' (Available media files).

Рис. 45. Менеджер звуковых файлов

2. В разделе «IVR» создайте новую систему голосового меню, используя добавленные звуковые файлы (Рисунок 15).

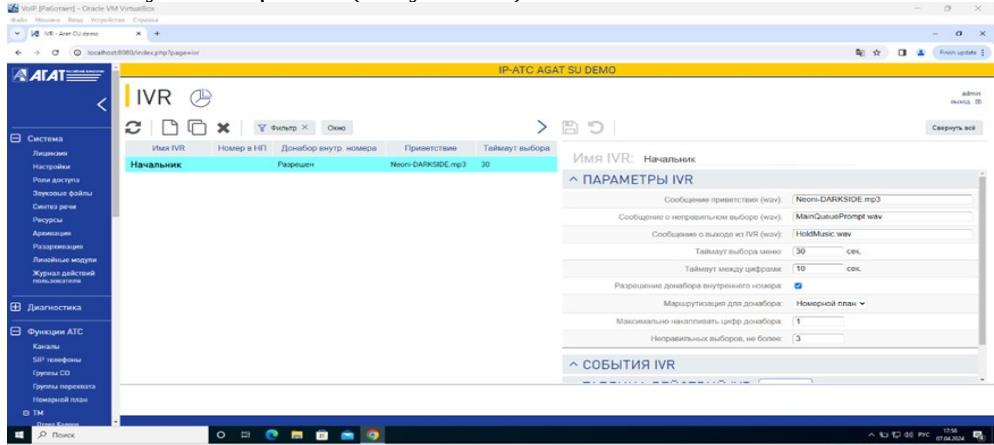


Рис. 46. IVR

3. Перейдите в таблицу действий IVR и с помощью кнопки "Добавить", добавьте необходимое количество строк с командами абонентов (Рисунок 16).

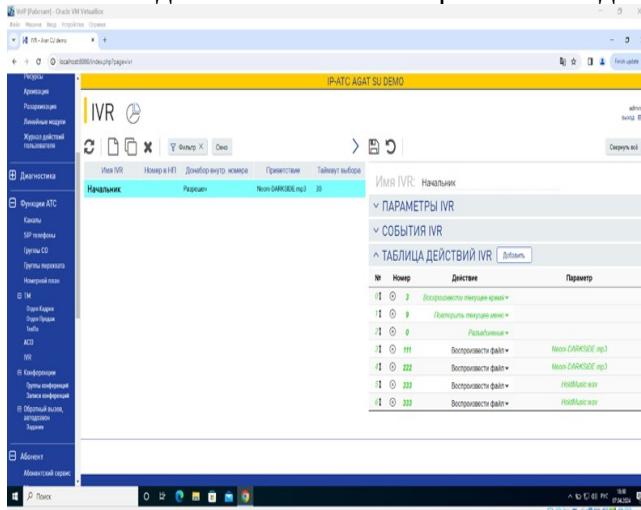


Рис. 47. Пример настройка таблицы действий IVR

Команда абонента включает в себя **Номер** - последовательность цифр или символов, который должен набрать абонент на номеронабирателе своего телефона. Он может состоять из одной или нескольких цифр / символов. После набора абонентом этой последовательности, IVR выполнит **Действие** с указанным **Параметром**.

С помощью функционала «Оповещения» IP-ATC Агат СУ может производить оповещение, как внутренних, так и внешних абонентов. Может производить оповещения в виде голосовых и текстовых сообщений. Также возможно преобразования текстового сообщения в голосовое с помощью встроенного функционала синтеза речи (TTS).

Расписание позволяет адресовать звонки в различных направлениях в зависимости от текущего времени на АТС. Расписание используется для абонентского сервиса, оповещения и автоматической архивации данных.

Часть 1. Подготовка списков абонентов оповещения

1. В разделе «Список контактов» создали новый список общего назначения с доступом всем пользователям (См. Рис. 1).

