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 01.03 «Технология монтажа и обслуживания мультисервисных сетей абонентского доступа**»**

Разработали преподаватели: Е.В. Нагорнова, А.Д. Насретдинов

Практическая работа № 1

«Конфигурирование и настройка программного обеспечения сервера IP-телефонии»

Цель: Научиться организовывать передачу голосовых данных в IP-сети.

Время выполнения: 14 часов.

Оборудование: аппаратные: 2 компьютера с возможностью подключения к Internet, гарнитура (наушники и микрофон); программные: ОС Windows 10; программный IP-телефон (SipPoint, Skype)

Ход работы:

Теоретические сведения:

Телефония основана на коммутации соединений, когда для создания соединения между абонентами на все время разговора выделяются каналы для передачи звука. Кроме этого, телефонные соединения можно организовывать и в цифровых сетях, где для передачи данных используется принцип коммутации пакетов. Именно эту задачу и решает Интернет-телефония (*IP-телефония, VoIP*). Главное преимущество *IP-телефонии* – себестоимость: минута разговора в случае междугородной, и тем более, международной связи оказывается во много раз дешевле, чем при использовании традиционной связи по сетям с коммутацией соединения. Это в значительной степени оправдывает даже сравнительно низкое качество звука, присущее современной *IP-телефонии*.

Сеть *IP-телефонии* представляет собой совокупность оконечного оборудования, каналов связи и узлов коммутации. Сети *IP-телефонии* строятся по тому же принципу, что и сети Интернет. Однако в отличие от сетей Интернет, к сетям *IP-телефонии* предъявляются особые требования по обеспечению качества передачи речи. Одним из способов уменьшения времени задержки речевых пакетов в узлах коммутации является сокращение количества узлов коммутации, участвующих в соединении.

Существует несколько **классификаций сетей IP-телефонии**:

1. По способу связи оконечных устройств между собой: выделенные, интегрированные, смешанные.
    - *В выделенных сетях* связь между оконечными устройствами осуществляется по выделенным каналам, и пропускная способность этих каналов используется только для передачи речевых пакетов. Чаще всего провайдеры *IP-телефонии* не строят собственную сетевую инфраструктуру, а арендуют каналы у провайдеров первичной сети. Главное преимущество выделенной сети – это высокое качество передачи речи. Кроме этого, для обеспечения гарантированного качества предоставляемых услуг в этих сетях, кроме протокола **IP**, применяются и другие транспортные протоколы: **ATM** и **FrameRelay**.
    - *В интегрированных сетях IP-телефонии* для связи между устройствами используется глобальная сеть Интернет. Это может быть уже существующая собственная сеть или доступ к сети Интернет через провайдеров.
    - *В сетях смешанного типа* для объединения устройств используются выделенные каналы и сеть Интернет. Вопрос о том, какие каналы

использовать для связи устройств между собой, решается оператором индивидуально в зависимости от возможностей.

2. По масштабу: международные, региональные, местные.
   - *Международная сеть IP-телефонии* имеет точки своего присутствия в нескольких странах и обеспечивает терминацию трафика практически в любую точку мира при минимальном использовании телефонной сети общего пользования. Международные сети строятся с использованием выделенных каналов и на базе уже существующих сетей Интернет.
   - *Национальная сеть* имеет точки своего присутствия в одной или, в крайнем случае, в нескольких близлежащих странах и обслуживает абонентов и местных операторов только этого региона. С помощью заключения договоренности с международными сетями национальная сеть предоставляет своим абонентам и другим местным сетям возможность терминации вызовов в любую точку мира.
   - *Местная сеть IP-телефонии* предоставляет возможность абонентам местной телефонной сети и частным компаниям воспользоваться услугами *IP-телефонии*. В основном, операторы местных сетей являются провайдерами доступа к сети IP-телефонии. Чаще всего, их сети имеют всего один шлюз, подключенный к более крупным сетям через сеть Интернет или по выделенным каналам. Для большинства операторов местная сеть является лишь промежуточным этапом развития, и они стремятся выйти на международный или национальный уровень.

Международный союз электросвязи (**IUT-T**) предложил стандарт **H.323** для построения сетей IP-телефонии. Этот стандарт охватывает практически все аспекты создания таких сетей и в настоящее время является наиболее распространенным. Сети **H.323** ориентированы на интеграцию с обычными телефонными сетями и рассматриваются как сети **ISDN**, работающие поверх сетей передачи данных – ***TCP/IP*** (Интернет), сетей **IPX, Ethernet, Fast Ethernet, Token Ring** и т.д. Стандарт **H.323** содержит большое количество протоколов, связанных с регистрацией оборудования, различными сценариями установления соединений, передачи речи, видео и данных, аутентификацией пользователей, тарификацией и многими другими задачами.

При использовании IP-телефонии необходимо учитывать, что адресация узлов в сети Интернет определяется не обычным числовым номером абонента, а IP-адресом компьютера, с которого (и на который) устанавливается соединение. Во многих случаях IP-адрес компьютера динамически меняется при очередном подключении, поэтому для соединения используют специальный узел сети – *сервер каталогов (directory server)*. Этот сервер хранит списки зарегистрированных на нем пользователей, причем каждый из них имеет уникальное имя в виде строки символов (обычно в формате адреса электронной почты) или традиционный номер, состоящий из цифр.

Существует еще одна разновидность узлов сети IP-телефонии – *шлюз (gateway)*. Это посредник между традиционной телефонной сетью и сетью передачи данных, преобразующий звонки одного типа в другой и обратно.

Передача телефонных переговоров по сети Интернет может осуществляться по нескольким сценариям.

Использование программы IP-телефонии. В этом случае на двух компьютерах, подключенных к Интернету, необходимо запустить специальную программу, которая на одном конце преобразует звук от микрофона в пакеты данных, а на другом конце

выполняет обратное преобразование и проигрывает звук в динамик. Далее работа осуществляется по следующему алгоритму:

1. Пользователь А запускает программу при установленном подключении к Интернет.
2. Программа IP-телефонии автоматически сообщает серверу каталогов, что вызывающий пользователь (А) доступен для входящих звонков и имеет такой-то IP-адрес.
3. Программа IP-телефонии пользователя Б запросит сервер каталогов по символьному имени пользователя А соответствующий ему IP-адрес и начнет передачу пакетных данных.
4. Пользователь А получит уведомление о входящем Интернет-звонке от пользователя Б и, ответив на звонок, окончательно установит соединение.

Использование IP-телефона. Внешне это устройство выглядит как обычный телефон, но подключается непосредственно к сети передачи данных. В отличие от компьютера IP-телефон, как и обычный телефон, всегда готов к работе. IP-телефония помимо передачи звуковой информации между двумя собеседниками может быть использована в качестве организации конференцсвязи (большинство существующих программ IP-телефонии поддерживает эту возможность), и как средство для организации видеотелефонии, если с обеих сторон имеется соответствующее программное и аппаратное обеспечение.

Выполнение работы

Задание 1.Создание учетной записи (на сайте поставщика услуг IP-телефонии)

1. Откройте в окне браузера сайт поставщика услуг IP-телефонии: **www.sipnet.ru**
2. В верхней части окна выберите ссылку **Зарегистрироваться!** (Регистрация новых пользователей)
3. Заполните **Регистрационную форму данных**. Обратите внимание на *обязательно заполняемые поля* и *Примечания*, описывающие правила заполнения регистрационной формы. Для принятия введенных данных выберите **Продолжить регистрацию**.
4. В случае успешной регистрации будет выведено окно **Клиент успешно зарегистрирован**. Вернитесь на главную страницу сайта (ссылка **Перейти на сайт** в правом верхнем углу).
5. Зайдите в **Личный кабинет**, используя только что созданную учетную запись (логин/пароль).
6. Изучите ***Информацию об аккаунте*** (верхняя часть окна): *SIP ID (персональный идентификатор – аналог телефонного номера), Статус аккаунта, количество средств на счете* и др.
7. Ознакомьтесь с информацией о возможностях присвоенного вам статуса аккаунта (ссылка **Изменить статус аккаунта**).
8. Сверните окно браузера на **Панель задач**.

Задание 2.Установка и настройка работы программного IP-телефона.

1. Установите программу **SipPoint** (файл инсталляции ***SippointSetup.exe***):
    - оставьте все предлагаемые по умолчанию параметры установки, приняв лицензионное соглашение;

- на шаге **Выберите дополнительные задачи** снимите флажок *Запускать программу при каждой загрузке Windows*.

2. Выполните настройку программы **SipPoint**, оставляя настройки «по умолчанию», за исключением:
   - при выборе полосы пропускания вашего подключения к сети Интернет установите радиокнопку *Dialup подключение 56 кбит/с*;
   - введите *учетные данные*, полученные вами при регистрации на сайте;
   - при выборе способа подключения к службе мгновенных сообщений оставьте *Автоматическая настройка*.

     *После закрытия **Мастера определения подключения к сети** программа IP-телефонии автоматически предлагает настройку звуковых и видеоустройств, подключенных к вашему ПК – окно **Audio and Video Tuning Wizard**.*

3. Настройка гарнитуры для общения в программе **SipPoint**.
   - подключите гарнитуру к соответствующим разъемам звуковой карты ПК и убедитесь, что закрыты любые другие программы воспроизведения медиа-файлов (***Далее***);
   - установите гарнитуру в рабочее положение (***Далее***);
   - проверьте правильность выбранных устройств в раскрывающемся списке (***Далее***);
   - настройте оптимальную громкость звука в наушниках, нажав кнопку **Click to Test** и используя бегунок регулятора **SpeakerVolume** (***Далее***);
   - настройте оптимальную чувствительность микрофона: проговаривая любую фразу и перемещая бегунок регулятора **MicrophoneVolume**, добейтесь наилучшей слышимости собственного голоса в наушниках (***Далее***);
   - закончите настройку гарнитуры (***Готово***).
4. Ознакомьтесь с интерфейсом программы **SipPoint** (подключение к сети происходит автоматически после запуска программы)
   - вкладка **Телефоны** содержит добавленные номера телефонов, на которые осуществляются звонки (является основной для осуществления звонка);
   - вкладка **Контакты** содержит доступные для работы группы;
   - вкладка **Звонки** показывает информацию о состоянии соединения (*Звонки отсутствуют, Звоним, Разговариваем, Конец разговора*), продолжительности разговора, используемом кодеке (в случае установленного соединения), уровень чувствительности микрофона и громкости наушников;
   - панель с кнопками ***Осуществить или принять звонок*** и ***Закончить или отклонить разговор*** (активны только для вкладок **Телефоны** и **Звонки**);
   - **статус-строка**, показывающая текущее значение счета и статус пользователя в сети.

Задание 3.Организация звонка с помощью программы SipPoint.

1. Организация звонка <u>не из списка контактов</u>:

- перейдите на вкладку **Телефоны** и введите в строку *Здесь введите SIP ID или номер для быстрого звонка* номер телефона (городской АТС) в формате: <код_страны>-<код_города>-<номер_телефона>;
- установите соединение, нажав на кнопку ***Осуществить или принять звонок***;
- закончите разговор, нажав на кнопку ***Закончить или отклонить разговор***.

2. Организация звонка абоненту из телефонной книги:
   - добавьте новый контакт на вкладке **Телефоны** в предложенном формате (***Контекстное меню/Добавить телефон***);

     В качестве нового телефона укажите, например, номер своего мобильного телефона или номер своего друга. Входящий звонок для него будет бесплатным.

   - выполните вызов двойным щелчком по названию контакта. Обратите внимание, что автоматически произойдет переключение на вкладку **Звонки**, вверху которой отобразится номер, на который вы осуществляете вызов.
   - закончите разговор, нажав на кнопку ***Закончить или отклонить разговор***.
3. Проверьте текущее значение счета в статус-строке и закройте приложение (***Файл/Выход***).
4. Создайте снимок экрана с обновленной информацией **Личного кабинета** в браузере и сохраните его в личной папке.
5. Выполните деинсталляцию программы **SipPoint (*Пуск/Панель управления/Установка и удаление программ*)**.

Самостоятельные задания.

1. Выполните настройку клиента (на физическом компьютере) и его подключение к серверу потоков мультимедиа.
2. Выполните одновременное подключение к серверу клиента на физическом компьютере и клиента в среде ВМ.
3. Создайте список воспроизведения, состоящий из стандартных звуковых файлов Windows (C:\Windows\Media) и настройте его потоковое вещание.
4. Выполните установку и настройку программы IP-телефонии Skype (на два компьютера).
5. Организуйте звонок с одного компьютера на другой.
6. Создайте видеозвонок с одного компьютера на другой при помощи программы Mail.Ru Агент, создав при необходимости учетную запись и добавив нужный контакт.
7. Удалите установленные на компьютеры Web-камеры, предварительно отключив их (Пуск/Панель управления/Установка и удаление программ)

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 2

«Оборудование технологии NGN: гибкий программный коммутатор Softswitch»

Цель: Изучение методики и получение практических навыков проектирования гибкого коммутатора (softswitch), используемых в сетях связи следующего поколения NGN..

Время выполнения: 8 часов.

Ход работы:

Теоретические сведения:

Задачей уровня управления коммутацией и передачей является управление установлением соединения в фрагменте сети NGN. Функция установления соединения реализуется на уровне элементов транспортной сети под внешним управлением оборудования гибкого коммутатора (softswitch). Исключением являются АТС с функциями MGC, которые сами выполняют коммутацию на уровне элемента транспортной сети.

Гибкий коммутатор должен осуществлять:

- обработку всех видов сигнализации, используемых в его домене;
- хранение и управление абонентскими данными пользователей, подключаемых к его домену непосредственно или через оборудование шлюзов доступа;
- взаимодействие с серверами приложений для предоставления расширенного списка услуг пользователям сети.

При установлении соединения оборудование гибкого коммутатора осуществляет сигнальный обмен с функциональными элементами уровня управления коммутацией. Такими элементами являются все шлюзы, терминальное оборудование сети (интегрированные устройства доступа (IAD), терминалы SIP и H.323), оборудование других гибких коммутаторов и АТС с функциями контроллера транспортных шлюзов (MGC). Для передачи информации сигнализации сети ТфОП через пакетную сеть используются специальные протоколы. Так, для передачи информации сигнализации ОКС№7, поступающей через сигнальные шлюзы от ТфОП к оборудованию гибкого коммутатора, используется протокол MxUA технологии SIGTRAN (в то же время в ряде реализаций гибкого коммутатора предусмотрен непосредственный ввод сигнализации ОКС№7). На основании анализа принятой информации и решения о последующей маршрутизации вызова оборудование гибкого коммутатора, используя соответствующие протоколы, осуществляет сигнальный обмен по установлению соединения с сетевым элементом назначения и управляет с использованием протокола H.248 (для IP коммутации) или BICC (для ATM коммутации) установлением соединения для передачи пользовательской информации. При этом потоки пользовательской информации не проходят через гибкий коммутатор, а замыкаются на уровне транспортной сети. В случае использования на сети нескольких гибких коммутаторов они взаимодействуют по межузловым протоколам (как правило, семейство SIP-T) и обеспечивают совместное управление установлением соединения. Структура уровня управления сетями доступа NGN представлена на рис. 1.

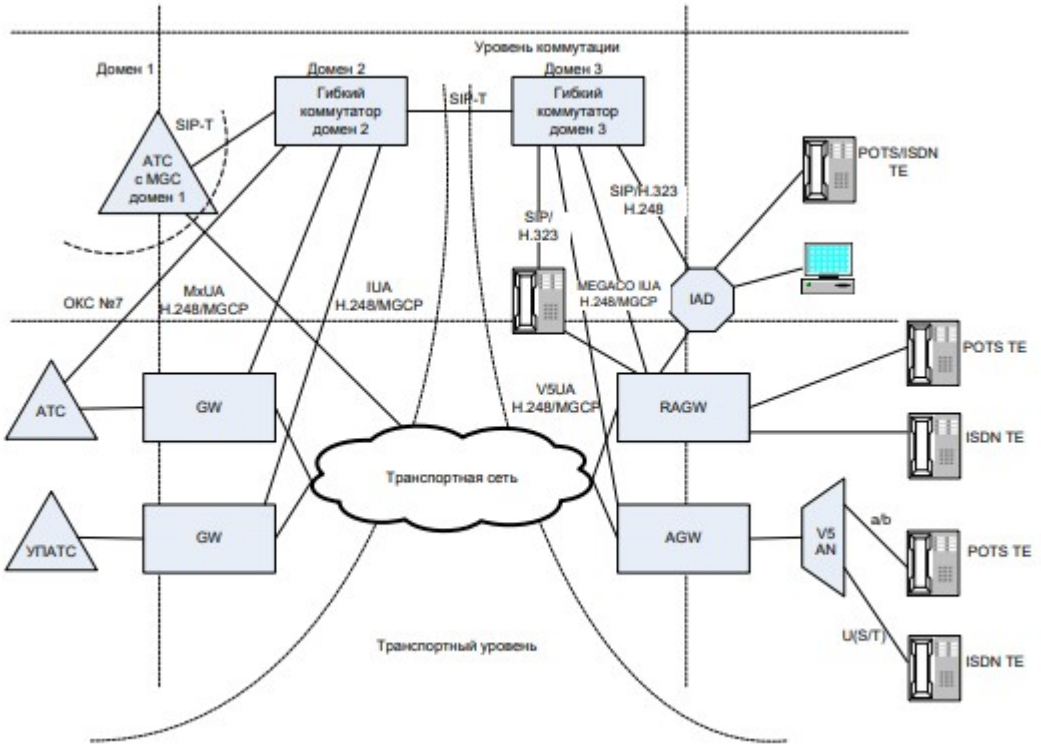


Рис. 1. Схема включения гибких коммутаторов для управления сетями доступа NGN

Терминальное оборудование пакетной сети взаимодействует с оборудованием гибкого коммутатора с использованием протоколов SIP и H.323. Пользовательская информация от терминального оборудования поступает на уровень узлов доступа пакетной сети и далее маршрутизируется под управлением гибкого коммутатора.

Расчет производительности гибкого коммутатора

Основной задачей гибкого коммутатора при построении распределенного абонентского концентратора являются обработка сигнальной информации обслуживания вызова и управление установлением соединений. Емкостные параметры абонентской базы гибкого коммутатора должны позволять обслуживание всех абонентов различных типов, подключение которых планируется при построении абонентского концентратора. При этом для обслуживания вызовов могут использоваться различные протоколы сигнализации.

Введем следующие переменные:
P_{PSTN} — удельная интенсивность вызовов от абонентов, использующих доступ по аналоговой телефонной линии в ЧНН;
P_{ISDN} — удельная интенсивность вызовов от абонентов, использующих доступ по базовому доступу ISDN;
P_{V5} — удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от абонентов, подключаемых к пакетной сети через сети доступа интерфейса V5;
P_{PBX} — удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от УПАТС, подключаемых к пакетной сети;
P_{SHM} — удельная интенсивность вызовов от абонентов, использующих терминалы SIP, H.323, MGCP.
В соответствии с «Общими техническими требованиями к городским АТС» интенсивность вызовов равна:
P_{PSTN} = 5 выз/чнн, P_{ISDN} = 10 выз/чнн, P_{PBX} = 35 выз/чнн.
Значение P_{SHM} можно принять равным P_{PSTN}. Значение P_{V5} можно принять равным P_{PBX}.