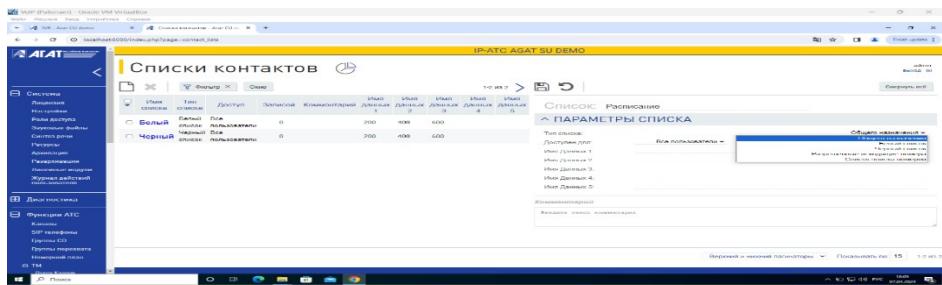


Рис. 1. Создание списка контактов

2. Перешли в созданный список, нажав на его название (См. Рис. 2). Создали абонентов с фамилиями участников бригады.

Абонент	Отдел	Должность	Основной контакт	Тип осн. контакта	Контакт 1	Тип контакта 1	Кс
Травкина Елизавета Алексеевна			12901	Моб тлф	13468987	СМС	
Федченко Александра Сергеевна			23141	Моб тлф		Не определен	
Ящук Анастасия Александровна			473826	Не определен		Не определен	

Рис. 2. Создание абонента

3. Создали абонентов в разделе «Контакты» по данным участников бригады и добавили их автоматическим вводом в список контактов (См. Рис. 49-50).

ИНФОРМАЦИЯ О КОНТАКТЕ

Федченко Александра Сергеевна

Организация: Наша организация
Должность: Начальник
Подразделение:
Звание: Роль:

КОНТАКТЫ

1-3 из 3

Рис. 3. Создание контакта

ДАННЫЕ ОБ АБОНЕНТЕ

Абонент: Ящук

12901

КОНТАКТНЫЕ ДАННЫЕ

Номер абонента	Тип номера
Основной:	Не определен
Дополнительный 1:	Не определен
Дополнительный 2:	Не определен
Дополнительный 3:	Не определен

Рис. 3. Добавление существующего контакта

4. Далее задали каждому абоненту индивидуальные параметры звона до абонента при оповещении (См. Рис. 51).

The screenshot shows a list of contacts on the left and a detailed configuration window on the right. The contacts listed include Травкина, Травкина Елизавета Алексеевна, Федченко, Федченко Александр Сергеевна, Ящук, and Ящук Анастасия Александровна. The configuration window displays the following parameters for the selected contact (Ящук Анастасия Александровна):

- Абонент:** Ящук Анастасия Александровна
- ПАРАМЕТРЫ ДОЗВОНА ДО АБОНЕНТА ПРИ ОПОВЕЩЕНИИ**
- ОБЩИЕ**
- Приоритет:** 3
- Персональный код подтверждения получения сообщения оповещения:** 14253
- Количество попыток оповещения ('0' - согласно настройкам Группы оповещения):** 3
- Время до следующей попытки звона ('0' - согласно настройкам Группы оповещения):** 60 сек.

Рис. 4. Параметры звона до абонента при оповещении

Часть 2. Создание и настройка расписаний

IP-АТС Агат СУ позволяет выполнять запуск оповещений автоматически, по расписанию. В разделе "Расписание" WEB-интерфейса создается периодически возникающее событие, которое может быть указано одному, нескольким или всем оповещениям. Также может быть создано несколько событий, возникающих с различной периодичностью, которые могут быть назначены группам оповещения. При активизации, группы оповещения, в которых установлено это событие, автоматически запустят оповещения абонентов.

1. В разделе "Расписание" WEB-интерфейса создали несколько расписаний для будущих групп оповещений (См. Рис. 52).

The screenshot shows the 'Schedule' interface with a list of scheduled events. The events listed are:

- Система (System)
- Ящук (Yashuk)
- Рязь (Ryaz')

Рис. 5. Расписание

2. В появившейся строке указать в полях (См. Рис. 53):

- "Пользователь" – выбрать в выпадающем меню пользователя, либо "==> Система", чтобы событие было доступно всем пользователям.
- "Тема" – указать произвольное наименование темы события.
- "Наименование" – указать произвольное наименование события, под которым оно будет доступно для выбора в группе оповещения.