Тогда общая интенсивность вызовов, поступающих на гибкий коммутатор от источников всех типов, равна:

$$P_{CALL} = P_{PSTN} \cdot (\sum_{l=1}^{L} N_{l\_PSTN} + \sum_{l=1}^{L} N_{l\_SHM}) + P_{ISDN} \cdot \sum_{l=1}^{L} N_{l\_ISDN} + P_{V5} \cdot (\sum_{l=1}^{L} \sum_{j=1}^{J} N_{j\_V5} + \sum_{l=1}^{L} \sum_{k=1}^{K} N_{k\_PX}) \quad (1)$$

где L — число шлюзов доступа, обслуживаемых гибким коммутатором.

Отметим, что удельная производительность коммутационного оборудования может отличаться в зависимости от типа обслуживаемого вызова, т.е. производительность при обслуживании, например, вызовов ССОП и ISDN, может быть разной.

В документации на коммутационное оборудование, как правило, указывается производительность для наиболее «простого» типа вызовов. В связи с чем при определении требований к производительности гибкого коммутатора можно ввести поправочные коэффициенты, которые характеризуют возможности системы по обслуживанию данного типа вызовов относительно «идеального» типа.

Например, если производительность системы для «идеальных» вызовов SIP равна 10 млн. выз/чнн, а для вызовов ССОП — 8 млн. выз/чнн, то интенсивность последних должна браться с коэффициентом 1,25.

Таким образом, нижний предел производительности гибкого коммутатора по обслуживанию потока вызовов с интенсивность P_{CALL} может быть определен по формуле:

$$P_{SN} = k_{PSTN} \cdot P_{PSTN} \cdot N_{PSTN} + k_{ISDN} \cdot P_{ISDN} \cdot N_{ISDN} + k_{V5} \cdot P_{V5} \cdot N_{V5} + k_{PBX} \cdot P_{PBX} \cdot N_{PBX} + k_{SHM} \cdot P_{SHM} \cdot N_{SHM} \quad (2)$$

Следует отметить, что требования по производительности предполагают работу оборудования гибкого коммутатора в условиях перегрузки с показателями не ниже определяемых в рекомендации Q.543 для нагрузок классов B и C.

Расчет параметров интерфейсов подключения гибкого коммутатора к пакетной сети

Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания вызовов.

Пусть:

L_{MEGACO} — средняя длина сообщения (в байтах) протокола MEGACO, используемого при передаче информации сигнализации по абонентским линиям;

N_{MEGACO} — среднее количество сообщений протокола MEGACO при обслуживании вызова;

L_{V5UA} — средняя длина сообщения протокола V5UA;

N_{V5UA} — среднее количество сообщений протокола V5UA при обслуживании вызова;

L_{IUA} — средняя длина сообщения протокола IUA;

N_{IUA} — среднее количество сообщений протокола IUA при обслуживании вызова;

L_{SH} — средняя длина сообщения протоколов SIP/H.323;

L_{SH} — среднее количество сообщений протоколов SIP/H.323 при обслуживании вызова;

L_{MGCP} — средняя длина сообщения протокола MGCP, используемого при управлении коммутацией на шлюзе;

N_{MGCP} — среднее количество сообщений протокола MGCP при обслуживании вызова. Тогда:

$$V_{SX} = k_{sig} \cdot [(L_{MEGACO} \cdot N_{MEGACO} \cdot P_{PSTN} \cdot N_{PSTN} + L_{V5UA} \cdot N_{V5UA} \cdot P_{V5} \cdot N_{V5} + \\ + L_{IUA} \cdot N_{IUA} \cdot (P_{ISDN} \cdot N_{ISDN} + P_{PBX} \cdot N_{PBX}) + L_{SH} \cdot N_{SH} \cdot P_{SH} \cdot N_{SH} + \\ + L_{MGCP} \cdot N_{MGCP} \cdot (P_{PSTN} \cdot N_{PSTN} + P_{V5} \cdot N_{V5} + P_{ISDN} \cdot N_{ISDN} + P_{PBX} \cdot N_{PBX})] / 450 \quad (3)$$

где:

V_{SX} — минимальный полезный транспортный ресурс, в бит/с, которым гибкий коммутатор SX должен подключаться к пакетной сети, для обслуживания вызовов в сети доступа;

k_{sig} — коэффициент использования транспортного ресурса при передаче сигнальной нагрузки. По аналогии с расчетом сигнальной сети ОКС№7 примем значение k_{sig} = 5, что соответствует нагрузке в 0,2 Эрл;

1/450— результат приведения размерностей «байт в час» к «бит в секунду» (8/3600 =1/450).

Ориентировочно можно принять, что средняя длина всех сообщений равна 50 байтам, а среднее количество сообщении в процессе обслуживания вызова равно 10.

Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети определяются следующим выражением:

$$N_{INT} = \frac{V_{SX}}{V_{INT}} \quad (4)$$

где V_{INT} — полезный транспортный ресурс одного интерфейса.

Расчет оборудования гибкого коммутатора для управления транспортными коммутаторами

Основной задачей гибкого коммутатора при управлении транзитным уровнем коммутации в сети NGN является обработка сигнальной информации обслуживания вызова и управление установлением соединений. Требования к производительности гибкого коммутатора определяются интенсивностью вызовов, требующих обработки.
Интенсивность поступающих вызовов определяется интенсивностью вызовов, приходящейся на один канал 64 кбит/с первичного потока E1, а также числом потоков E1, используемых для подключения станции к транспортному шлюзу (рис 2).

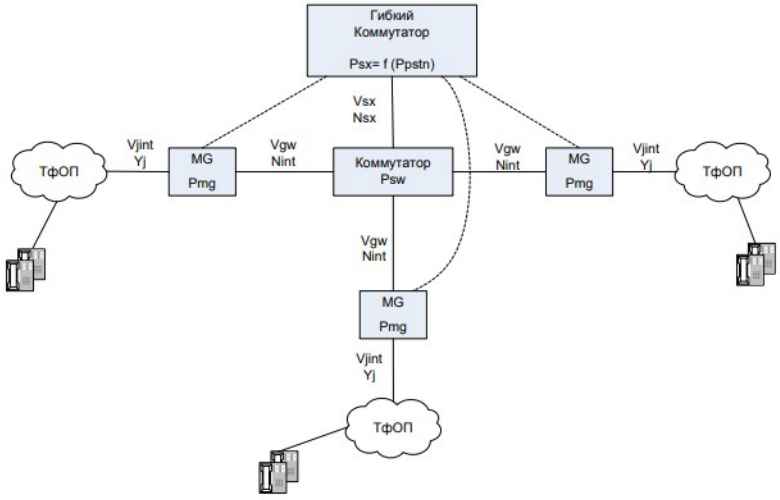


Рис. 2. Схема включения гибких коммутаторов для управления транзитными уровнем NGN

Пусть
P_{CH} — интенсивность вызовов, обслуживаемых одним каналом 64 кбит/с;
P_{GW} — интенсивность вызовов, обслуживаемых транспортным шлюзом.
Тогда интенсивность вызовов, поступающих на транспортный шлюз l, определяется формулой:

$$P_{l\_GW} = N_{l\_E1} \cdot 30 \cdot P_{CH}, \text{ выз/ЧНН} \quad (5)$$

Следовательно, интенсивность вызовов, поступающих на гибкий коммутатор, можно вычислить как

$$P_{SX} = \sum_{l=1}^{L} P_{l\_GW} = 30 \cdot P_{CH} \cdot \sum_{l=1}^{L} N_{l\_E1}, \text{ выз/ЧНН} \quad (6)$$

где L — число транспортных шлюзов, обслуживаемых гибким коммутатором.
Значение удельной интенсивности нагрузки определяется общими техническими требованиями к используемой опорной станции ОПС.
Требования по производительности предполагают работу оборудования гибкого коммутатора в условиях перегрузки с показателями не ниже определяемых в рекомендации Q.543 для нагрузок классов B и C.
Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания вызовов. При использовании гибкого коммутатора для организации распределенного транзитного коммутатора сообщения сигнализации ОКС№7 поступают на SX в формате сообщений протокола M2UA или M3UA, в зависимости от реализации.

Пусть:
L_{MXUA} — средняя длина сообщения (в байтах) протокола MxUA;
N_{MXUA} — среднее количество сообщений протокола MxUA при обслуживании вызова;
L_{MGCP} — средняя длина сообщения (в байтах) протокола MGCP, используемого для управления транспортным шлюзом;
N_{MGCP} — среднее количество сообщений протокола MGCP при обслуживании вызова.
Тогда транспортный ресурс SX, необходимый для передачи сообщений протокола MxUA, составляет:

$$V_{SX\_MXUA} = k_{sig} \cdot L_{MXUA} \cdot N_{MXUA} \cdot P_{SX}, \text{ байт/ЧНН} \quad (7)$$

где k_{sig} — коэффициент использования ресурса.
Аналогично, транспортный ресурс гибкого коммутатора, необходимый для передачи сообщений протокола MGCP, составляет

$$V_{SX\_MGCP} = k_{sig} \cdot L_{MGCP} \cdot N_{MGCP} \cdot P_{SX}, \text{ байт/ЧНН} \quad (8)$$

Суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в структуре транзитного коммутатора, составляет

$$V_{SX} = V_{SX\_MXUA} + V_{SX\_MGCP}$$

После приведения размерностей получаем

$$V_{SX\_MXUA} = k_{sig} \cdot P_{SX} \cdot (L_{MXUA} \cdot N_{MXUA} + L_{MGCP} \cdot N_{MGCP}) / 450, \text{ бит/с} \quad (9)$$

Также ориентировочно можно принять, что средняя длина всех сообщений равна 50 байтам, а среднее количество сообщении в процессе обслуживания вызова равно 10.
Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными коммутаторами могут быть определены по формуле (4).

Задание:

1. Изобразить проектируемую сеть NGN, обслуживаемую гибким коммутатором.
2. Рассчитать параметры гибкого коммутатора.

Контрольные вопросы

1. Назначение и функции гибкого коммутатора (softswitch) в сети NGN.
2. Какие протоколы используются в гибком коммутаторе (softswitch) для управления сетью доступа?
3. Какие протоколы используются в гибком коммутаторе (softswitch) для управления транспортной сетью?
4. От чего зависит выбор производительности гибкого коммутатора (softswitch)?
5. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию сетей доступа?

6. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию транзитного уровня NGN?

7. Как определить необходимые интерфейсы для подключения гибкого коммутатора к пакетной сети?

Содержание отчета

1. Таблица с исходными данными для проектирования гибкого коммутатора.

2. Схема подключения гибкого коммутатора к сети NGN с указанием используемыхпротоколов для управления сетью доступа и транспортной сетью.

3. Результаты расчетов оборудования гибкого коммутатора:

нижний предел производительности гибкого коммутатора для управления сетью доступа;

тип и количество интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления сетью доступа;

суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в транзитных коммутаторах;

тип и количество интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными коммутаторами.

Индивидуальные задания:

№	Исходный параметр	Варианты заданий									
		0	1	2	3	4	5	6	7	8	9
1.	Число абонентов ССОП	2000	2500	3000	3500	4000	4500	3000	2500	3500	2000
2.	Число абонентов ISDN-BRA	250	200	150	300	350	400	450	250	300	350
3.	Число сетей доступа с интерфейсом V.5/Число потоков E1 для подключения	2/5	3/3	5/4	0	3/5	2/1	6/3	4/4	3/6	0
4.	Число УПАТС, подключаемых к шлюзу /Число потоков PRI для подключения УПАТС	4/2	0	1/2	3/5	1/2	2/3	4/2	0	4/1	3/3
5.	Число абонентов с терминалами SIP/H.323/MGCP	500	450	600	250	350	550	300	400	200	450
6.	Поправочный коэффициент для ССОП	1,1	1,2	1,3	1,4	1,1	1,2	1,3	1,4	1,1	1,2
7.	Поправочный коэффициент для ISDN	1,3	1,5	1,6	1,2	1,4	1,3	1,2	1,1	1,5	1,4
8.	Поправочный коэффициент для V.5	1,2	1,3	1,5	1,1	1,2	1,4	1,5	1,3	1,2	1,1
9.	Поправочный коэффициент для УПАТС	1,5	1,1	1,1	1,3	1,3	1,5	1,1	1,2	1,3	1,3
10.	Поправочный коэффициент для пакетной сети	1,2	1,3	1,4	1,5	1,2	1,3	1,4	1,2	1,1	1,5
11.	Интенсивность вызовов, обслуживаемых одним каналом 64 кбит/с, вызовов/ЧНН	5	7	6	8	4	5	6	7	5	8
12.	Число потоков E1, используемых для подключения станции к транспортному шлюзу	2	3	4	5	2	3	4	2	3	5
13.	Число транспортных шлюзов, обслуживаемых гибким коммутатором	1	2	3	4	5	1	2	3	4	3

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 3

«Оборудование технологии NGN: универсальный медиашлюз»

Цель: Изучить назначение, технические характеристики и конструкцию гибкого коммутатора универсального медиашлюза UMG8900 Huawei.

Время выполнения: 8 часов.

Оборудование: универсальный медиашлюз UMG8900 Huawei.

Ход работы:

Теоретические сведения:

Немаловажным элементом предлагаемого решения NGN является и универсальный медиашлюз UMG8900, позволяющий осуществлять стыковку между сетями ТфОП и IP. Разнообразие поддерживаемых интерфейсов и функций позволяет устройству взаимодействовать с широким спектром оборудования. Оправдывая свое название, UMG8900 может использоваться как в качестве медиашлюза соединительных линий (TMG), так и в качестве медиашлюза абонентского доступа (AMG). Встроенное коммутационное поле TDM позволяет замыкать голосовой трафик внутри шлюза в ряде случаев, обеспечивая более высокое качество передачи речи, а также экономя ресурсы сети IP.

Еще одним несомненным преимуществом оборудования является встроенный шлюз сигнализации. Производительность встроенного SG позволяет, в большинстве случаев, строить сети без установки независимого шлюза сигнализации, оптимизируя, таким образом, показатель CAPEX для проектов.

Рис.2.1. Внешний вид медиашлюза UMG8900

6.1. 2. Основные характеристики UMG8900

Параметр	Значение	
	UMG8900 mini	**Стандартный UMG8900**
Поддерживаемая емкость	от 8 E1 до 48 E1 на полке шаг масштабирования – 8 E1	от 32 E1 до 448 E1 на полке шаг масштабирования – 32 E1
Применение	• TMG – Trunk Media Gateway (медиашлюз соединительных линий) • AMG – Access Media Gateway (медиашлюз доступа) • VIG – Video Interworking Gateway (шлюз видеовзаимодействия между абонентами мобильной и NGN сетей)	
Восходящие интерфейсы	• FE	• FE • GE
Нисходящие интерфейсы	• E1	• E1 • STM-1
Количество поддерживаемых сигнальных линков (64кбит/с)	• до 24	• до 896
Протоколы сигнализаций ТфОП	• OKC7 • DSS-1 • R1.5 • R2 • V5	
Протоколы сигнализаций IP/ NGN и управления	• H.248 • SIGTRAN • H.245 • H.223 • SNMP	
Поддерживаемые аудио (факс)-кодеки	• G.711 • G.723.1 • G.726 • G.729 • T.38	
Поддерживаемые видеокодеки	• MPEG4 • H.263	
Дополнительные функции	• поддержка распознавания набора номера в режимах PULSE/ DTMF; • поддержка смешивания аудио-сигналов для организации конференц-связи; • встроенный шлюз сигнализации (SG); • встроенные коммутационные поля TDM и IP	
Емкость коммутационного поля TDM	• 4K, неблокируемая матрица	• 256K/ 32K в зависимости от конфигурации, неблокируемая матрица
Емкость пакетного	• 800 Мбит/с	• 16 Гбит/с / 12 Гбит/с

коммутационного поля		в зависимости от конфигурации
Механизмы обеспечения качества голоса	• эхокомпенсация (EC); • поддержка статического и динамического буфера джиттера; • поддержка VAD – Voice Activity Detection; • поддержка CNG – Comfort Noise Generation	
Механизмы обеспечения безопасности	• поддержка аутентификации пользователей; • поддержка IPSec; • поддержка ACL и функций файервола	

На рис.2.1. представлен универсальный медиашлюз UMG8900, который представляет собой устройство опорной сети в мобильных системах стандарта GSM, разработанное компанией Huawei Technologies. Сети мобильной связи стандарта GSM, ориентированные на будущее, обеспечивают экономию инвестиций и высокий доход операторов связи. UMG8900 может работать в качестве различных сетевых устройств в зависимости от сетевых требований

Аппаратная платформа UMG8900 разработана с целью комбинирования пакетного и узкополосного коммутаторов, что должно обеспечить эффективную поддержку узкополосных услуг на базе TDM и пакетных услуг поверх IP. Для потоков услуг и потока управляющих команд шлюз UMG8900 использует различные коммутационные поля.

Оборудование UMG8900 поддерживает режимы передачи данных IP/TDM и различные типы интерфейсов, обеспечивающих возможности взаимодействия с другими типами сетей:

- TDM: STM-1 SDH (электрооптический интерфейс), E1, T1
- IP: FE, GE (оптоволоконный интерфейс), STM-1/4 POS (оптоволоконный интерфейс)
- IPoA: STM-1 IPoA (Оптоволоконный интерфейс)

Система поддерживает следующие услуги и функции:

- встроенного шлюза сигнализации;
- эхоподавления, проигрывание тональных сигналов и объявлений, соединение с оборудованием IN, предоставляющим дополнительные услуги;
- детектор голосовой активности (VAD) и функции буфера джиттера позволяют экономить полосу пропускания и повышает качество голоса.

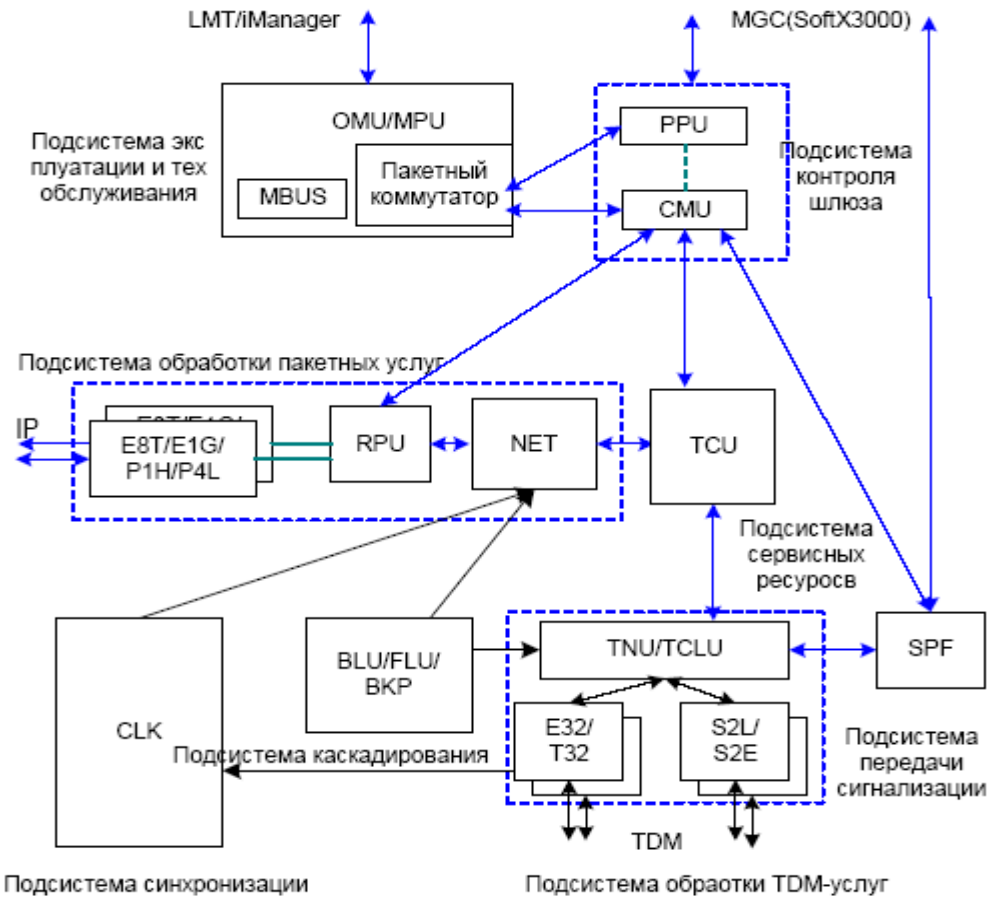


Рис. 2.1. Архитектура медиашлюза UMG8900

В системе подвижной связи UMG8900 выполняет изменение различных характеристик несущего канала, в том числе и хэндовера.

Задание:

1. Изучить назначение и технические характеристики универсального медиашлюза UMG8900 Huawei.
2. Изучить конструкцию универсального медиашлюза UMG8900 Huawei.

Контрольные вопросы

1. Назначение универсального медиашлюза UMG8900.
2. Область применения универсального медиашлюза UMG8900.
3. Основные особенности медиашлюза UMG8900.
4. Основные характеристики медиашлюза UMG8900.
5. Архитектура UMG8900.
6. Место медиашлюза UMG8900 в архитектуре NGN.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 4

«Оборудование технологии NGN: сервер медиаресурсов»

Цель: Получить практические навыки по разработке сетевых решений с использованием сервера медиаресурсов MRS6100 Huawei.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

Сервер медиаресурсов MRS6100 является ключевым ресурсным компонентом сети NGN и предоставляет дополнительные услуги.

Сервер MRS6100 предлагает следующие услуги обработки мультимедийных данных в сети NGN:

Воспроизведение сообщений;
Синтез речи;
Распознавание речи;
Запись;
Аудиоконференция;
Видеоконференция.

MRS6100 контролируется такими устройствами, как Softswitch и сервером приложений (AS). Он предоставляет функции ресурсов мультимедиа в сети NGN.

Если управление осуществляется SoftSwitch, то MRS6100 предоставляет следующие функции:

− Ресурсы тонов сигнализации; − Ресурсы конференцсвязи; − Ресурсы сбора цифр.

MRS6100 может использоваться совместно с SoftSwitch и AS (MediaX3600) для создания сети. Сеть предоставляет услуги интерактивного речевого ответа (IVR). Поддерживаются следующие функции:

− Резервирование конференции; − Участие в конференции; − Завершение конференции; − Изменение полномочий для участников конференции.

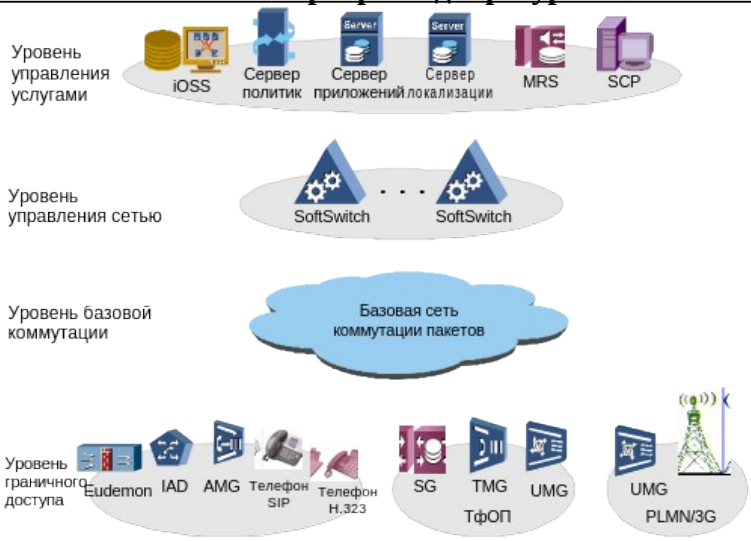
MRS6100 может использоваться совместно с SoftSwitch, AS и медиа устройствами для создания сети.

Основные характеристики:

Поддерживаемая емкость • 7200 каналов
Производительность • До 1440 обращений в секунду
• 5 184 000 BHCA
Емкость общей шины • 4,8 Гбит/с
Протоколы сигнализаций IP/ NGN • H.248
• MGCP
• SIP

• SNMP
Поддерживаемые аудио-кодеки • G.711
• G.723.1
• G.726
• G.729A
Поддерживаемые видео-кодеки • H.263
Поддерживаемые функции • проигрывание анонсментов
• распознавание набора номера
• синтезация речи
• распознавание речи
• запись
• поддержка аудио и видеоконференций
• работа с факсами
Организация аудиоконференции • поддержка до 120 участников конференции
• поддержка до 2400 трехсторонних конференций
• поддержка распознавания номера, проигрывания анонсментов и записи для каждого из участников конференции

<u>Сетевое решение с использованием сервера медиаресурсов MRS6100 Huawei</u>



Сервер медиаресурсов MRS6100 Huawei входит в состав у*ровня управления услугами*, который служит для предоставления дополнительных услуг и поддержки эксплуатации на основе установленных соединений.

Задание:

Разработать сетевые решения с использованием сервера медиаресурсов MRS6100 Huawei.
Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Схемы, графики, результаты вычислений.
4. Выводы по выполненной работе.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 5

«Оборудование и ПО интегрированной системы управления фиксированной сетью»

Цель: Получить практические навыки по разработке сетевых решений с использованием интегрированной системы управления фиксированной сетью iManager N2000 Huawei.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

Интегрированная система управления фиксированной сетью типа iManager N2000 предназначена для управления устройствами фиксированной сети корпорации Huawei.

В структуре сети система iManager N2000 **реализует** уровень сетевого управления (NML).

Система iManager N2000 **осуществляет** комплексное управление всеми устройствами FN корпорации Huawei, как то:

Устройствами широкополосного доступа;
Устройствами доступа к интегрированным службам;
Устройствами сетей следующего поколения (NGN);
Устройствами узкополосного доступа.
Помимо этого, iManager взаимодействует с NMS верхнего уровня и OSS.

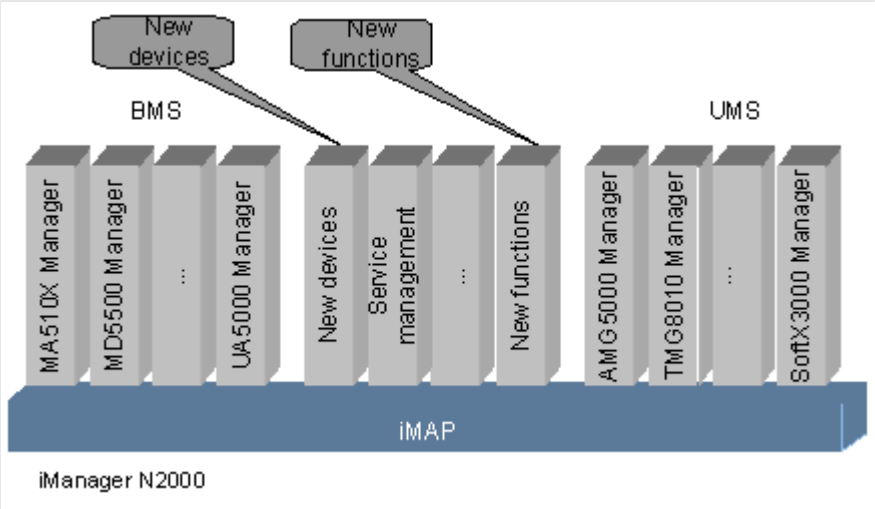
В сети NGN iManager N2000 **осуществляет** управление следующими устройствами, разработанными корпорацией Huawei:

Гибкий коммутатор (SoftSwitch) типа SoftX3000 (SoftX3000);
Медиа-шлюз доступа (серии AMG5000);
Медиа-шлюз соединительных линий TMG8010 (TMG8010);
Устройства интегрального доступа серии (серии IAD);
Универсальный медиа-шлюз UMG8900 (UMG8900);
Шлюз сигнализации SG7000 (SG7000);
Сервер ресурсов MRS6000/MRS6100 (MRS6000/MRS6100);
Менеджер ресурсов RM9000 (RM9000);
Контроллер сессии Eudemon2100/2200 (Eudemon2000/2200);
MA5800 CMTS (MA5800);
SHLR9200;
iGateway Bill (iGWB).

iManager N2000 **реализует** следующие функции:

Управление топологией;
Управление конфигурацией;
Управление при сбоях и неисправностях;
Управление характеристиками сети;
Управление безопасностью.

Программные модули iManager N2000



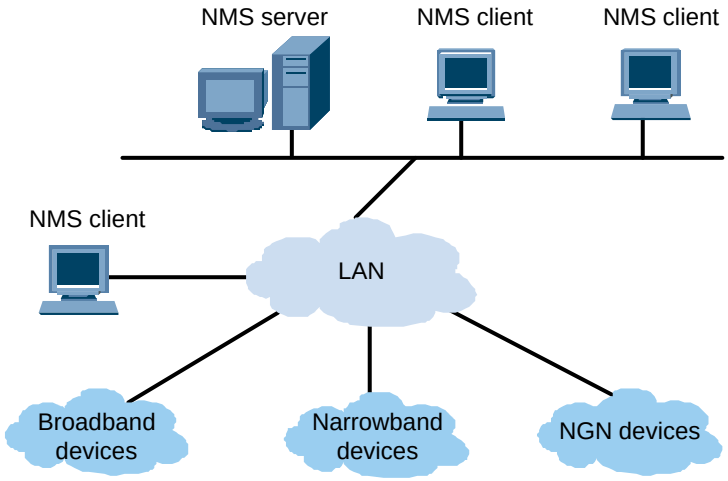
New devices	- Новые устройства
New functions	- Новые функции
Service Management	- Управление услугами
MA510K Manager	- Менеджер MA510K
MD5500K Manager	- Менеджер MD5500K
AMG5000 Manager	- Менеджер AMG5000
TMG8010 Manager	- Менеджер TMG8010
SoftX3000 Manager	- Менеджер SoftX3000

Рис. 1 Архитектура программного обеспечения iManager N2000

Каждый из модулей, показанных на рисунке, поддерживает одну определенную систему управления услугами. Например, "MD5500 Manager" осуществляет управление услугами, обеспечиваемыми устройствами MD5500.

Аппаратные средства iManager N2000

N2000 состоит из одного сервера NMS и нескольких клиентов NMS. Взаимодействие между сервером NMS и клиентами NMS осуществляется через LAN или WAN.
Рисунок 2 иллюстрирует структуру сервер/клиент системы iManager N2000.



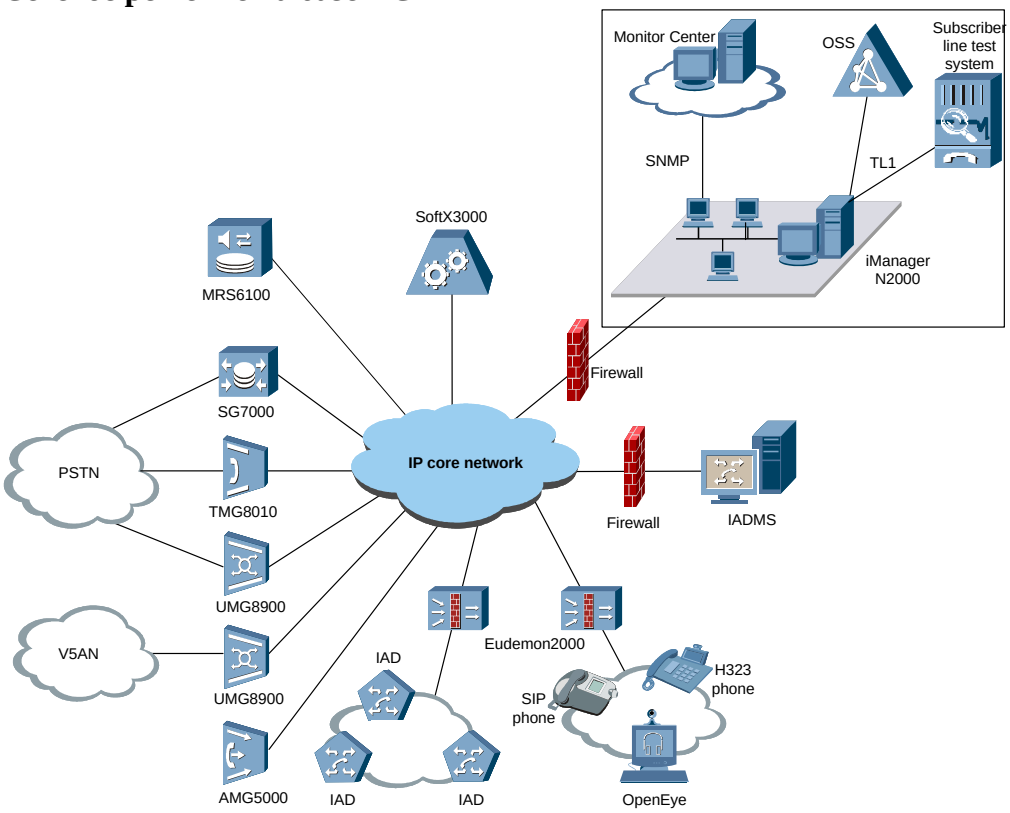
NMS server	- сервер NMS
NMS client	- клиент NMS
Broadband devices	- устройства широкополосного доступа
Narrowband devices	- устройства узкополосного доступа
NGN devices	- устройства NGN

Рис. 2 Структура аппаратных средств системы iManager N2000

Сервер NMS может быть реализован на базе рабочей станции SUN или PC. В качестве OS может использоваться операционная система Solaris или Windows 2000 Server.

Программное обеспечение сервера и клиента NMS может быть установлено в одном и том же PC. Для реализации недорогой системы NM можно использовать ПО SQL Server.

Сетевое решение на базе NGN



Monitor Center	- Центр мониторинга
Subscriber line test system	- Система тестирования абонентских линий
IP core network	- Базовая сеть IP
Firewall	- сетевой экран
H323 phone	- телефон H323
SIP phone	- телефон SIP
OpenEye	- персональный терминал на базе ПК

Рис. 3 Построение сети при реализации NM на базе NGN

В данной реализации iManager N2000 осуществляет управление следующими устройствами NGN, разработанными корпорацией Huawei:

SoftX3000
TMG8010
UMG8900
IAD

Кроме того, iManager N2000 обеспечивает:

Интерфейс SNMPV3 в сторону NMS верхнего уровня

Интерфейс поддержки услуг TL1 в сторону OSS верхнего уровня

Интерфейс MML в сторону элементов верхнего уровня системы тестирования абонентских линий.

Задание:

Разработать сетевые решения с использованием интегрированной системы управления фиксированной сетью iManager N2000 Huawei.

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Схемы, графики, результаты вычислений.
4. Выводы по выполненной работе.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 6

«Конфигурирование аппаратной части Softswitch»

Цель: Получить практические навыки по конфигурированию аппаратной части гибкого коммутатора SoftX3000 Huawei..

Время выполнения: 4 часа.

Оборудование: ПК; Гибкий коммутатор SoftX3000 Huawei.

Ход работы:

Теоретические сведения:

Существуют два режима конфигурирования в системе: добавление данных в режиме online и добавление данных в режиме offline. В режиме offline данные сохраняются на BAM-е и при переходе в режим online сразу же отправляются на полку (host). В режиме online все данные немедленно передаются с BAM- а на полку. Как правило, при начальной конфигурации мы используем режим offline.

6.1. Переход в режим offline .

LOF:;

Режим форматирования базы данных предназначено для упорядочивания данных в таблицах и преобразования в нужный формат для плат CDBI.

Выключение режима форматирования.

SET FMT: FMT=OFF;

Добавление статива:

ADD SHF. SN=0, LT="Huawei Training Center", PN=707, RN=1, CN=0; SN=0 номер статива;

LT="Huawei Training Center" расположение;

PN=0 707 комната;

RN=0 ряд;

CN=0 позиция;

Добавление полки:

ADD FRM: FN=0, SN=0, PN=2;

FN=0 номер полки; SN=0 номер статива;

PN=2 расположение полки в стативе (4 позиции в стативе).

Добавление плат:

ADD BRD: FN=0, SN=0, LOC=FRONT, BT=IFMI, MN=132, ASS-1;

FN=0 номер полки;

SN=0 номер слота в котором расположена плата; LOC=FRONT фронтальное или тыльное расположение платы;

BT=IFMI тип платы;

MN= 132 номер модуля;

ASS=T номер слота в котором расположена резервная плата.

ADD BRD: FN=0, SN=4, LOC=FRONT, BT=FCCU, MN=22, ASS=5;

ADD BRD: FN=0, SN=10, LOC=FRONT, BT=CDBI, MN=102, ASS=11; ADD BRD: FN=0, SN=12, LOC=FRONT, BT=BSGI, MN=136, ASS=255; ADD BRD: FN=0, SN=13, LOC=FRONT, BT=BSGI, MN=137, ASS=255; ADD BRD: FN=0, SN=14, LOC=FRONT, BT=MSGI, MN=211, ASS=255;

ADD BRD: FN=0, SN=4, LOC=FRONT, BT=MSGI, MN=210, ASS=255;

Распределение протоколов по модулям:

Разные модули обрабатывают разные протоколы, по умолчанию модуль BSGI обрабатывает протоколы MGCP,H.248, SCTP, а модуль MSGI обрабатывает протоколы TRIP, ENUM, STUN, MIDCOM и RADIUS. Это уже определено в системе в команде ADD BRD, команда SET DPA определяет для конкретного модуля обработку конкретного протокола, допустим у нас много абонентов MGCP, данная функция позволяет определить целый модуль для обработки только MGCP протокола.

SET DP: MN=136, DA=MGCP-1&H248-1&SCTP-1;

Стандартно

MN=133 номер модуля;

DA=MGCP-1&H248-1&SCTP-1 поддержка обработки протоколов

SET DPA: MN=211, DA=TRIP-L&ENUM-L&STUN-L&MIDCOM-L&RADIUS-L;

Дополнительно

TRIP

ENUM

STUN

MIDCOM

RADIUS

Назначение функций плате CDBI:

ADD CDBFUNC: CDPM=102, FCF=LOC-L&TK-L&MGWR-L&BWLIST_-L&-IPN-L&DISP-1 &SPDNC-1 &RACF-1 &PRESEL-1 &UC-1 &KS-1; CDPM=102 номер модуля;

FCF - выбираем все функции в случае одного модуля CDBI или половину функций на один модуль и половину функций на второй модуль в случае двух модулей плат CDBI.

Включение режима форматирования:

SET FMT: FMT=ON;

6.2. Переход в режим online.

LON:;

Выполнение форматирования данных для соответствия баз данных MS SQL и базы на плате CDBI:

FMT:;

Перезагрузить полку SoftX3000!!!

Добавление IP-адреса на плату IFMI.

ADD FECFG: MN=132, ГР="10.7.5.1", MSK="255.255.255.0", DGW=" 10.7.5.254";

MN=132 номер модуля IFMI;

IP="10.7.5.1" IP-адрес SofftX3000;

MSK="255.255.255.0" маска сети;

DGW="10.7.5.254" шлюз по умолчанию.

Общие параметры для протокола H.323.

ADDH323SYS: SYSNM="Huawei_V3", IRC=3;

SYSNM="Huawei_V3" имя, которое используется при регистрации на внешнем GK;

IRC=3 это количество посылаемых ответов IRR до получения подтверждения LACK от GK.