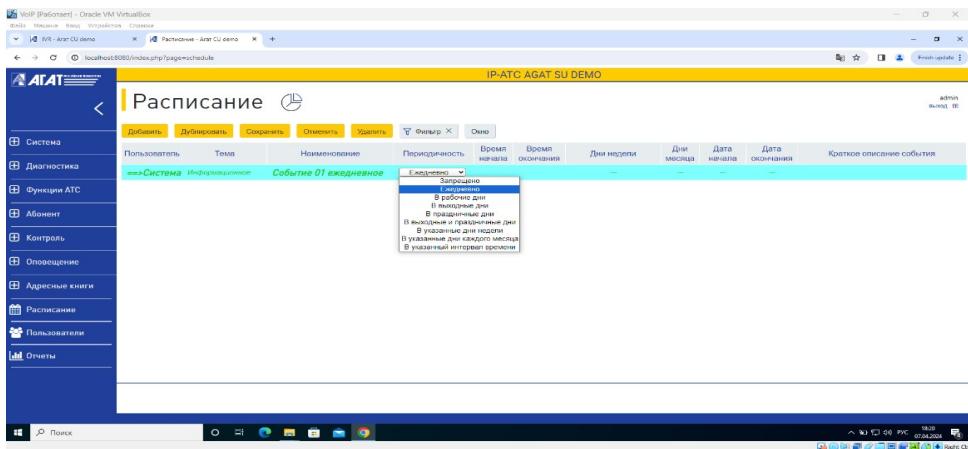


Рис. 7. Создание расписания

3. По завершению настроек параметров расписания, нажали на кнопку "Сохранить".

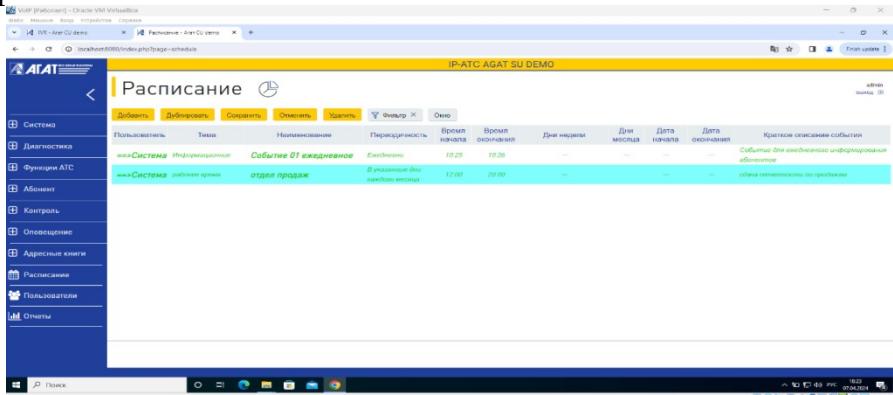


Рис. 6. Результат создания расписаний

Часть 3. Создать сообщения оповещения

Для оповещения абонентов используются звуковые сообщения, текстовые, и формируемые из текстовых сообщений звуковые сообщения. Используйте для каждого расписания разный способ оповещения, чтобы рассмотреть каждый из них.

1. Настроили синтез речи в разделе «Система» → «Синтез речи», согласно рисунку 34.1. Затем преобразовали текст в звук и скачали на ПК получившееся сообщение (См. Рис. 55).

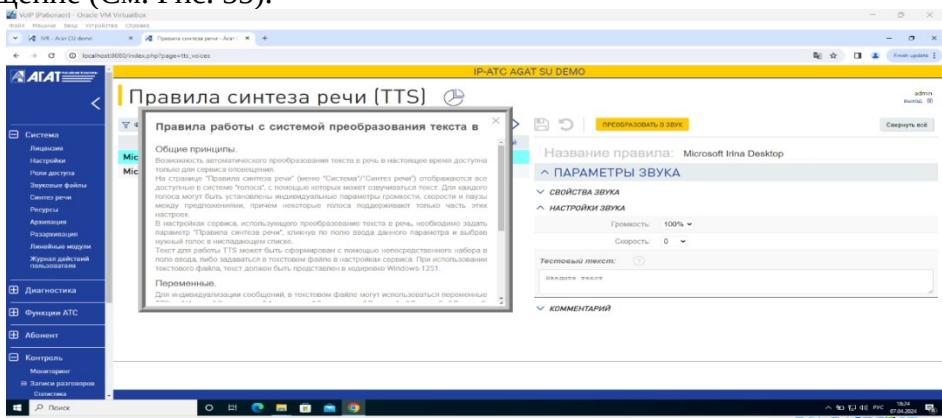


Рис. 7. Правила синтеза речи

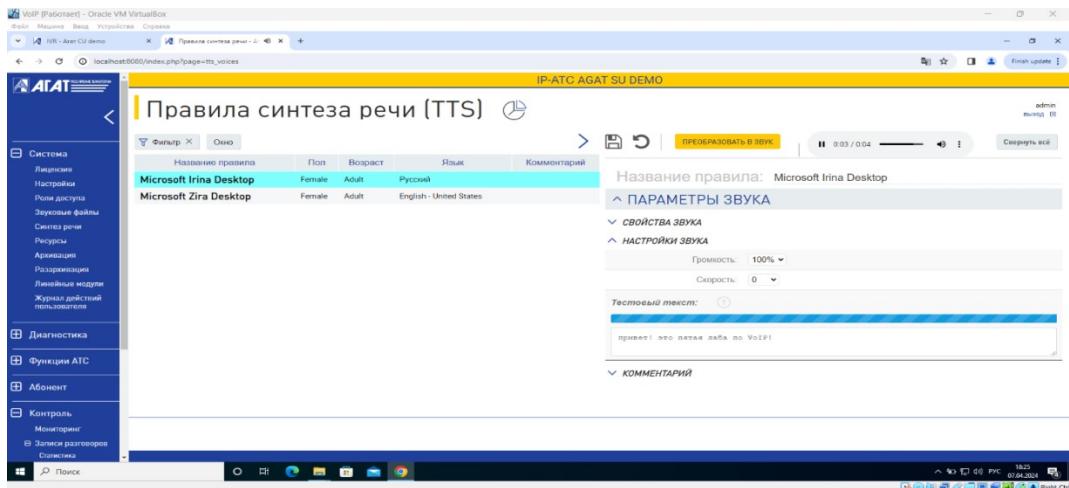


Рис. 8. Преобразование текста в звук

2. Записали звуковое сообщение в WEB-интерфейсе (См. Рис. 57). По завершению записи, сформированный звуковой файл будет доступен в группе параметров "Информация оповещения", также будут доступны элементы управления файлом (См. Рис. 58)

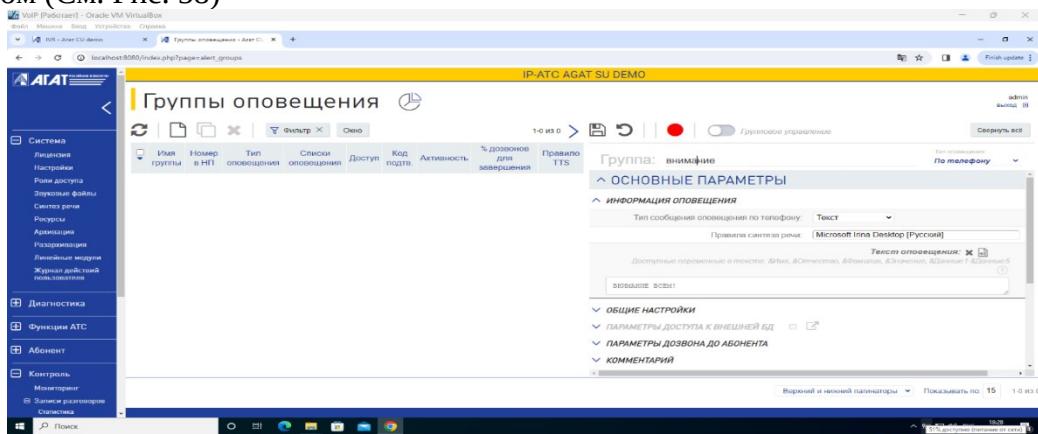


Рис. 9. Запись сообщения оповещения

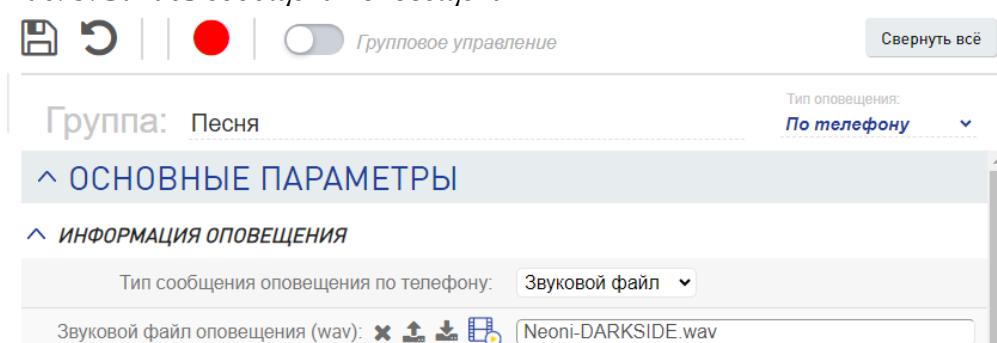
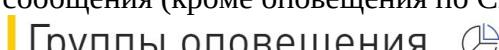