Общие параметры для протокола H.323:

ADD H323APP: MN=134, IPDMN=132, MTYP-RCAPP; CALLMINPRT=6000, CALLMAXPRT=10000;

MN=134 номер модуля;

IPDM1SN132 номер модуля;

MTYP=RCAPP прохождение протоколов RAS и Q.931; CALLMINPRT=6000 минимальное значение порта; CALLMAXPRT=10000 максимальное значение порта;

Общие параметры для протокола SIP:

SET SIPCFG: UCH=NO,UST=YES;

UCH=NO отмена использования компактных SIP - заголовков;
UST=YES использование всех внутренних таймеров протокола SIP.
SET SIPLP: MN=134,PORT=5061;
MN=211 номер модуля MSGI;
PORT=5061 номер порта для этого модуля.

Задание:

1. Сконфигурировать SoftX3000 Huawei в режим offline .
2. Сконфигурировать SoftX3000 Huawei в режиме online.

Контрольные вопросы:

1. Пояснить конфигурирование в режиме offline.
2. Какую информацию содержит меню «Добавление статива»?
3. Какую информацию содержит меню «Добавление модуля»?
4. Какую информацию содержит меню «Добавление платы»?
5. Пояснить конфигурирование в режиме online.
6. Какие протоколы используются в работе SoftX3000 Huawei?

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 7

«Базовая настройка Softswitch.»

Цель: Изучить назначение, технические характеристики и конструкцию гибкого коммутатора SoftX3000 Huawei.

Время выполнения: 8 часов.

Оборудование: Гибкий коммутатор SoftX3000 Huawei.

Ход работы:

Теоретические сведения:

SoftX3000 представляет собой программный коммутатор большой емкости и высокой производительности.
SoftX3000 может применяться на уровне управления сетью NGN и обеспечивает управление вызовами и управление соединениями для услуг передачи речи, данных и мультимедийных услуг на базе IP-сети.
SoftX3000 предоставляет богатый набор моделей организации сети и услуг. В процессе развития и интеграции традиционных сетей ТфОП в сеть NGN, оборудование SoftX3000 может использоваться в качестве оконечной станции (станции C5), транзитной станции (станции C4), междугородной станции, шлюзовой станции, SSP и т. д.

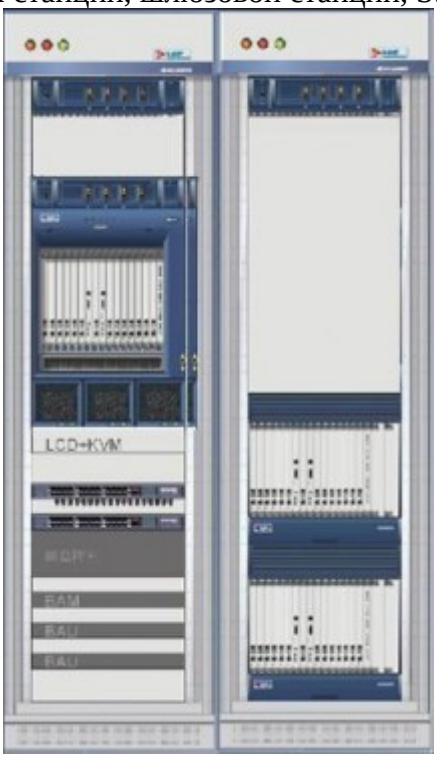


Рис. 1. Внешний вид

Использование в качестве оконечной станции (станция C5)
SoftX3000 полностью унаследовал все услуги ТфОП и поддерживает несколько протоколов сигнализации, включая:

- MGCP (NCS и TGCP);
- H.248;
- V5;

Цифровая абонентская сигнализация №1 (DSS1);

- SIP;
- H.323.

Телефонные аппараты POTS, ISDN, MGCP, H.248, SIP и H.323 могут подключаться к сети, если сеть содержит SoftX3000, IAD, UA и UMG.

SoftX3000 предоставляет несколько типов услуг, например, услуг передачи голоса, данных и мультимедийных данных.

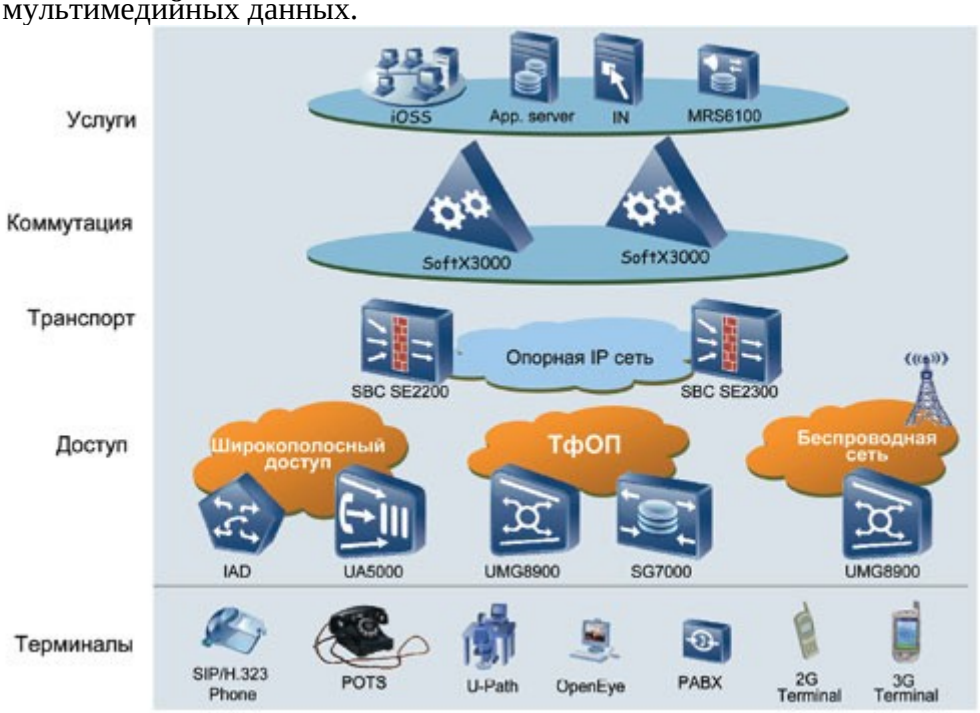


Рис. 2. Архитектура NGN

Использование в качестве транзитной станции (станция С4) или междугородной станции

SoftX3000 поддерживает традиционную сигнализацию ТфОП, например:

- SS7;
- Система сигнализации по общему каналу №5 (SS5);
- Сигнализация R2;
- DSS1;
- V5.

При взаимодействии с SG, TMG, UMG и другими шлюзами SoftX3000 предоставляет доступ и возможности соединительной линии в качестве коммутатора ТфОП.

Использование в качестве шлюзовой станции

SoftX3000 поддерживает черный и белый списки, аутентификацию вызовов, перехват вызовов, большую емкость для хранения данных квитанций и т. д.

SoftX3000 может действовать в качестве шлюзовой станции.

Использование в качестве SSP

SoftX3000 поддерживает INAP и расширенный MTP. SoftX3000 может выступать в качестве SSP в традиционной системе IN или интеллектуальной сети.

Использование в качестве GK или GW

SoftX3000 поддерживает H.323. Он может функционировать в качестве GK или GW в сети VoIP.

Использование в качестве сервера SIP

SoftX3000 поддерживает SIP и может действовать в качестве сервера SIP.

Использование в качестве VIG

SoftX3000 поддерживает RAS, Q.931 и H.245 и может работать в качестве шлюза видеовзаимодействия (VIG) вместе с оборудованием UMG8900 компании Huawei.

Разнообразные функции предоставления услуг

SoftX3000 не только наследует различные сервисные функции от традиционных ТфОП и IN, но и предоставляет дополнительные виды обслуживания на основе архитектуры NGN. SoftX3000 поддерживает следующие сервисные модели:

Поддержка всех голосовых услуг C&C08 Switch, включая основные голосовые услуги и дополнительные услуги.

Предоставление оптимизированного решения IP Centrex для поддержки услуг IP Centrex, консоли IP и глобальных услуг Centrex.

Поддержка протоколов T.38 и T.30 и предоставление высококачественных IP-услуг факсимильной и модемной связи.

Поддержка SIP и H.323, для предоставления услуг видеотелефонии, электронных досок объявлений, видеоконференцсвязи и совместного использования программ.

Совместное функционирование с SCP в INAP для предоставления традиционных услуг IN, таких как CCS, APS, FFPH и VPN.

Использование SIP для функционирования в качестве сервера приложений SIP.

Взаимодействие с SHLR по расширенному MAP для предоставления в интеллектуальной сети дополнительных видов обслуживания, таких как подписка на услуги IN для вызывающих и вызываемых абонентов, услуги NP, услуги MON и услуги CUG.

Мощные и гибкие функции организации сети

Система SoftX3000 предоставляет открытые и стандартные интерфейсы. SoftX3000 поддерживает множество протоколов сигнализации, включая MGCP, H.248, SIP, SIGTRAN и ряд традиционных систем сигнализации ТфОП, например, OKC7, R2, DSS1 и V5. SoftX3000 имеет мощные и гибкие функции организации сети.

Поддержка MGCP и H.248 в качестве протоколов управления медиашлюзом, возможность взаимодействия с устройствами IAD, UA, TMG и UMG, а также предоставление доступа к пакетным терминалам MGCP и H.248.

Поддержка протоколов SIP и SIP-T для взаимодействия с другими системами Softswitch и серверами приложений SIP, а также предоставление непосредственного доступа пакетным терминалам SIP.

Поддержка протокола H.323 для взаимодействия с традиционными шлюзами VoIP и блоками управления многоточечной связью (MCU), а также предоставление непосредственного доступа пакетным терминалам H.323.

Поддержка V5.2, DSS1 и R2. При взаимодействии с UMG, SoftX3000 может подключаться к PBX, NAS, устройствам доступа и BSC.

Использование MTP, подсистемы телефонных пользователей (TUP) и подсистемы пользователей ISDN (ISUP) для подключения к пунктам сигнализации (SP) и транзитным пунктам сигнализации (STP) в сети SS7. При взаимодействии с TMG, UMG, SoftX3000 предоставляет соединительные линии №7 для взаимодействия со станциями ТфОП.

Поддержка подсистемы управления сигнальными соединениями (SCCP), прикладной подсистемы возможностей транзакций (TCAP), INAP и MAP, реализация функции коммутации услуг (SSF), благодаря чему может использоваться в качестве SSP в IN.

Использование подсистемы передачи сообщений 2 Уровня адаптации пользователя (M2UA) для подключения к TMG со встроенными функциями шлюза сигнализации.

Использование простого прохождения дейтаграмм UDP через преобразователи сетевых адресов (STUN) для получения доступа к корпоративным сетям по устройствам NAT.

Использование стандартных интерфейсов для доступа к NMS, включая простой протокол управления сетью (SNMP) и язык человек-машина (MML).

Поддержка протокола передачи файлов (FTP) и протокола доступа и управления передачей файлов (FTAM) для доступа к центру биллинга.

Большая емкость и высокий уровень интеграции оборудования

При полной конфигурации SoftX3000 поддерживает:

40 модулей обработки услуг

BHCA 16000k
360000 соединительных линий TDM или 2000000 абонентов

Высокая надежность

Для обеспечения высокой надежности системы в структуре аппаратных средств, структуре программного обеспечения, средствах управления перегрузкой системы и системе тарификации SoftX3000 принят ряд защитных мер.

Конструкция аппаратной части: использует активный/резервный режим, режим разделения нагрузки и конфигурирование избыточности для плат; оптимизирует обнаружение неисправностей и технологии изоляции плат и системы для обеспечения удобства эксплуатации всей системы.

Конструкция программного обеспечения: применяется иерархическая модульная архитектура с защитными характеристиками, функциями отказоустойчивости и функцией мониторинга неисправностей.

Управление перегрузками системы: Предусмотрены четыре уровня ограничения перегрузки, режим динамической корректировки кодов и управление трафиком для полного обеспечения надежности системы.

Систем тарификации: Сервер iGWB используется в качестве шлюза тарификации SoftX3000. Он применяет функцию двойного горячего резервирования и конфигурируется с массивом жестких дисков Hot RAID5 для реализации двойного резервирования и хранения большого количества сетов.

Высокая безопасность

NGN является открытой и распределенной сетью. В сети используются открытые протоколы и интерфейсы, посредством которых компоненты сети взаимодействуют друг с другом. Организация сети NGN является весьма гибкой. Однако такая открытость приводит также к неизбежным проблемам безопасности, так как IP-сеть характеризуется бесшовными соединениями.

Для обеспечения безопасности сети и пользователей SoftX3000 оборудован совершенным механизмом защиты от следующих видов атак:

Злонамеренные атаки;

Нелегальная регистрация;

Анонимные вызовы;

Перехват телефонных разговоров;

Хищение учетных записей;

Другие нелегальные атаки.

Безопасность сетевых приложений

Закрытие неиспользуемых интерфейсов;

Поддержка контента расширений протокола безопасности IP (IPSec).

Блокировка атак отказа в обслуживании (DoS).

Безопасность протоколов и соединений

Поддержка защиты протоколов и шифрования пакетов протоколов, в том числе MGCP, H.248, SIP и H.323.

Безопасность данных

Резервирование данных между активными и резервными платами в режиме реального времени.

Автоматическое резервное копирования базы данных активного блока обработки во флэш-память.

Автоматическое резервное копирования счетов.

Безопасность абонентов

Сертификация и аутентификация всех устройств, подключаемых к SoftX3000.

Шифрование данных аутентификации пользователя.

Безопасность эксплуатации и технического обслуживания

Поверка учетной записи и IP-адреса при входе в систему.

Управление уровнями полномочий абонентов.

Возможности плавного расширения

В SoftX3000 предусмотрена возможность плавного расширения аппаратных средств и производительности обработки системы, причем учтены потенциальные требования к расширению со стороны пользователей.

Дизайн аппаратного обеспечения:

Система SoftX3000 использует архитектуру на базе открытых интерфейсов (OSTA) в качестве аппаратной платформы. Эта платформа имеет модульную структуру с перекрытиями.

Путем добавления полок обработки с использованием стандартных блоков (полки соединяются между собой через коммутатор LAN) можно легко сконфигурировать от 1 до 18 полок, что позволяет удовлетворить требования пользователей к плавному расширению.

Оптимизированные возможности тарификации и функции управления квитанциями

Краткий обзор

SoftX3000 имеет улучшенные правила тарификации и может выполнять тарификацию услуг передачи голоса, данных и видео с помощью режимов тарификации и типов квитанций и управлять счетами. Основные характеристики:

Поддержка нескольких режимов тарификации на основе длительности вызовов, пропускной способности, временного сегмента, категории времени и тарифицируемой стороны (вызывающий абонент, вызываемый абонент или третья сторона).

Поддержка тарификации дополнительных услуг.

Поддержка тарификации вызовов Centrex.

Поддержка ограничений вызовов по квотам и по времени.

Поддержка квитанций различных типов, в частности, подробных квитанций, квитанций тарифных счетчиков абонентских линий, квитанций тарифных счетчиков соединительных линий, квитанций тарифных счетчиков, квитанций продолжительности занятия соединительной линии, аварийных квитанций, квитанций отказов, квитанций жалоб и квитанций интеллектуальных вызовов.

Поддержка разделенной квитанции при длительном вызове.

Поддержка тарификации мультимедийных услуг предоплаты (отдельно видео и аудио).

Поддержка записи потока вызова в направлении отправки и в направлении приема.

Основные характеристики оборудования.

Таблица

Параметр	Значение
Поддерживаемая емкость	• До 2 миллионов аналоговых абонентов • До 360 000 цифровых СЛ (64 кбит/с)
Производительность	• 16M BHCA
Протоколы сигнализаций IP/ NGN	• H.323 • H.248 • MGCP • SIP/SIP-T • BICC • SIGTRAN
Протоколы сигнализаций ТфОП	• OKC7 (включая INAP-R, ISUP-R) • DSS-1 • R1.5 • R2 • V5
Дополнительные функции	• Поддержка черных/белых списков (до 2 млн абонентов) • Аутентификация вызовов • Перехват вызовов • Возможность работы в двухсвязном режиме (dual-homing) • Поддержка до 50 кодов стран • Поддержка до 500 зональных кодов • Поддержка до 256 кодов пунктов сигнализации • Поддержка до 1000 категорий тарификации • IP Centrex

Задание:

1. Изучить назначение и технические характеристики гибкого коммутатора SoftX3000 Huawei.
2. Изучить конструкцию SoftX3000 Huawei.

Контрольные вопросы.

1. Назначение гибкого коммутатора SoftX3000 Huawei.
2. Область применения гибкого коммутатора SoftX3000 Huawei.
3. Основные особенности SoftX3000.
4. Основные характеристики SoftX3000.
5. Место SoftX3000 в архитектуре NGN.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 8

«Настройка потоков E1»

Цель: Изучение настройки потоков E1.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

E1 – это цифровой поток передачи данных, соответствующий первичному уровню европейского стандарта иерархии PDH. В отличие от американской T1, E1 имеет 30-каналов каждый по 64 кбит/сек для голоса или данных и 2 канала для сигнализации – один для синхронизации оконечного оборудования – содержит кодовые синхрослова и биты сигнализации, другой для передачи данных об устанавливаемых соединениях. Общая пропускная способность E1 = 2048 Кбит/с.

Существуют три вида структуры потока E1: неструктурированный поток, поток с цикловой структурой и поток с цикловой и сверхцикловой структурой.

Неструктурированный поток используется в сетях передачи данных и не имеет цикловой структуры, т.е. разделения на каналы.

Цифровые системы передачи и коммутации работают только со структурированным потоком E1.

Поток,структурированный по циклу предусматривает разделение на 32 ОЦК. Передача 32 канальных интервалов образует цикл (рис 1.2.).

Для каждого КИ в цикле отводится 8 бит, т.е. цикл состоит из 8 бит х 32 КИ = 256 битов, что составляет $T_ц=T_д=125$ мкс.

В течение одного КИ, длительность которого равна 3910 нс, передаётся кодовая комбинация одного телефонного канала.

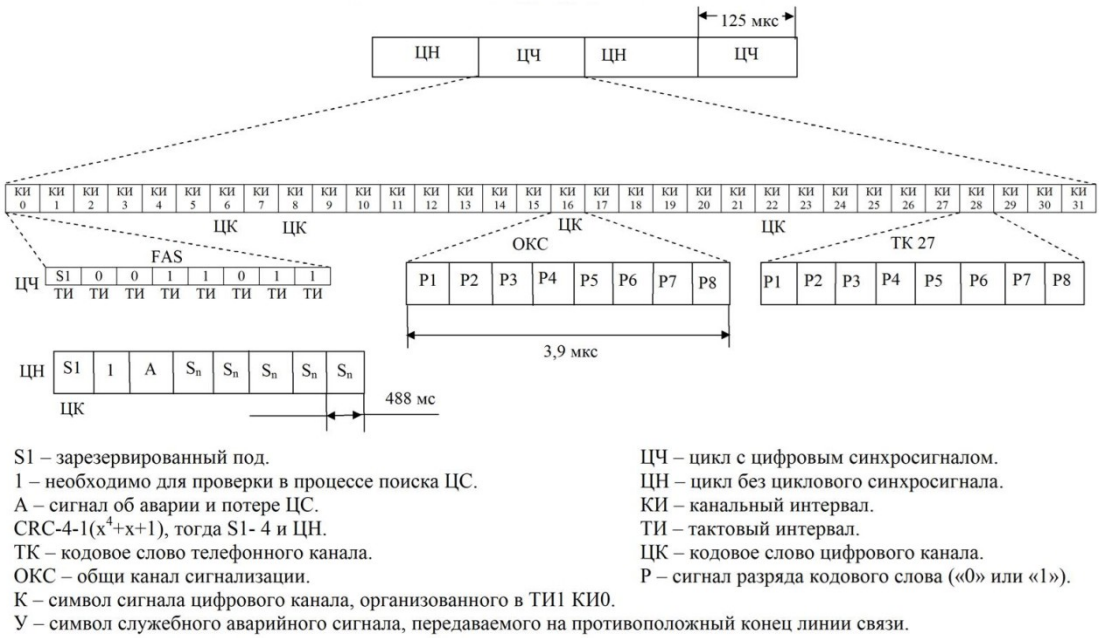
Нулевой канальный интервал КИ0 чётных циклов отводится под передачу сигнала цикловой синхронизации (FAS – Frame Alignement Signal), который передаётся в разрядах 2 – 8 и имеет вид 0011011. В разряде 1 КИ0 передаётся бит Si, зарезервированный под задачи международного использования.