Рис. 10. Завершение записи

Часть 4. Создание групп оповещения и их запуск

1. Создали группы оповещения с разными параметрами типа оповещения и типа сообщения (кроме оповещения по СМС) (См. Рис. 59).



Имя группы	Номер в НП	Тип оповещения	Списки оповещения	Доступ	Код подтв.	Активность	% звонков для завершения
голос		По телефону	расписание	Пользователей: 1	---	100	---
из текста в голос		Комбинированный	расписание	Пользователей: 1	---	100	---
текст		СМС	расписание	Пользователей: 1	---	100	---

Рис. 11. Группы оповещений

2. Добавили в настройках созданное расписание и созданный или записанный в WEB-интерфейсе звук оповещения (См. Рис. 60).

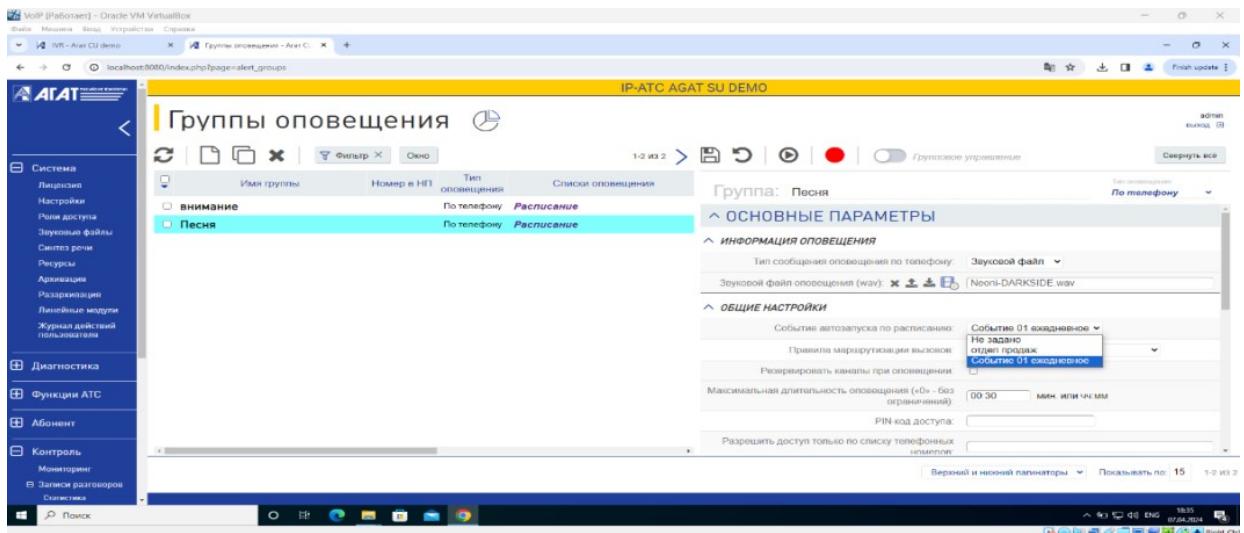


Рис. 12. Настройка группы оповещения

3. Для создания оповещения с помощью преобразования текста в голос, использовали следующие правила написания текста (См. Рис. 61).

4.