Разряд 3 в КИ0 нечётных циклов используется для передачи сигналов об аварии и потери цикловой синхронизации (бит А). В разряде 2 КИ0 нечётных циклов постоянно передаётся "1", что необходимо для проверки в процессе поиска циклового

синхросигнала. Остальные разряды (с 4 по 8) в КИ0 нечётных циклов обычно незаняты, зарезервированы под задачи национального использования.

Передача потока Е1 с цикловой структурой ИКМ-30 имеет важный механизм – процедуру встроенной диагностики параметров ошибки. Для этой цели используются биты S_i в составе циклового заголовка FAS и NFAS, т.е . четных и нечетных циклов. Процедура использует сверхцикловую структуру 16 циклов и механизм расчета параметра ошибки по контрольному избыточному коду CRC-4 (полином x^4+x+1).

Принцип CRC-4 базируется на простом математическом расчете, производимом в каждом сверхцикле. Оборудование передачи производит расчет суммы CRC-4 и включает результаты суммы в сигнал следующего сверхцикла. Оборудование приемника принимает сигнал и производит аналогичный расчет и сравнение полученной суммы и переданной. Если в двух полученных суммах имеется расхождение, генерируется сигнал ошибки CRC-4.



S1 – зарезервированный под.
1 – необходимо для проверки в процессе поиска ЦС.
А – сигнал об аварии и потере ЦС.
CRC-4-1(x^4+x+1), тогда S1- 4 и ЦН.
ТК – кодовое слово телефонного канала.
ОКС – общи канал сигнализации.
К – символ сигнала цифрового канала, организованного в ТИ1 КИ0.
У – символ служебного аварийного сигнала, передаваемого на противоположный конец линии связи.

ЦЧ – цикл с цифровым синхросигналом.
ЦН – цикл без циклового синхросигнала.
КИ – канальный интервал.
ТИ – тактовый интервал.
ЦК – кодовое слово цифрового канала.
Р – сигнал разряда кодового слова («0» или «1»).

Рис 1.2. Поток Е1, структурированный по циклам

В структурированном по циклам и сверхциклам потоке Е1 16 циклов Ц0 – Ц15 объединяются и образуют сверхцикл длительностью 2 мс (16 циклов ´ 125 мкс), которая приведена на рис. 1.3.

Начало сверхцикла определяется по циклу, который содержит сверхцикловой синхросигнал MFAS вида 0000XYXX. Сам синхросигнал сверхцикловой синхронизации передаётся в разрядах 1 – 4 КИ16 Ц0. X – запасные биты; Y – удаленная неисправность MFAS (равен 1, если потеряна сверхцикловая синхронизация).

В остальных циклах Ц1 – Ц15 КИ16 используется для передачи сигналов управления и взаимодействия между АТС. Сигналы управления и взаимодействия между АТС не требуют 8-ми разрядного кодирования, поэтому в каждом цикле для одного телефонного канала организуются по два одноразрядных сигнальных канала СК. В Ц1 для первого (1 и 2 разряды) и шестнадцатого (5 и 6 разряды) разговорных каналов, в Ц2 – для 2 и 17 разговорных каналов и т.д.

В КИ1 – КИ15 и КИ17 – КИ31 всех циклов передаются кодовые комбинации каналов ТЧ.

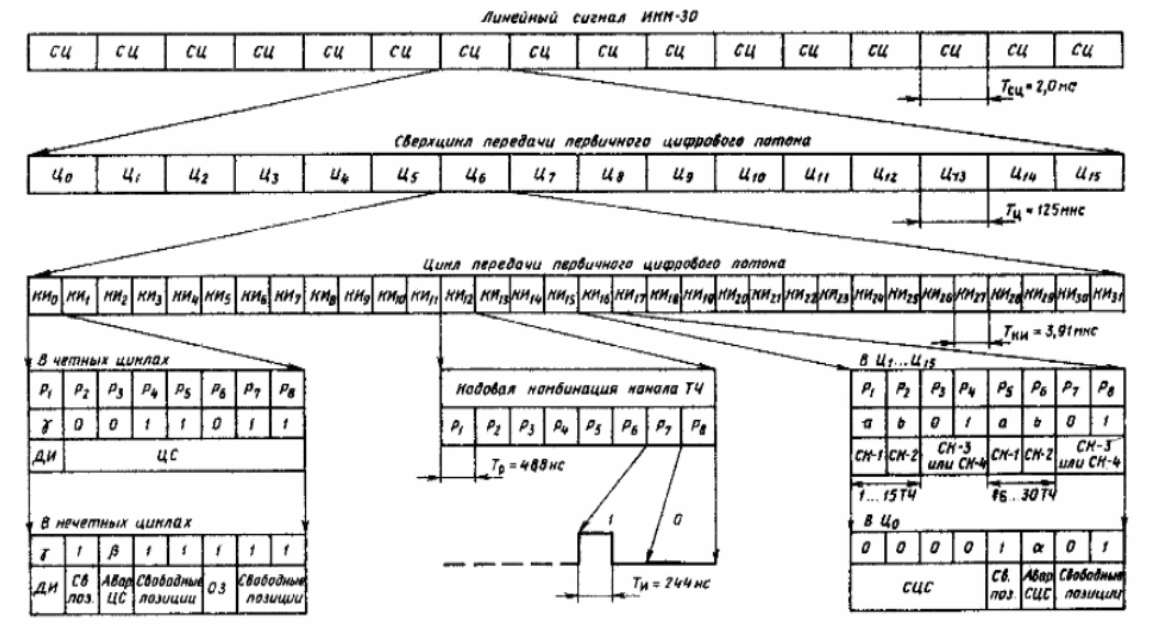


Рис. 1.3. Структурированный по циклам и сверхциклам.

Физический уровень E1 включает в себя описание электрических параметров интерфейсов E1 и параметров сигналов передачи. Маска импульса E1 отражающая параметры интерфейса и форму импульса приведена на рис. 1.4.

Согласно рекомендации G.703 основные характеристики интерфейса, следующие:

Скорость передачи – 2048 кбит/с ± 50 ppm (1 ppm (point per million) равен 10^{-6}), таким образом, допускается отклонение частоты передаваемого сигнала на ± 102,4 Гц. Используемые типы кодирования: HDB3 (AMI – в старых системах передачи).

Помимо параметров частоты сигнала и типа линейного кодирования, рекомендация G.703 определяет следующие нормы на электрические параметры интерфейса (таблица).

Электрический интерфейс E1 представляет собой симметричный интерфейс на 120 Ом. Ему соответствует значения либо ± 3В (для сигнала бинарной 1), либо 0В (для сигнала 0). Реальный сигнал обычно находится в пределах ± 10 % от этой величины.

В идеальном случае передаваемый импульс является совершенно симметричным. Однако в реальной практике импульс сильно искажается при генерации и передаче по каналу связи. Форма импульса потока Е1 должна соответствовать «маске», описанной в рекомендации ITU-T G.703.

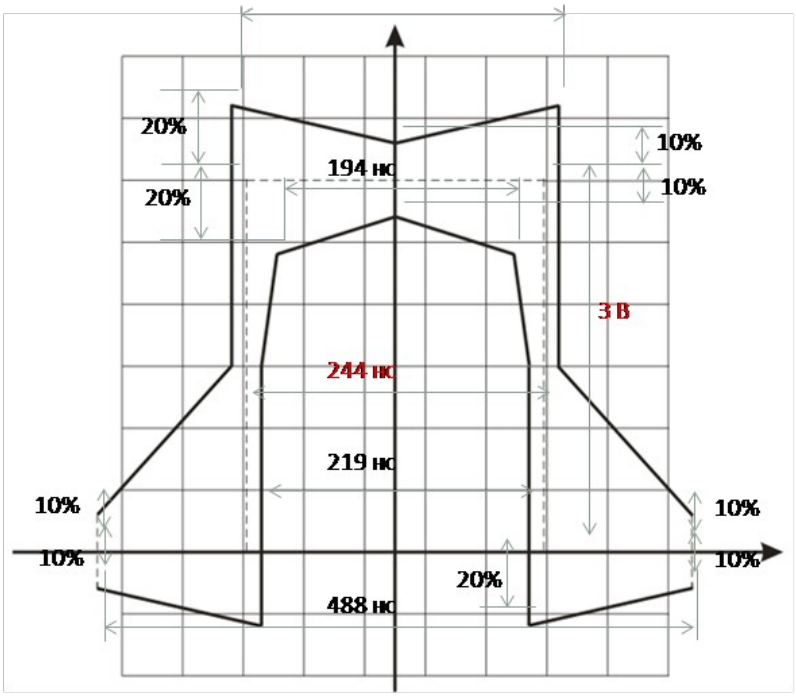


Рис. 1.4. Маска формы импульса Е1

Комплекс измерений параметров, представляющий собой анализ потока Е1 предназначен для определения состояния, предупреждения повреждения и накопления статистических данных, используемых при разработке мероприятий по повышению надежности связи. Измерения производятся в следующих случаях:

·при инсталляции оборудования;

·при проведении приемо-сдаточных испытании;

·во время эксплуатации оборудования при выполнении профилактических, контрольных и аварийных измерений.

Целью измерени ,выполняемых во время инсталляции оборудования является достижением ее соответствующим нормам и стандартам. Приемо-сдаточные измерения проводятся приемными комиссиями для проверки качества выполнения работ и соответствия параметров стандартам и другим нормативным документам. Эксплуатационные измерения проводятся техническим персоналом в процессе текущей эксплуатации оборудования. Их принято делить на профилактические, аварийные и контрольные.

Профилактические измерения выполняются с целью выявления и устранения в процессе эксплуатации отклонений параметров от установленных норм. Программа и

методики этих измерений в основном схожи с программами и методиками приемо-сдаточных испытаний. Правила проведения профилактических измерений этого вида зависит от условий эксплуатации, состояния контролируемых объектов и требований по поддерживанию эксплуатационной готовности.

Аварийные измерения проводятся с целью определения характера и места повреждения. Основными требованиями к аварийным измерениям являются высокая скорость и точность определения характера аварии.

Контрольные измерения осуществляются после окончания ремонтных и аварийных работ. Их целью является определение качества выполнения ремонтно-восстановительных работ. Обычно они включают в себя весь комплекс проверок параметров потока E1 и выполняются по правилам и методикам, принятым для проведения приемо-сдаточных измерений.

Все измерения потока E1 делятся по уровням семиуровневой модели OSI на измерения параметров физического, канального и сетевого уровня.

Задание:

Контрольные вопросы.

1.Определение потока E1?

2.Сколько видов структуры потока E1 и какие?

3.Чему должна соответствовать форма импульса потока E1 в рекомендации ITU-T G.703?

4. В каких случаях производятся измерения параметров потока E1?

Опишите каждый из этих параметров измерения потока E1

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 9

«Настройка интерфейсов SIP»

Цель: изучить основы протокола SIP: понять его архитектуру, роль сообщений (INVITE, REGISTER, ACK, BYE и т.д.) и принципы маршрутизации вызовов. Научиться настраивать SIP-интерфейсы: создание SIP-учетных записей (endpoint’ов), настройка SIP-сервера и SIP-клиентов. Овладеть навыками диагностики и устранения неисправностей: анализ SIP-трафика, поиск и исправление ошибок в настройке. Практически освоить взаимодействие между SIP-устройствами: регистрация, установление и завершение звонков, а также настройка SIP-транков для межсетевого взаимодействия.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

2.1. Основы протокола SIP

- **Что такое SIP:**
  SIP (Session Initiation Protocol) – это прикладной протокол для установления, управления и завершения мультимедийных сессий (голосовых, видео, текстовых и прочих). Он работает на основе текстовых сообщений, схожих с HTTP, что облегчает его понимание и отладку.
- **Архитектура SIP:**
  Протокол оперирует понятиями SIP-клиентов (User Agents), SIP-серверов (Proxy, Registrar, Redirect) и SIP-транков. Каждый участник сессии может выполнять как клиентские, так и серверные функции.
- **Основные SIP-сообщения и их назначение:**
  - **INVITE:** инициирует звонок, приглашая другого участника.
  - **ACK:** подтверждает получение ответа на INVITE.
  - **BYE:** завершает сессию.
  - **REGISTER:** регистрирует SIP-клиента на сервере.
  - **OPTIONS:** проверяет доступность участника.
  - Другие сообщения (например, CANCEL, REFER) используются для управления сессиями.

2.2. Структура SIP-сообщений и параметры

- **Заголовки и тело сообщений:**
  SIP-сообщения состоят из стартовой строки, набора заголовков и, опционально, тела сообщения, в котором часто передаётся информация с описанием медиа-потока (формат SDP – Session Description Protocol).
- **Настройки кодеков и параметров безопасности:**
  Важными аспектами являются выбор кодеков (например, G.711, G.729), поддержка SRTP для шифрования, а также учет особенностей NAT, если SIP-устройства расположены за сетевыми экранами.

2.3. Роль SIP-сервера и SIP-клиентов

- **SIP-сервер (Registrar/Proxy):**
  Обеспечивает регистрацию пользователей, маршрутизацию вызовов, выполнение аутентификации и обработку сигнализации.
- **SIP-клиенты (User Agents):**
  Программные или аппаратные устройства, которые регистрируются на сервере и осуществляют звонки. Примеры – IP-телефоны, софтфоны, мобильные приложения.

Задание:

3.1. Подготовка рабочего окружения

- **Оборудование и ПО:**
  - Сервер с установленной ОС (например, Linux) и SIP-сервером (Asterisk, FreeSWITCH, Kamailio и т.д.).
  - SIP-клиенты: софтфоны (например, Zoiper, X-Lite) или IP-телефоны.
  - Средства для анализа трафика: Wireshark.
- **Подготовка окружения:**
  Убедитесь, что сервер и клиенты находятся в одной сети или настроена корректная маршрутизация/порт-проброс (если используются NAT).

3.2. Настройка SIP-сервера (на примере Asterisk)

3.2.1. Конфигурация файла `sip.conf`

Пример базовой конфигурации:

```
[general]
; Общие настройки
context=default
allowguest=no
udpbindaddr=0.0.0.0
```

```
srvlookup=yes
; Логирование SIP-сообщений для отладки
; debug=yes

; Настройка первого SIP-участника
[101]
type=friend
secret=pass101
host=dynamic
context=internal
disallow=all
allow=ulaw
allow=alaw

; Настройка второго SIP-участника
[102]
type=friend
secret=pass102
host=dynamic
context=internal
disallow=all
allow=ulaw
allow=alaw
```

3.2.2. Конфигурация файла `extensions.conf`

Пример простейшего диалплана для внутренних звонков:

```
[internal]
exten => 101,1,Dial(SIP/101,20)
exten => 102,1,Dial(SIP/102,20)
; Общий пример: все номера набираются с префиксом 9
exten => _9XX,1,Dial(SIP/${EXTEN:1},20)
```

3.3. Настройка SIP-клиентов

- **Регистрация SIP-участников:**

  Настройте SIP-аккаунты в используемом софтфоне, используя следующие параметры:

  - **SIP-сервер:** IP-адрес или доменное имя сервера, где установлен Asterisk.
  - **Номер (логин):** 101 или 102.
  - **Пароль:** pass101 или pass102.
  - **Протокол:** UDP (либо TCP, если настроено).

- **Проверка регистрации:**

  После настройки запустите софтфон и убедитесь, что регистрация прошла успешно (это можно проверить как в интерфейсе клиента, так и через консоль сервера Asterisk с командой `asterisk -rvvv`).

3.4. Тестирование работы SIP-интерфейсов

1. **Регистрация и тестовый звонок:**
   Зарегистрируйте оба SIP-участника (например, 101 и 102) и выполните тестовый звонок между ними:
   - С клиента 101 наберите номер 102.
   - Проверьте установление звонка, передачу аудио и корректное завершение сессии (с помощью кнопки «Hangup» или набора команды BYE).
2. **Анализ SIP-трафика:**
   Используя Wireshark, проследите SIP-сообщения. Обратите внимание на:
   - Регистрационные запросы (REGISTER) и ответы.
   - SIP-сообщения INVITE, ACK, BYE и т.д.
   - Возможные ошибки (например, 404 – Not Found, 486 – Busy Here).
3. **Диагностика и устранение ошибок:**
   Если регистрация или звонок не устанавливается, проверьте:
   - Правильность настроек в sip.conf (логин, пароль, параметры codec).
   - Настройки сети (открыты ли нужные порты, корректно ли настроен NAT, если требуется).
   - Логи сервера Asterisk (подробный вывод с опцией debug).

3.5. Дополнительные эксперименты

- **Настройка SIP-транка:**
  Попробуйте настроить связь между двумя SIP-серверами (например, для межофисной связи). Это позволит ознакомиться с параметрами маршрутизации вызовов между разными доменами.
- **Обеспечение безопасности:**
  Проведите настройку шифрования SIP-сообщений с использованием TLS и SRTP, если программное обеспечение и инфраструктура поддерживают данные возможности.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 10

«Соединение медиашлюза и Softswitch по протоколу H.248»

Цель: Получить практические навыки по конфигурированию Charging Data.

Время выполнения: 8 часов.

Оборудование: ПК;Гибкий коммутатор SoftX3000; Универсальный медиашлюз UMG8900.

Ход работы:

Теоретические сведения:

Указание к выполнению работы:

1. Сделать краткий анализ изученного материала.
2. Раскрыть достоинства и недостатки данной темы.
3. Найти решения проблем, связанных с данной темой.
4. После выполнения работы, сделать выводы по проделанной работе.

Добавление Charging Data

Добавление тарифа: **ADD CHGANA**: CHA=0;

CHA=0 номер тарифа.

Описание тарифа:

MOD CHGMODE: CHA=0, DAT-NORMAL, TS1="00&00", TA1="60", PA1=1, TB1="6 0",
PB1=1, AGIO1=100; CHA=0 номер тарифа; DAT=NORMAL дни работы; TS1=00&00 время окончания первой временной зоны;
TA1="60" первый интервал времени; PA1=1 число тарификационных импульсов;
TBI ="60" последующие интервалы времени;
PB1=1 число тарификационных импульсов за последующие интервалы; AGIO1=100 процент оплаты.

Связь тарифа с абонентом и набираемым префиксом:

ADD CHGIDX: CHSC-0, RCHS-0, LOAD-ALL, BT-ALLBT, CODEC=ALL, CHA=0;
CHSC=0 код выбора тарификации; RCHS=0 код источника тарификации;
LOAD=ALLопределяем сервисы; BT=ALLBT тип квитанций; CODEC=ALL тип кодека;
CHA=0 номер тарифа.

Задание.

1. Сконфигурировать SoftX3000.
2. Сконфигурировать UMG8900.
3. Добавить маршруты и подмаршруты SoftX3000.

Практические задания:

Задание №1. Изобразить схему телекоммуникационной сети (привести расшифровку основных элементов).

Задание №2. Требуется рассчитать транспортный ресурс, необходимый для организация взаимодействия между S-CSCF (Serving - Call State Control Function) и Softswitch, со следующими исходными данными. Ответ указать в Мбит/с. Исходные данные для расчета транспортного ресурса сети представлены в таблице.

Таблица – Исходные данные расчета транспортного ресурса

Nsip	Psx	Lsip	Ksig
15	178 000	160	5

Задание №3. В ходе первоначальной настройки корпоративной мультисервисной сети, для проверки работоспособности оборудования, необходимо произвести базовую настройку IP- телефонии оборудования Cisco, согласно схеме (рисунок).

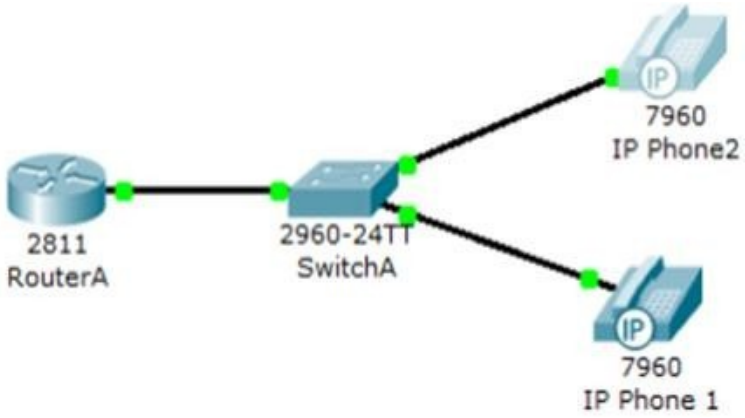


Рисунок – Схема подключения устройств для первоначальной настройки

Разработайте алгоритм базовой настройки с указанием команд и необходимыми пояснениями.

Контрольные вопросы.

1. Описать префиксы выхода на междугороднюю и международную сеть .
2. Пояснить добавление кода зоны.
3. Пояснить добавление города.
4. Пояснить добавление источника вызова.
5. Пояснить добавление и описание тарифа.
6. Пояснить связь тарифа с абонентом и набираемым префиксом

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 11

«Маршрутизация вызовов»

Цель: Изучение маршрутизации вызовов.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

На станции SDE 3000 предусмотрена гибкая система маршрутизации, которая позволяет направить вызов адресату немедленно после получения необходимой информации. Для обеспечения маршрутизации вызовов, в станционной базе данных должна содержаться вся информация, необходимая для интерпретации набранного номера. Для выполнения маршрутизации исходящего вызова на основании числа набранных цифр определяется кодовая точка. Кодовая точка, в свою очередь, определяет адресата для установления соединения. Доступ к этому адресату может быть получен по различным маршрутам, связанным с адресатом. Каждый маршрут задействует различные группы соединительных линий. Кодовая точка используется станцией для определения адресата (к которому должен быть получен доступ) на основании принятых цифр. Анализируемые цифры могут поступить от собственного абонента или могут быть переданы удаленной станцией. Механизмы маршрутизации на станции используют таблицы трансляции цифр, состоящие из взаимосвязанных блоков, которые образуют кодовые точки. Каждый блок анализирует следующее: • Набранный номер. • Абонентская/соединительная линия-источник. • Категория вызывающего абонента. • Тип маршрута. • Ограничение трафика для абонентской/соединительной линии. Анализ последних четырех позиций не обязателен и выполняется в зависимости от того, как определены кодовые точки по MML-команде. Число кодовых точек, которые могут быть определены в каждом конкретном случае, зависит от длины и распределения кодовых точек. Максимальное количество блоков трансляции цифр в таблице трансляции цифр составляет 512, 256 блоков для анализа категории и 256 для анализа источника. Адресат – это некоторый пункт на телефонной сети, доступ к которому возможен со стороны станции. Существует таблица адресатов, в которой содержится вся необходимая информация. Может быть определено максимум 256 адресатов. Маршруты «связывают» адресата с конкретной группой исходящих соединительных линий. Может быть определено максимум 512 маршрутов. Для одного и того же адресата может быть назначено три маршрута: первичный маршрут, который используется при выполнении всех вызовов для данного адресата, а также два альтернативных маршрута, которые используются в случае переполнения на первичном маршруте, называемом также

«маршрутом первого выбора». Группы соединительных линий и соединительные линии. Различают группы исходящих, входящих или двунаправленных соединительных линий (максимум 128). Оператор может устанавливать значения параметров, которыми характеризуются группы соединительных линий: категория, класс обслуживания группы, процедура набора номера, приоритеты и т. д. Максимальное количество соединительных линий – 492. Перехват – это специальная процедура, выполняемая станцией в том случае, когда не может быть обеспечено нормальное прохождение вызова. При этом выполняются определенные действия, заменяющие обычную обработку вызовов. Результат перехвата может быть следующим: • Выполнение трансляции цифр с целью получения нового кода (это приводит к новому вызову); • Посылка многочастотного сигнала по линии; • Подача акустического тонального сигнала или записанного извещения; • Включение параметра cause («причина») в ISUP-сообщение об освобождении. Зоновый пункт определяет тарифную зону для начисления оплаты. Существует специальная таблица зоновых пунктов, которая позволяет оператору определить надлежащий тип учета стоимости (в соответствии с цифрами, набранными абонентом, и с зависимостью от абонентских типов источника, категории и маршрута): • Учет стоимости выполняется на станции SDE 3000, на основе номера зоны, содержащегося в соответствующем номере; • Учет стоимости выполняется на вышестоящей станции; • Учет стоимости выполняется на предыдущей станции; • Учет стоимости не выполняется. Затем оператор может определить зоны, для которых должен выполняться учет стоимости способом LAMA, и назначить этим зонам перечисленные выше типы учета стоимости. После выбора первого доступного определяется уникальным образом. После того как выбрана соединительная линия в группе соединительных линий, устанавливается физическое соединение с позиционным номером станции назначения. Связь между двумя блоками SWU станции SDE или между одним блоком SWU и блоком, реализующим функции транзитной связи (блок Tandem) осуществляется «внутренними соединениями». Такие соединения представляют собой физическую линию связи между двумя блоками SWU, и они характеризуются парами линий PDC, которые определяются концами соединения. Процесс анализа информации о набранном номере представлен на рисунке 1.

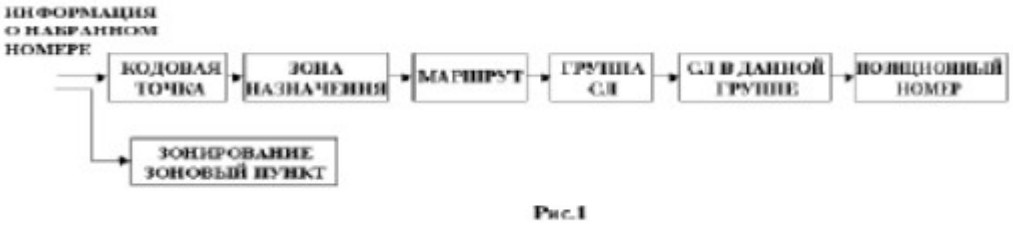


Рис.1

Рис. 1. Процесс анализа информации о набранном номере

Информация о набранном номере указывает кодовую точку. Кодовая точка указывает на адресата. Доступ к адресату осуществляется по маршруту. Маршрут занимает группу соединительных линий. Группа соединительных линий содержит соединительные линии. Соединительная линия ведет к позиционному номеру, определяющему физический порт, через который устанавливается соединение со станцией на противоположной стороне. Последовательность маршрутизации для местного вызова между различными блоками SWU приведена на рисунке 2. В этом случае информация о набранном номере представляет собой номер Вабонента, относящегося к другому блоку SWU. На основании этой информации определяется SWU-адресат. Выбирается внутреннее соединение ICONN, связывающее задействованные блоки SWU. ICONN содержит соединения SPICONN. Производится занятие SPICONN, ведущего к позиционному номеру, определяющему физический порт, через который устанавливается соединение с другим SWU.

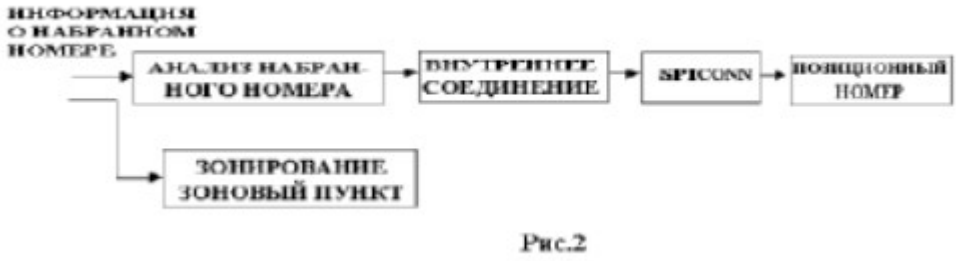


Рис.2

Рис. 2. Последовательность маршрутизации для местного вызова между различными блоками SWU.

Когда соединение не может быть установлено из-за отсутствия кодовой точки, из-за перегрузки и т.д., информация о набранном номере приводит к перехвату, соединяющего абонента с тональным сигналом или с новым кодом, который указывает на другую кодовую точку (тогда выполняется обычная последовательность действий).

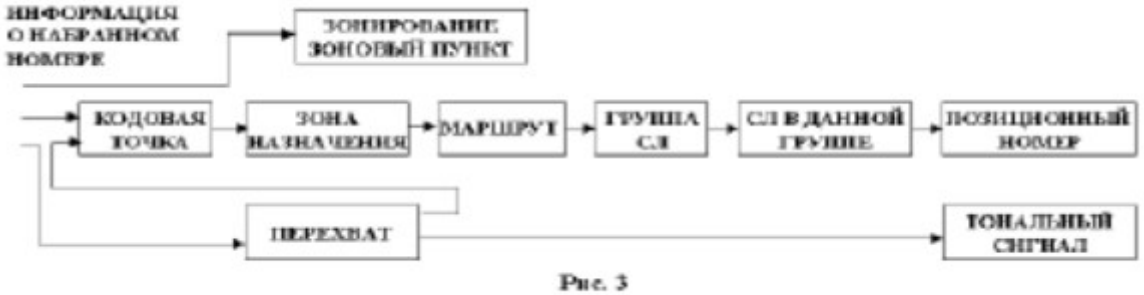


Рис. 3

Рис. 3.

Другая ситуация возникает тогда когда информация о набранном номере ведет к кодовой точке, указывающей на адресата, приводящего к новому коду, указывающему на другую кодовую точку (далее выполняется обычная последовательность действий).

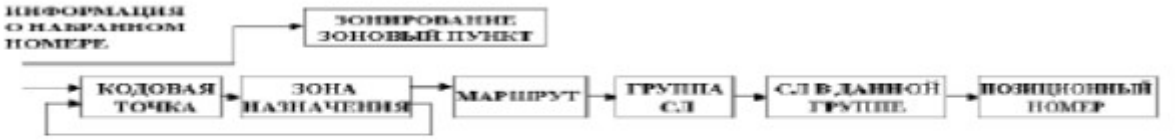


Рис.4

Этот случай часто используется для создания услуг экстренного вызова (спецслужб) типа «FIREBRIGADE» («ПОЖАРНАЯ КОМАНДА»), «POLICE» («МИЛИЦИЯ») и «AMBULANCE» («СКОРАЯ ПОМОЩЬ») с легко запоминаемыми и легко набираемыми комбинациями из 3 цифр. Так как при вводе системы нумерации станции исключается возможность использования коротких кодов спецслужб, то необходимо создание кодовой точки с коротким и удобным кодом спецслужбы, которая в свою очередь порождала бы новый код, удовлетворяющий системе нумерации станции. Пример: XYTHTU – номер полиции (POLICE), должен быть создан легко запоминаемый код доступа (например 101), выполняется следующая последовательность действий: • Создается DESTINATION=POLI с новым кодом доступа к XYTHTU. • Создается кодовая точка для кода 101, указывающая на адресата «POLI». • Создается зоновый пункт для учета стоимости вызовов по коду 101. Кодовая точка создается командой CR CPT: CODE=XÖX, DEST=XÖX; Анализируемыми цифрами могут быть либо набранные цифры, либо цифры, переданные с удаленной станции. Команда отклоняется в следующих случаях: • адресат не существует; • для адресата не созданы маршруты и отсутствует преобразование цифр. Команда создания кодовой точки (когда она создается для пункта назначения) имеет следующие обязательные параметры: CODE – код 1 ÷ 8 шестнадцатиричных цифр. DEST – имя адресата 1 ÷ 6 алфавитно-цифровых символов. Указывается имя зоны назначения, которая адресуется посредством кода. Отмена кодовой точки производится командой CAN CPT: CODE=XÖX; Просмотр кодовой точки ñ командой DISP CPT: DEST=XÖX; Адресат в таблице данных адресатов создается командой CR DEST. Формат ввода команды: CR DEST: DEST=X..X [,DINO=XX] [,MINMAX=XX_XX] [,TLIM=X..X] [,DICON=X..X] [,NADI=X..X]; Команда отклоняется в следующих случаях: • адресат уже существует; • введен DICON и какой-то другой необязательный параметр (DICON не может вводиться вместе с другими параметрами); • количество цифр (DINO) больше минимального значения параметра MINMAX. Команда создания адресата имеет следующие параметры: DEST – имя адресата (1 ÷ 6 алфавитно-цифровых символов) указывает имя зоны назначения, которая адресуется посредством кода. DINO – минимальное количество цифр

для занятия исходящей соединительной линии (от 0 до 20). Этот параметр используется для указания количества цифр, которые необходимо проанализировать для выполнения занятия. Это значение должно быть меньше или равно минимальному значению параметра MINMAX. Значение по умолчанию - 1. MINMAX – минимальное и максимальное число цифр в телефонных номерах, соответствующих этому адресату. Вводится в формате -. Возможные значения: минимум ñ от 1 до 20, максимум от 1 до 20. Если этот параметр пропущен, то в качестве значений по умолчанию используются следующие значения: минимум 1, максимум 20 TLIM – предельное время отключения вызывного сигнала (сек.). Возможные значения от 0 до 600. Этот параметр указывает предельное время получения сигнала ответа при подаче вызывного сигнала. Значение 0 указывает отсутствие предельного времени, это значение применяется в том случае, если удаленная станция не передает сигнал ответа, когда В-абонент снимает трубку. Значения, отличные от 0, лежат в диапазоне от 40 до 600 секунд. Типовые значения: 40, 60, 90, 120 и 150 секунд. Если этот параметр пропущен, то по умолчанию устанавливается предельное время, равное 90 секундам. DICON – код преобразования цифр (от 1 до 16 алфавитно-цифровых символов). Этот параметр указывает последовательность цифр, которая используется для трансляции, требуемой для выполнения новой маршрутизации. В коде должно быть сделано, по крайней мере, одно изменение. Для замены существующей последовательности используются следующие четыре управляющих символа: X – указывает на то, что цифра в этой позиции не изменяется. . – указывает на то, что цифра в этой позиции подавляется. + – указывает на то, что следующая за этим символом цифра должна быть вставлена в указанной позиции. ! – указывает на то, что подавляются все цифры от этой позиции до конца. Наличие цифры (перед которой отсутствуют управляющие символы) указывает на то, что эта цифра заменяет цифру, занимающую текущую позицию (при ее наличии), или в противном случае добавляется к последовательности цифр. Пример 1 Старый код: 09789 DICON: 12X+4 Новый код: 127489 Пример 2 Старый код: 09789 DICON: XX!12489 Новый код: 0912489 NADI – характер индикатора адреса. Этот параметр имеет следующие значения (таблица 1): • Отмена адресата производится командой CAN DEST: DEST=X..X; • Просмотр адресата ñ командой DISP DEST: DEST=XXX; • Зоновый пункт создается командой CR ZOPT. По этой команде вводятся индексы, требуемые для компоновки таблицы трансляции зон. Такая таблица позволяет системе определять номер зоны, которому соответствуют набранные цифры.

Таблица 1

Значение	Описание
1	Абонентский номер (национальное использование)
2	Неизвестный (национальное использование)
3	Национальный номер
4	Международный номер
112 - 126	Зарезервировано для национального использования

Команда будет отклонена, если код зоны уже существует. Формат ввода, для зонового пункта без начисления оплаты следующий (для других видов зоновых пунктов используются дополнительные параметры) CR ZOPT: CODE=XÖX, ZOCHA=XÖX; В случае зонового пункта без начисления оплаты обязательны следующие параметры: CODE ñ код, от 1 до 8 шестнадцатиричных цифр. ZOCHA – характеристика зоны. Указывает, на какой станции должно выполняться зонирование: CONZON – зонируемое соединение, NOCHARGE – без начисления оплаты, ZONINHI – зонирование на вышестоящей станции.

Задание:

Практическое задание

1. Используя пример из теоретической части, создайте службу экстренного вызова с новым кодом доступа, принадлежащим одному из местных телефонов. При создании зонового пункта учета стоимости, используйте параметр: nocharge ñ без учета стоимости.

2. Проверьте прохождение вызовов к экстренной службе.

3. Отмените объекты, созданные для организации экстренной службы.

Контрольные вопросы

1. Дайте определение терминам: кодовая точка, адресат, маршрут, группа соединительных линий, соединительная линия, зоновый пункт, перехват.

2. Объясните схему анализа информации о набранных цифрах номера (рисунок 1).

3. Объясните случай, когда информация о набранном номере ведет к кодовой точке, указывающей на адресата, приводящего к новому коду, указывающему на другую кодовую точку (рисунок 4). На данном примере объясните организацию «коротких» номеров экстренных служб.

4. Каким образом создается адресат с кодом преобразования цифр (DICON)?

5. Какие команды используются при создании кодовых точек, адресатов, зоновых пунктов? Какие параметры вводятся с этими командами?

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 12

«Сетевые настройки»

Цель: Изучение базовых понятий компьютерных сетей: понять, что такое IP-адресация, маска подсети, шлюз, DNS-сервер и их роль в организации сетевого соединения. Освоение методов настройки сетевых параметров: научиться настраивать сетевой адаптер в операционных системах, переключаться между статической и динамической (DHCP) конфигурацией. Получение навыков диагностики сетевых подключений: изучить и использовать инструменты для проверки работоспособности сети (ping, traceroute, nslookup, arp и др.). Формирование представления о маршрутизации и разрешении доменных имен: разобраться в работе протоколов DHCP, DNS и базовых принципах маршрутизации в локальных сетях.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

2.1. Основы компьютерных сетей

- **IP-адрес и маска подсети:**
  IP-адрес – уникальный адрес узла в сети, позволяющий идентифицировать устройство. Маска подсети определяет, какая часть IP-адреса относится к сети, а какая – к узлу.
  Пример: В адресе 192.168.1.100 с маской 255.255.255.0 сеть – 192.168.1.0, а узловая часть – 100.
- **Шлюз по умолчанию (Default Gateway):**
  Это маршрутизатор, через который устройство выходит за пределы своей локальной сети для доступа к другим сетям или в Интернет.
- **DNS-сервер:**
  Служба доменных имен, которая преобразует легко запоминаемые доменные имена (например, www.example.com) в IP-адреса.
- **DHCP (Dynamic Host Configuration Protocol):**
  Протокол, позволяющий автоматически выдавать IP-адреса и другие сетевые настройки клиентским устройствам.

2.2. Режимы настройки сетевых параметров

- **Статическая настройка:**
  Администратор вручную задаёт IP-адрес, маску, шлюз и DNS-сервер. Такой подход используется для серверов и других устройств, требующих постоянного адреса.
- **Динамическая настройка (DHCP):**
  Параметры выдаются автоматически DHCP-сервером. Это удобно для рабочих станций, ноутбуков и мобильных устройств, часто подключающихся к разным сетям.