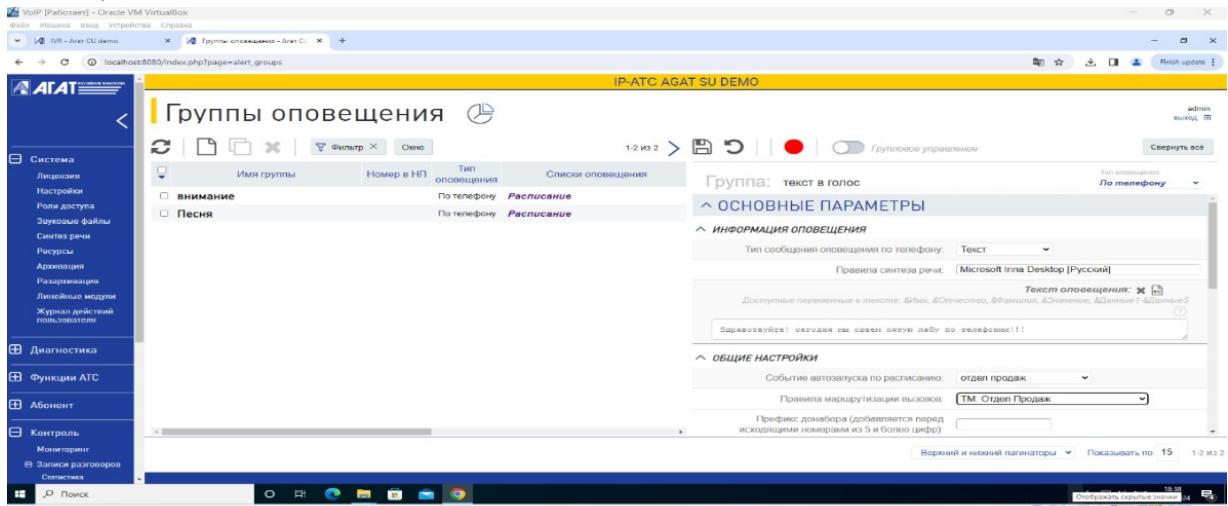


Рис. 13. Пример написания текстового оповещения

Текстовое сообщение, которое будет использоваться для оповещений, может иметь и не иметь переменных в своем составе. Если необходимо персонализированное оповещение абонентов, с воспроизведением индивидуальных данных, то в текстовом сообщении необходимо указывать шаблоны переменных данных для включения в воспроизводимом абоненту сообщении.

При воспроизведении сообщения абоненту, система оповещения подставит вместо шаблона переменной данные абонента из списка. Если некоторые или все переменные данные абонента не указаны, соответствующий переменной текст не будет воспроизведен, прочий текст и имеющиеся данные будут воспроизведены. Если в тексте нет переменной для воспроизведения какого-либо вида данных абонентов, то этот вид данных не будет абонентам воспроизведен.

Переменные имеют вид: "& <Имя_переменной>". Каждая из переменных может быть использована в тексте неограниченное количество раз.

4. Произвели запуск сразу всех групп оповещений (См. Рис. 62).

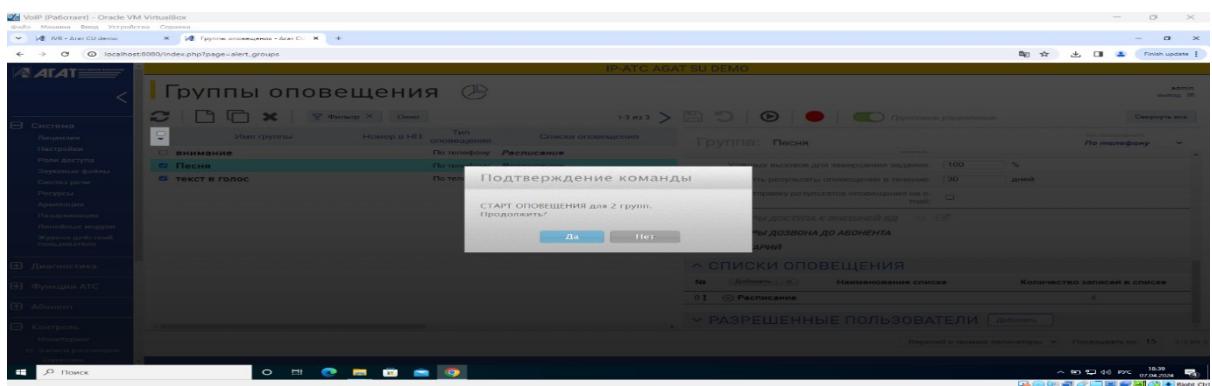


Рис. 14. Запуск 2 групп оповещений

Часть 5. Изучить информацию о состоянии и общих результатах оповещения

1. Запущенные группы оповещения (См. Рис. 63). Перешли во вкладку «Абоненты оповещений» (См. Рис. 64-65).

2.