2.3. Основные инструменты для диагностики сети

- **ping:**
  Проверяет доступность удалённого узла и измеряет время отклика.
- **traceroute (tracert в Windows):**
  Определяет маршрут пакетов до целевого узла, что помогает выявить проблемы на определённых участках сети.
- **nslookup/dig:**
  Инструменты для проверки работы DNS и разрешения доменных имен.
- **arp:**
  Показывает таблицу сопоставления IP-адресов с MAC-адресами в локальной сети.

Задание:

3.1. Подготовка рабочего окружения

- **Оборудование и ПО:**
  - Компьютер или виртуальная машина с установленной операционной системой (Windows или Linux).
  - Доступ к административным правам для изменения настроек сети.
  - Набор стандартных утилит: ipconfig (Windows) или ifconfig/ip (Linux), ping, tracert/traceroute, nslookup/dig, arp.
  - При наличии – доступ к DHCP-серверу (например, роутеру), чтобы переключаться между режимами статической и динамической настройки.

3.2. Практические задания

Задание 1. Просмотр текущих сетевых настроек

1. **В Windows:**
   - Откройте командную строку (cmd) и выполните команду:

```
ipconfig /all
```

   - Обратите внимание на IP-адрес, маску, шлюз и DNS-серверы, назначенные вашему адаптеру.
2. **В Linux:**
   - Откройте терминал и выполните команду:

```
ip addr show

или

ifconfig
```

- Проверьте информацию о сетевом интерфейсе (IP-адрес, маску).

Задание 2. Настройка статического IP

1. **В Windows:**
   - Перейдите в «Панель управления» → «Сеть и Интернет» → «Центр управления сетями и общим доступом» → «Изменение параметров адаптера».
   - Выберите нужное сетевое подключение, нажмите правой кнопкой мыши и выберите «Свойства».
   - Найдите «Протокол Интернета версии 4 (TCP/IPv4)», нажмите «Свойства».
   - Выберите «Использовать следующий IP-адрес» и введите:
     - **IP-адрес:** (например) 192.168.1.50
     - **Маска подсети:** 255.255.255.0
     - **Основной шлюз:** IP адрес вашего роутера (например, 192.168.1.1)
     - **DNS-серверы:** (например) 8.8.8.8 и 8.8.4.4
   - Нажмите «ОК» для сохранения настроек и проверьте изменения с помощью команды `ipconfig`.

2. **В Linux (на примере Ubuntu):**

   - Редактируйте конфигурационный файл (вариант для систем с NetworkManager может отличаться):

     bash — Копировать — Редактировать

     ```
     sudo nano /etc/netplan/01-netcfg.yaml
     ```

   - Пример конфигурации для статического IP:

     yaml — Копировать — Редактировать

     ```yaml
     network:
       version: 2
       renderer: networkd
       ethernets:
         enp3s0:
           addresses: [192.168.1.50/24]
           gateway4: 192.168.1.1
           nameservers:
             addresses: [8.8.8.8, 8.8.4.4]
     ```

   - Сохраните файл и примените настройки командой:

     bash — Копировать — Редактировать

     ```
     sudo netplan apply
     ```

   - Проверьте настройки с помощью:

     bash — Копировать — Редактировать

     ```
     ip addr show
     ```

Задание 3. Возврат к динамической настройке (DHCP)

1. **В Windows:**
   - Повторите шаги по доступу к свойствам TCP/IPv4.
   - Выберите «Получить IP-адрес автоматически» и «Получить адрес DNS-сервера автоматически».
   - Нажмите «OK» и проверьте командой `ipconfig /all`.
2. **В Linux:**
   - Если используется NetworkManager, можно переключиться в автоматическое получение IP через графический интерфейс.
   - Либо отредактируйте конфигурационный файл netplan, задав автоматическую настройку:

     yaml Копировать Редактировать

     ```yaml
     network:
       version: 2
       renderer: NetworkManager
       ethernets:
         enp3s0:
           dhcp4: yes
     ```

   - Примените настройки командой:

     bash Копировать Редактировать

     ```bash
     sudo netplan apply
     ```

   - Проверьте командой `ip addr show`.

Задание 4. Диагностика сетевых подключений

1. **Проверка доступности шлюза и внешних ресурсов:**

   - Используйте команду ping:

```bash
ping 192.168.1.1        # Проверка доступа к шлюзу (роутеру)
ping 8.8.8.8            # Проверка доступа к внешнему серверу (Google
```

2. **Определение маршрута до удалённого узла:**

   - В Windows:

```batch
tracert 8.8.8.8
```

   - В Linux:

```bash
traceroute 8.8.8.8
```

3. **Проверка работы DNS:**

   - Используйте nslookup:

     bash Копировать Редактировать

     ```
     nslookup www.google.com
     ```

     или, в Linux, альтернативно:

     bash Копировать Редактировать

     ```
     dig www.google.com
     ```

4. **Анализ ARP-таблицы:**

   - В Windows:

     batch Копировать Редактировать

     ```
     arp -a
     ```

   - В Linux:

     bash Копировать Редактировать

     ```
     arp -n
     ```

Задание 5. Дополнительное задание

- **Сравнение статической и динамической настройки:**
  Изучите, как меняется поведение системы при использовании статического IP и DHCP. Обратите внимание на:
  - Скорость получения настроек.
  - Возможные конфликты IP-адресов при неправильной конфигурации.
  - Поведение системы при смене сетевой инфраструктуры (например, при подключении к другой сети).

3.3. Сбор результатов и анализ

- **Документирование:**
  Запишите результаты выполнения каждой команды, сделайте скриншоты настроек (если это возможно) и сформулируйте выводы по каждому заданию.
- **Анализ ошибок:**
  Если в процессе настройки или диагностики возникли ошибки, проанализируйте их причины (неверно введённые параметры, проблемы с DHCP-сервером, сбои в работе сетевого адаптера и т.д.) и предложите способы устранения.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 13

«Настройка работы свитча»

Цель: Изучить основные принципы работы сетевого свитча (коммутатора): понять его роль в локальной сети, основные функции и особенности передачи данных на канальном уровне (Layer 2). Овладеть навыками базовой конфигурации свитча: настройка имени устройства (hostname), IP-адреса для управления, создание и назначение VLAN, настройка trunk и access-портов. Изучить технологии повышения отказоустойчивости и безопасности: ознакомление с протоколом Spanning Tree (STP) для предотвращения петель в сети, настройка безопасности портов (Port Security) для ограничения несанкционированного доступа. Развить навыки диагностики и устранения неисправностей: использование команд для просмотра состояния конфигурации, диагностики STP, мониторинга трафика и контроля доступа.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

2.1. Основы работы свитча

- **Что такое свитч:**

  Сетевой коммутатор (свитч) – это устройство, которое осуществляет коммутацию кадров данных на канальном уровне (Layer 2) модели OSI. Он принимает данные, анализирует MAC-адреса и пересылает информацию только на тот порт, где находится адресованный получатель.

- **Функции свитча:**
  - **Коммутация:** передача кадров только на нужный порт.
  - **Фильтрация трафика:** уменьшение количества лишнего широковещательного трафика.
  - **Поддержка VLAN:** логическое разделение сети на сегменты для повышения безопасности и оптимизации трафика.
  - **Поддержка STP:** предотвращение возникновения петель в сети за счёт динамического определения резервных путей.

2.2. VLAN и режимы портов

- **VLAN (Virtual Local Area Network):**
  Позволяет разделить физическую сеть на несколько логических сегментов, что улучшает управление трафиком, безопасность и уменьшает размер широковещательных доменов. Каждому VLAN присваивается уникальный идентификатор (номер) и, как правило, имя.
- **Режимы портов:**
  - **Access-порт:** предназначен для подключения конечных устройств. К каждому access-порту привязывается один VLAN.
  - **Trunk-порт:** используется для соединения между свитчами или между свитчем и маршрутизатором, передаёт трафик сразу из нескольких VLAN, используя механизм тегирования (например, IEEE 802.1Q).

2.3. Протокол Spanning Tree (STP) и безопасность

- **Spanning Tree Protocol (STP):**
  Протокол, предназначенный для обнаружения и устранения петель в сети. Он обеспечивает избыточность, автоматически выбирает корневой мост и блокирует резервные пути для предотвращения дублирования трафика.
- **Безопасность портов (Port Security):**
  Механизм ограничения количества MAC-адресов, которые могут быть ассоциированы с конкретным портом. При превышении лимита возможны действия типа shutdown порта или блокировка дополнительных устройств, что позволяет снизить риск несанкционированного доступа.

Задание:

3.1. Подготовка оборудования и рабочего окружения

- **Оборудование:**
  - Физический свитч (например, модели Cisco, HP, Juniper) или виртуальный эмулятор (Cisco Packet Tracer, GNS3, EVE-NG).
  - Консольный кабель или доступ по Telnet/SSH для выполнения команд конфигурации.
  - Компьютеры или виртуальные машины для эмуляции подключения конечных устройств.
- **Программное обеспечение:**
  - Терминальный эмулятор (например, PuTTY, SecureCRT).
  - При наличии – веб-интерфейс управления свитчем.

3.2. Базовая настройка свитча

Шаг 1. Подключение и начальная конфигурация

1. **Подключение к свитчу:**

   Используйте консольный кабель или установите удалённое подключение (Telnet/SSH) к свитчу.

2. **Настройка имени устройства и баннера:**

   plaintext Копировать Редактировать

   ```
   Switch> enable
   Switch# configure terminal
   Switch(config)# hostname Switch1
   Switch1(config)# banner motd # Добро пожаловать! #
   ```

3. **Настройка IP-адреса для управления (на интерфейсе VLAN):**

   plaintext Копировать Редактировать

   ```
   Switch1(config)# interface vlan 1
   Switch1(config-if)# ip address 192.168.1.2 255.255.255.0
   Switch1(config-if)# no shutdown
   Switch1(config-if)# exit
   ```

   Важно: Убедитесь, что в сети настроен шлюз (если требуется) и что свитч имеет доступ для управления.

Шаг 2. Настройка VLAN

1. **Создание VLAN:**

```plaintext
Switch1(config)# vlan 10
Switch1(config-vlan)# name HR
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name Finance
Switch1(config-vlan)# exit
```

2. **Назначение VLAN для портов (например, порт FastEthernet0/2 в VLAN 10 и FastEthernet0/3 в VLAN 20):**

```plaintext
Switch1(config)# interface fastEthernet 0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit

Switch1(config)# interface fastEthernet 0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# exit
```

Шаг 3. Настройка trunk-порта

1. **Настройка порта для передачи трафика нескольких VLAN (например, порт FastEthernet0/1):**

```
plaintext                                                    Копировать  Редактировать

Switch1(config)# interface fastEthernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk encapsulation dot1q
Switch1(config-if)# exit
```

Примечание: На некоторых моделях свитчей настройка encapsulation может отличаться или по умолчанию быть установлена.

Шаг 4. Настройка Spanning Tree Protocol (STP)

1. **Проверка состояния STP:**

   Введите команду:

```
plaintext                                                    Копировать  Редактировать

Switch1# show spanning-tree
```

Цель: Определить корневой мост, проверить, какие порты находятся в состоянии блокировки, прослушивания и передачи. При необходимости можно настроить приоритет для выбора корневого моста:

```
plaintext                                                    Копировать  Редактировать

Switch1(config)# spanning-tree vlan 10 priority 24576
```

Шаг 5. Настройка безопасности портов (Port Security)

1. **Настройка Port Security на одном из access-портов (например, FastEthernet0/4):**

```plaintext
Switch1(config)# interface fastEthernet 0/4
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport port-security
Switch1(config-if)# switchport port-security maximum 2
Switch1(config-if)# switchport port-security violation shutdown
Switch1(config-if)# switchport port-security mac-address sticky
Switch1(config-if)# exit
```

Описание настроек:

- **maximum 2:** ограничивает число разрешённых MAC-адресов до двух.
- **violation shutdown:** в случае нарушения (появления третьего неизвестного MAC-адреса) порт будет переведён в состояние shutdown.
- **sticky:** автоматически сохраняет адреса подключенных устройств в конфигурации.

3.3. Диагностика и проверка настроек

1. **Просмотр настроек VLAN и назначения портов:**

```
plaintext                                                    Копировать

Switch1# show vlan brief
```

2. **Проверка статуса trunk-портов:**

```
plaintext                                                    Копировать

Switch1# show interfaces trunk
```

3. **Проверка состояния STP:**

```
plaintext                                                    Копировать

Switch1# show spanning-tree detail
```

4. **Диагностика безопасности портов:**

```
plaintext                                                    Копировать

Switch1# show port-security interface fastEthernet 0/4
```

5. **Тестирование подключения:**

   Подключите конечные устройства к портам, настроенным в разных VLAN, и проверьте, что устройства внутри одного VLAN могут обмениваться данными, а между разными VLAN – нет (если не настроен меж VLAN routing). При необходимости настройте меж VLAN маршрутизацию через маршрутизатор или Layer 3 свитч.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 14

«Настройка параметров безопасности»

Цель: Изучение настройки параметров безопасности.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

Компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. *Основные опасности при работе в сети Интернет* с помощью браузера следующие:

- переносимые программы (ActiveX и Java-апплеты) внедренные в web_страницу;
- языки сценариев (JavaScript и VBScript), которые призваны превратить статичное содержимое HTML-страницы в динамическое.
- cookie, сохраняемые браузером могут позволить заинтересованным лицам следить за Вашими действиями в сети и знать о Ваших интересах.

Современные веб-страницы часто содержат небольшие программы: *Java-апплеты*, управляющие элементы *ActiveX*, скрипты *JavaScript*. Загрузка и выполнение таких переносимых программ, очевидно, связаны с большим риском возникновения массовых атак. Разработаны различные методы, направленные на минимизацию этого риска.

Java-апплеты – это программы на языке Java, откомпилированные в машинный язык, которые размещаются на веб-странице и загружаются вместе с ней. Апплеты обрабатываются интерпретатором **JVM (*Java Virtual Machine*** — виртуальная машина Java) в браузере, как показано на рисунке 1.

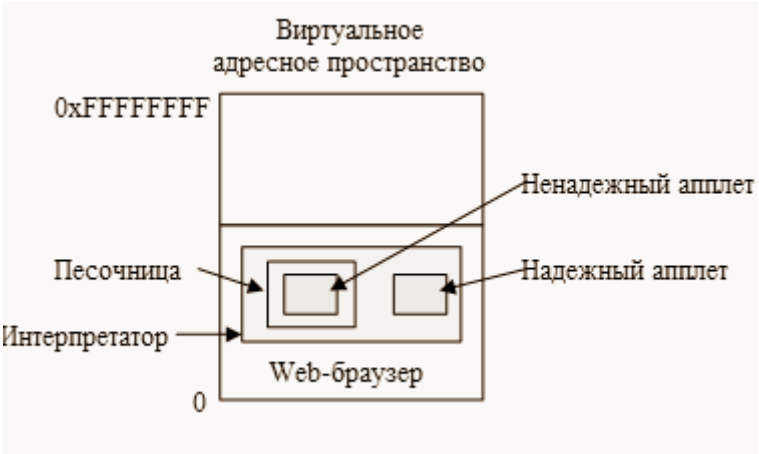


Рисунок 1. Обработка апплетов браузером

Преимущество интерпретируемого кода перед компилируемым состоит в том, что перед его исполнением изучается каждая инструкция. Это дает интерпретатору возможность проверить состоятельность адреса инструкции. Кроме того, системные вызовы также перехватываются и интерпретируются. Как именно они обрабатываются, зависит от политики защиты информации.

- если апплет *надежный* (например, он был создан на локальном диске), его системные вызовы могут обрабатываться без дополнительных проверок;
- если апплет *не может считаться надежным* (например, он был загружен из Интернета), его можно поместить в так называемую песочницу, регулирующую его поведение и пресекающую его попытки использовать системные ресурсы;
- если апплет *пытается захватить системный ресурс*, вызов передается монитору безопасности, который может разрешить или запретить данное действие. Монитор исследует вызов с точки зрения локальной политики защиты информации и затем принимает решение.

Таким образом, можно предоставить апплетам доступ к некоторым (но не ко всем) ресурсам.

Управляющие элементы ActiveX — двоичные программы, которые можно внедрять в веб-страницы. Когда на странице встречается такая программа, производится проверка необходимости ее выполнения, и в случае положительного ответа она запускается. Эти программы не интерпретируются и не помещаются в песочницы, поэтому они обладают такими же возможностями, как обычные пользовательские программы, и, в принципе, могут нанести большой вред. Таким образом, вся защита информации в данном случае сводится к вопросу о том, стоит ли запускать управляющий элемент.

Для принятия таких решений корпорацией Microsoft был выбран метод, базирующийся на подписях кода (*система Authenticode*). Суть в том, что каждый элемент *ActiveX* снабжается цифровой подписью, а именно *хэшем кода*, подписанным его создателем с использованием открытого ключа. Когда браузер встречает управляющий элемент, он сначала проверяет правильность подписи, убеждаясь в том, что код не был заменен по дороге. Если подпись корректна, браузер проверяет по своим внутренним таблицам, можно ли доверять создателю программы. Если создатель надежный, программа выполняется, в противном случае игнорируется. Поскольку нет никакой возможности проследить за деятельностью всех компаний, пишущих переносимые программы, вскоре метод подписания кода может представлять собой довольно серьезную угрозу.

В *JavaScript* вообще отсутствует какая-либо официальная модель системы защиты информации. Каждый производитель пытается что-нибудь придумать. Например, в ***Netscape Navigator 2.0*** было реализовано нечто подобное Java-модели, а в четвертой версии прослеживаются черты модели подписей кода.

В обозревателе ***Internet Explorer*** имеется несколько возможностей, позволяющих обеспечить защиту конфиденциальности, а также повысить безопасность личных данных пользователя.

Параметры конфиденциальности позволяют защитить личные данные пользователя – с помощью этих параметров можно понять, как просматриваемые web-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли web-узлам сохранять файлы *cookie* на компьютере.

К *параметрам конфиденциальности* ***Internet Explorer*** относят следующие:

- *параметры конфиденциальности*, определяющие обработку на компьютере файлов cookie.

- *оповещения безопасности*, выдаваемые пользователю при попытке получить доступ к web-узлу, не соответствующему заданным параметрам конфиденциальности;
- *возможность просмотра политики конфиденциальности* стандарта P3P (***Platform for Privacy Preferences***) для web-узла.

Средства безопасности позволяют предотвратить доступ других пользователей к таким сведениям, на доступ к которым у них нет разрешения. Это, например, сведения о кредитной карточке, вводимые при покупках в Интернете, от небезопасного программного обеспечения.

Когда производится загрузка или запуск программ, полученных из Интернета, необходимо убедиться, что программа получена из известного, надежного источника. В связи с этим, при выполнении загрузки на компьютер программы из Интернета, обозреватель ***Internet Explorer*** использует для проверки ее подлинности технологию ***Microsoft Authenticode***, проверяющую наличие у программы действующего сертификата. Следует отметить, что эта мера не препятствует загрузке и запуску на компьютере программ, разработанных с ошибками, но снижает риск использования фальсифицированной программы.

Цифровая подпись — это способ введения электронной метки для файла данных. В этом случае файл подписывается его создателем (издателем). Наличие цифровой подписи позволяет сделать следующие выводы: имеется имя издателя файла, и этот файл не был изменен с тех пор, как он был подписан. При любой попытке фальсификации подпись становится недействительной.