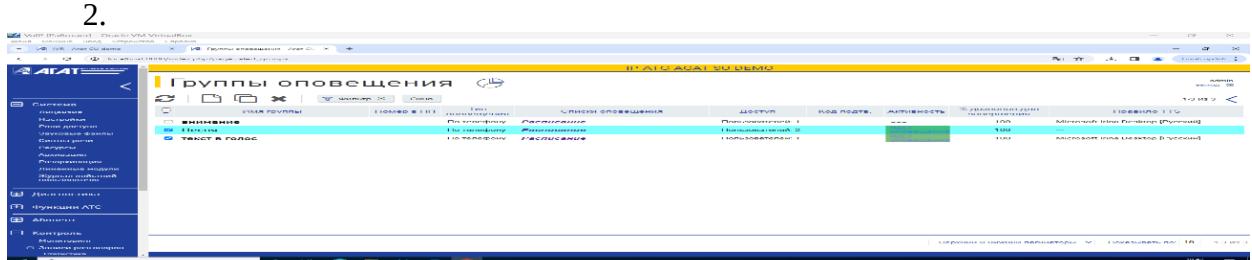


Рис. 15. Активность групп оповещения



Рис. 18. Переход к мониторингу оповещения

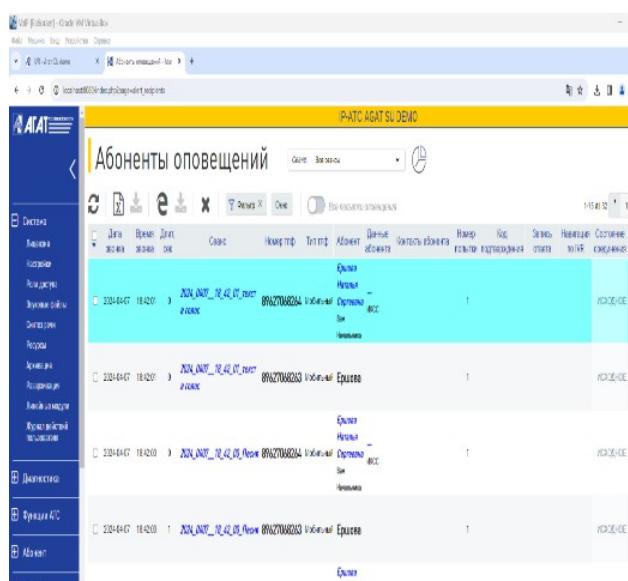


Рис. 16. Абоненты оповещений

2. Перешли во вкладку «Сеансы оповещения», в которой видно, какие оповещения сейчас работают и какие были выполнены. Изучили статистику данных оповещений (См. Рис. 66-67).

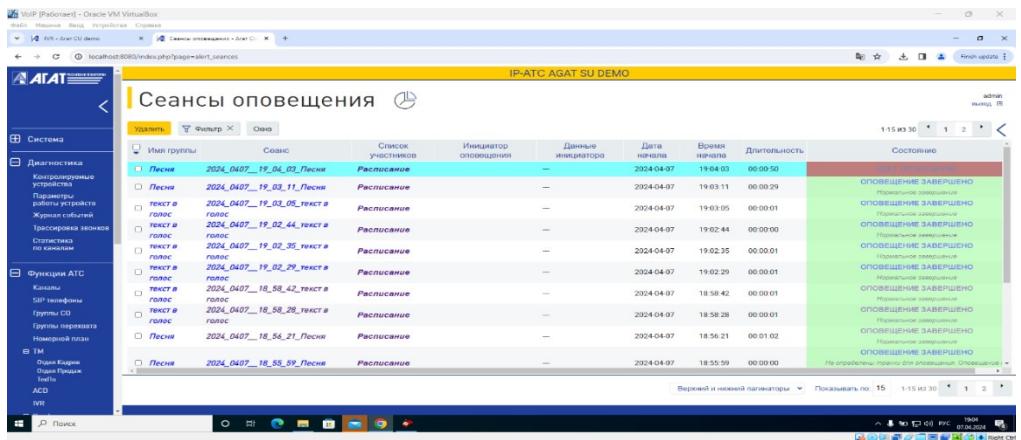


Рис. 17. Сеансы оповещения

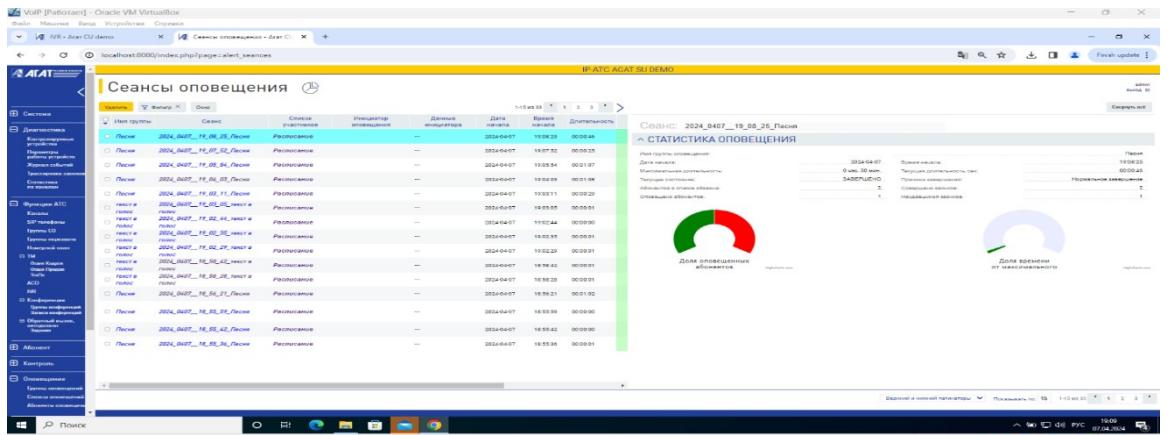


Рис. 18. Статистика данных оповещения

3. Попробовали проверить режим оповещений через PhonerLite, настроенный ранее (См. Рис. 68).

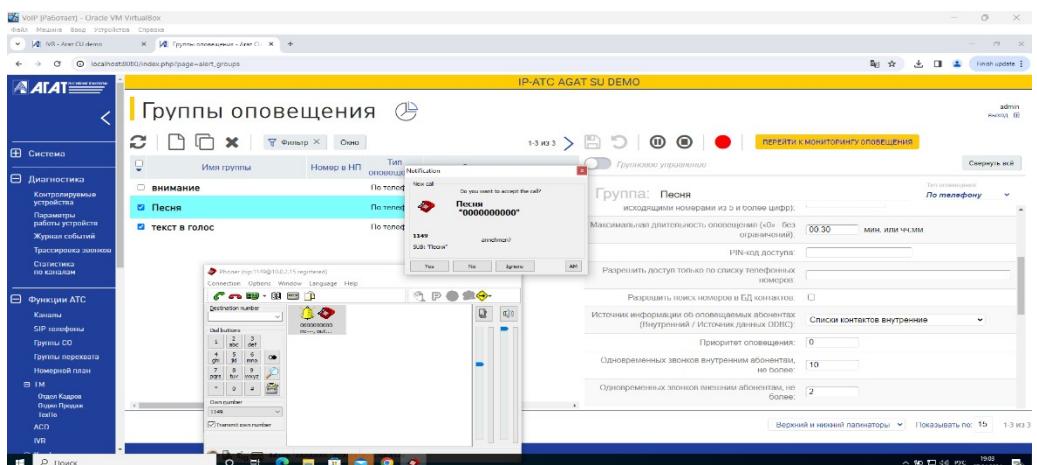


Рис. 19. Проверка режима оповещений

Ход работы:

- Создать 2 дополнительных внутренних номера
- Настроить на каждый из них голосовую почту
- Первый номер оставить без пароля и режим почты активируется если вызываемый абонент не доступен. Второй номер защитить паролем и запись в голосовую почту ведется сразу с момента дозвона.
- Прослушать оставленные сообщения.

5. После проверки работы преподавателем удалить файлы голосовой почты и 2 дополнительных внутренних номера.
6. Корректно завершить работы Trixbox.

Контрольные вопросы:

1. Для чего нужна голосовая почта?
2. В каких системах связи активно применяется?
3. Каким образом можно сделать одну голосовую почту на несколько абонентов?

Список дополнительных источников:

1. Гольдштейн В.С., Пинчук А.В., Суховицкий А.В. IP-телефония. – М.: Радио и связь, 2001.
2. Меггелен Дж., Мадсен Л., Смит Дж. Asterisk™: будущее телефонии. – Пер. с англ. – СПб: Символ-Плюс, 2009.
3. Ben Sharif, Trixbox without tears.

Форма отчета.

1. Ответить на контрольные вопросы.