Виды цифровых подписей:

- подписи с симметричным ключом;
- подписи с открытым ключом.

В *первом случае* суть метода состоит в создании некоего центрального авторитетного органа, которому все доверяют. Затем каждый пользователь выбирает секретный ключ и лично относит его в офис этого авторитетного органа. Когда возникает необходимость послать открытым текстом подписанное сообщение, оно (сообщение) шифруется ключом. Затем сообщение посылается в авторитетный орган, который расшифровывает его и посылает получателю со своей собственной подписью. Этим авторитетный орган подтверждает, что сообщение подлинное.

Во *втором случае* ключ делится на две части: закрытая и открытая части. С помощью закрытой части можно подписать данные, причем это может сделать только владелец ключа, а с помощью открытой части можно проверить подпись.

Сертификат – цифровой документ, широко используемый для проверки подлинности и безопасного обмена данными в открытых сетях, таких как Интернет, экстрасети и интрасети. Сертификат связывает открытый ключ с объектом, хранящим соответствующий закрытый ключ. Сертификаты имеют цифровые подписи, поставленные выдавшими центрами сертификации, и могут предоставляться пользователю, компьютеру или службе. Наиболее широко применяемый формат для цифровых сертификатов определяется международным стандартом ITU-T X.509 версии 3.

Задание Настройте параметры безопасности браузера Internet Explorer:

1. Откройте диалоговое окно **Свойства: Интернет (*Пуск/Панель управления/Свойства обозревателя*)**;
2. Перейдите на вкладку **Безопасность** и откройте параметры зоны Интернет с помощью кнопки ***Другой…***;
3. Установите ***Проверку имени пользователя*** в режим **Запрос имени пользователя и пароля**;
4. Разрешите в соответствующих полях указанные ниже действия:
    - Блокировать всплывающие окна;
    - Доступ к источникам данных за пределами домена;
    - Переход между кадрами через разные домены;
5. Установите **Разрешения канала программного обеспечения** на *Высокий уровень безопасности*;
6. Отключите *Использование элементов ActiveX не помеченных как безопасные*;
7. Отключите загрузку *Неподписанных элементов ActiveX*;
8. Примените параметры кнопкой ***OK***;
9. Установите параметры конфиденциальности:
    - перейдите на вкладку **Конфиденциальность**;
    - установите регулятор на уровень *Умеренно высокий*;
    - разрешите загружать файлы ***cookie*** с узла **www.mail.ru**:
        - щелкните по кнопке ***Узлы***;
        - введите в поле *www.mail.ru* и щелкните по кнопке ***Разрешить***;
    - аналогично разрешите загружать cookie со следующих узлов: **www.yandex.ru, www.pochta.ru**;
    - примените параметры кнопкой ***OK***;
10. Настройте ограничения на доступ к ресурсам по содержанию информации на них:
    - перейдите на вкладку **Содержание** и откройте окно **Ограничение доступа** кнопкой ***Включить*** в разделе **Ограничения доступа**;
    - установите пароль:
        - перейдите на вкладку **Общие**;
        - откройте окно создания пароля кнопкой ***Создать пароль***;
        - введите **пароль** - *user* и **подсказку** к нему - *user*;
        - примените параметры кнопкой ***OK***.
    - перейдите на вкладку **Оценки** и установите уровни **Службы оценки Recreational Software Advisory Council** по своему усмотрению;
    - примените параметры кнопкой ***OK***;
    - очистите пароли, которые браузер автоматически запоминает. Для этого на вкладке **Содержание**, щелкните по кнопке ***Автозаполнение***, а затем по кнопке ***Очистить пароли***;
    - удалите временные фалы Интернет и ***cookies*** на вкладке **Общие**.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 15

«Работа с RADIUS сервером»

Цель: Изучение принципов работы RADIUS: понять роль протокола RADIUS (Remote Authentication Dial-In User Service) в процессе аутентификации, авторизации и учета (AAA) пользователей. Освоение установки и базовой настройки RADIUS сервера: научиться устанавливать RADIUS сервер (на примере FreeRADIUS), настраивать клиентов и пользователей, а также проверять корректность работы сервера. Получение навыков интеграции RADIUS: научиться связывать RADIUS сервер с сетевыми устройствами (например, NAS, VPN-серверами, точками доступа) для централизованного контроля доступа. Развитие навыков диагностики и устранения ошибок: освоить инструменты тестирования (radtest) и анализ логов для выявления и решения проблем при аутентификации.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

2.1. Основы RADIUS

- **Что такое RADIUS:**
  RADIUS (Remote Authentication Dial-In User Service) – это протокол, обеспечивающий централизованную аутентификацию, авторизацию и учет доступа пользователей к сетевым ресурсам. Он широко используется для организации контроля доступа в VPN, беспроводных сетях, а также в корпоративных системах.
- **Основные функции:**
  - **Аутентификация:** проверка подлинности пользователя (например, с помощью логина/пароля, сертификатов и др.).
  - **Авторизация:** определение прав доступа для аутентифицированного пользователя.
  - **Учет (Accounting):** сбор и хранение информации о сессиях (время подключения, объем переданных данных и пр.), что полезно для аналитики и отчетности.

- **Архитектура RADIUS:**
  - **RADIUS сервер:** обрабатывает запросы на аутентификацию и учет, принимает решения (Access-Accept, Access-Reject, Access-Challenge) и отправляет ответы клиентским устройствам.
  - **RADIUS клиент:** устройство (например, маршрутизатор, точка доступа, VPN-концентратор), которое пересылает запросы пользователей на сервер.
  - **База данных пользователей:** может находиться локально (в конфигурационных файлах) или использовать внешние источники (LDAP, Active Directory, MySQL).
- **Порты и безопасность:**
  RADIUS использует UDP:
  - Порт **1812** для аутентификации.
  - Порт **1813** для учета.
    Для защиты передаваемой информации между клиентом и сервером применяется общий секрет (shared secret).

2.2. Принципы работы RADIUS

- **Процесс аутентификации:**
  1. Клиент (например, NAS) получает запрос на доступ от пользователя.
  2. Клиент отправляет запрос на аутентификацию (с набором атрибутов, таких как имя пользователя, пароль, идентификатор сессии) на RADIUS сервер.
  3. RADIUS сервер проверяет предоставленные данные (сравнивая их с локальными записями или обращаясь к внешнему источнику) и выдает ответ:
     - **Access-Accept:** если аутентификация прошла успешно.
     - **Access-Reject:** если аутентификация не удалась.
     - **Access-Challenge:** если требуется дополнительная проверка (реже используется).
- **Учёт сессии (Accounting):**
  При установлении и завершении сессии RADIUS сервер фиксирует данные (например, время начала и окончания, объем переданных данных) для последующего анализа.

Задание:

3.1. Подготовка рабочего окружения

- **Оборудование и программное обеспечение:**
  - Сервер или виртуальная машина под управлением Linux (например, Ubuntu, CentOS).
  - Пакет FreeRADIUS (версия 3.0 или выше).
  - Терминальный эмулятор (например, PuTTY или встроенный терминал Linux).
  - Клиент для тестирования (можно использовать утилиту `radtest`).

3.2. Установка FreeRADIUS (на примере Ubuntu)

1. **Обновление системы и установка:**

   bash Копировать Редактировать

   ```
   sudo apt update
   sudo apt install freeradius freeradius-utils
   ```

2. **Проверка статуса сервиса:**

   bash Копировать Редактировать

   ```
   sudo systemctl status freeradius
   ```

   Убедитесь, что сервис запущен и работает без ошибок.

3.3. Настройка FreeRADIUS

3.3.1. Конфигурация RADIUS клиентов

1. **Редактирование файла клиентов:**

   Откройте файл `/etc/freeradius/3.0/clients.conf`:

   ```bash
   sudo nano /etc/freeradius/3.0/clients.conf
   ```

2. **Добавление клиента:**

   Пример записи для клиента с IP-адресом `192.168.1.100`:

   ```conf
   client myclient {
       ipaddr = 192.168.1.100
       secret = testing123
       shortname = myclient
       nastype = other
   }
   ```

   Примечание: Убедитесь, что IP-адрес и общий секрет соответствуют настройкам вашего сетевого устройства, которое будет обращаться к RADIUS серверу.

3.3.2. Конфигурация пользователей

1. **Редактирование файла пользователей:**

   Откройте файл `/etc/freeradius/3.0/users`:

   ```bash
   sudo nano /etc/freeradius/3.0/users
   ```

2. **Добавление тестового пользователя:**

   Добавьте следующую запись:

   ```conf
   testuser Cleartext-Password := "password123"
       Reply-Message = "Добро пожаловать, testuser!"
   ```

   Здесь:

   - **testuser** — имя пользователя.
   - **password123** — его пароль.
   - **Reply-Message** — сообщение, отправляемое клиенту после успешной аутентификации.

3.3.3. Применение настроек

- **Перезапуск сервиса:**

  После внесения изменений перезапустите FreeRADIUS:

  ```bash
  sudo systemctl restart freeradius
  ```

3.4. Тестирование работы RADIUS сервера

3.4.1. Тестирование аутентификации

1. **Использование утилиты radtest:**

   Выполните команду (на сервере или с клиентской машины, если установлены необходимые утилиты):

   ```bash
   radtest testuser password123 127.0.0.1 0 testing123
   ```

   Где:

   - `testuser` — имя пользователя.
   - `password123` — пароль.
   - `127.0.0.1` — IP-адрес RADIUS сервера (если тестирование производится на локальной машине).
   - `0` — значение NAS-Port.
   - `testing123` — общий секрет (должен совпадать с настройками в clients.conf).

2. **Анализ результата:**

   При успешной аутентификации вы получите ответ с кодом `Access-Accept` и указанным Reply-Message. В случае ошибки отобразится сообщение об отказе (Access-Reject).

3.4.2. Просмотр логов и диагностика

- **Мониторинг логов:**

  Для анализа работы сервера можно просматривать журнальные файлы:

  ```bash
  sudo tail -f /var/log/freeradius/radius.log
  ```

  Логи помогут выявить ошибки в конфигурации или неправильные учетные данные.

3.5. Дополнительные задания

1. **Настройка RADIUS Accounting:**
   - Изучите файл `/etc/freeradius/3.0/sites-available/default` в секции `accounting { ... }`.
   - Настройте параметры учета сессий, чтобы сервер записывал данные о подключениях в журнал (можно направить записи в файл или на внешний сервер).
2. **Интеграция с сетевым устройством:**
   - Настройте сетевое устройство (например, маршрутизатор, точку доступа) для использования вашего RADIUS сервера. Введите IP-адрес сервера, порт 1812 и общий секрет.
   - Проведите тестовую аутентификацию через устройство и проверьте корректность передачи запросов на сервер.
3. **Расширенная настройка:**
   - Попробуйте интегрировать FreeRADIUS с внешней базой данных (например, MySQL или LDAP) для хранения учетных данных.
   - Изучите возможности создания дополнительных политик авторизации с использованием модулей FreeRADIUS.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 16

«Работа с биллингом»

Цель: Изучение основ биллинга: Понять, что представляет собой биллинговая система, её роль в автоматизации учета услуг и финансовых операций, а также основные задачи, решаемые с её помощью.Ознакомление с этапами обработки данных: Изучить процесс сбора, обработки и тарификации данных (например, Call Detail Record – CDR в телекоммуникациях) для расчёта стоимости услуг. Освоение методов интеграции: Научиться настраивать связь биллинговой системы с источниками данных (телефонными системами, сетевыми устройствами, базами данных) и внешними системами (CRM, ERP, системы отчетности). Получение практических навыков настройки и тестирования: Настроить тарифные планы, реализовать алгоритмы тарификации, произвести расчет стоимости оказанных услуг и сформировать отчеты по итогам работы системы.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

2.1. Понятие и роль биллинга

- **Что такое биллинг:**
  Биллинг – это совокупность процессов по учёту, расчёту и выставлению счетов за оказанные услуги. Он обеспечивает автоматизацию финансовых операций, контроль затрат и аналитическую отчетность.
- **Функции биллинговой системы:**
  - **Сбор данных:** Получение информации о сессиях или операциях (например, звонках, интернет-трафике, использовании сервисов).
  - **Тарификация:** Применение алгоритмов расчёта стоимости услуг в зависимости от заданных тарифных планов (по минутам, по объёму, по времени суток, по зонам и т.д.).
  - **Учет и выставление счетов:** Формирование счетов для пользователей, сбор статистических данных для последующего анализа.
  - **Отчетность и контроль:** Генерация отчетов, мониторинг использования услуг, анализ доходности и выявление аномалий.

2.2. Основные компоненты биллинговой системы

- **Источник данных (CDR, логи, события):**
  Информация, которая поступает из сетевых устройств или программных систем (например, данные о звонках, интернет-сессиях или иных операциях).
- **Модуль тарификации:**
  Содержит алгоритмы расчета стоимости, основанные на тарифных планах, скидках, наценках и дополнительных услугах. Может включать поддержку различных моделей тарификации (фиксированная плата, плата за использование, гибридные схемы).
- **База данных:**
  Хранение информации о пользователях, тарифах, операциях и финансовых операциях. Часто используется SQL-сервер или специализированное хранилище данных.
- **Интерфейсы интеграции:**
  API, коннекторы, файлопередачи или web-сервисы для обмена данными между биллинговой системой и внешними источниками или потребителями информации (CRM, ERP, системы мониторинга).

2.3. Алгоритмы тарификации и отчетность

- **Алгоритмы расчёта:**
  Обеспечивают корректное вычисление стоимости услуги на основании:
  - Продолжительности использования (например, длительность телефонного разговора).
  - Объёма переданных данных или количества операций.
  - Временных интервалов (пиковые/непиковые часы, выходные дни).
  - Дополнительных параметров (например, географическое положение, тип соединения).
- **Отчетность:**
  Формирование детальных отчетов по:
  - Использованию услуг.
  - Финансовым результатам.
  - Анализу эффективности тарифных планов и выявлению тенденций в поведении пользователей.

Задание:

3.1. Подготовка рабочего окружения

- **Оборудование и ПО:**
  - Сервер или виртуальная машина под управлением Linux/Windows.
  - База данных (например, MySQL, PostgreSQL или MS SQL).
  - Программное обеспечение для обработки CDR или биллинговая платформа (например, open-source решения, специализированные скрипты или ERP-модули, в зависимости от сферы применения).
  - Инструменты для генерации тестовых данных (скрипты на Python, Bash или готовые эмуляторы CDR).
- **Исходные данные:**
  Набор тестовых данных, представляющих операции (например, звонки, интернет-сессии или транзакции), с которыми будет работать биллинговая система.

3.2. Этапы практической работы

Шаг 1. Сбор и подготовка данных

1. **Имитация поступления CDR/логов:**

   Создайте или получите файл с тестовыми записями, содержащими поля:

   - Идентификатор пользователя/абонента.
   - Время начала и окончания операции.
   - Тип услуги.
   - Дополнительные параметры (например, географическое положение, номер вызываемого абонента).

2. **Импорт данных в базу:**

   Разработайте скрипт или воспользуйтесь готовым ETL-инструментом для загрузки данных в таблицу базы данных. Например, в MySQL:

   sql Копировать Редактировать

   ```sql
   CREATE TABLE cdr (
       id INT AUTO_INCREMENT PRIMARY KEY,
       user_id VARCHAR(50),
       start_time DATETIME,
       end_time DATETIME,
       service_type VARCHAR(50),
       additional_info VARCHAR(255)
   );
   ```

   Импортируйте данные с помощью утилиты `LOAD DATA INFILE` или SQL-скрипта.

Шаг 2. Настройка тарифных планов и алгоритмов тарификации

1. **Создание таблицы тарифов:**

   Определите тарифные планы для различных услуг:

```sql
CREATE TABLE tariffs (
    id INT AUTO_INCREMENT PRIMARY KEY,
    service_type VARCHAR(50),
    rate DECIMAL(10,2),
    unit VARCHAR(10)  -- например, минута, мегабайт и т.д.
);
```

   Заполните таблицу тестовыми данными:

```sql
INSERT INTO tariffs (service_type, rate, unit)
VALUES ('voice', 0.10, 'minute'), ('data', 0.05, 'MB');
```

2. **Реализация алгоритма тарификации:**

   Напишите SQL-запрос или скрипт (на Python, PHP, JavaScript и т.д.) для расчета стоимости операции. Пример на SQL для голосовых вызовов:

```sql
SELECT c.user_id,
       TIMESTAMPDIFF(MINUTE, c.start_time, c.end_time) AS duration,
       t.rate,
       TIMESTAMPDIFF(MINUTE, c.start_time, c.end_time) * t.rate AS cost
FROM cdr c
JOIN tariffs t ON c.service_type = t.service_type
WHERE c.service_type = 'voice';
```

   Аналогичным образом можно реализовать расчет для других типов услуг.

Шаг 3. Выставление счетов и генерация отчетности

1. **Формирование счетов:**

   На основе рассчитанных данных создайте таблицу счетов:

```sql
CREATE TABLE invoices (
    invoice_id INT AUTO_INCREMENT PRIMARY KEY,
    user_id VARCHAR(50),
    billing_period VARCHAR(20),
    total_cost DECIMAL(10,2),
    generated_at DATETIME DEFAULT CURRENT_TIMESTAMP
);
```

   Разработайте скрипт, который суммирует стоимость всех операций за определённый период для каждого пользователя и сохраняет итоговую сумму в таблице счетов.

2. **Генерация отчетов:**

   Подготовьте SQL-запросы для формирования отчетов, например:

   - Отчет по доходам за месяц:

```sql
SELECT billing_period, SUM(total_cost) AS monthly_income
FROM invoices
GROUP BY billing_period;
```

   - Детальный отчет по операциям для конкретного абонента:

```sql
SELECT c.*, (TIMESTAMPDIFF(MINUTE, c.start_time, c.end_time) * t.rate) AS cost
FROM cdr c
JOIN tariffs t ON c.service_type = t.service_type
WHERE c.user_id = 'user123'
ORDER BY c.start_time;
```

Шаг 4. Тестирование и диагностика

1. **Проверка корректности расчётов:**
   Сравните результаты тарификации с ожидаемыми значениями, протестируйте различные сценарии (разные тарифы, типы услуг, периоды использования).
2. **Анализ логов и ошибок:**
   Организуйте журналирование (логирование) операций, чтобы отслеживать ошибки импорта данных, расчётов и формирования счетов. Это можно реализовать как средствами базы данных (триггеры, процедуры) так и с помощью внешних скриптов.
3. **Интеграция с внешними системами:**
   При наличии настройте обмен данными с другими системами (например, отправку счетов по email, интеграция с CRM), используя API или файловый обмен.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 17

«Работа с SIP-абонентами»

Цель: получение базовых навыков работы конфигурации элементов IP-сети (Ethernet коммутатор второго уровня, прикладной процесс Asterisk операционной системой семейства Linux и софтфон 3CX Phone), конфигурации шлюза VoIP, необходимые для взаимодействия с традиционной телефонной сетью.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

Ознакомление с элементами IP-сети (коммутатором второго уровня, шлюзом, программным телефоном 3CX Phone и прикладным процессом Asterisk) и с особенностями и возможностями операционной системы Linux (идеология файловой системы, структура каталогов, основные дистрибутивы, основные команды по конфигурированию и настройке сервисов).

5.3.1 Прикладной процесс Asterisk – это программная АТС, способная коммутировать как VoIP вызовы, так и вызовы, осуществляемые между IP-телефонами и традиционной телефонной сетью общего пользования. Количество абонентов в сети может достигать 2000 и ограничено только мощностью сервера.

Asterisk поддерживает следующие протоколы:

- IAX;
- SIP;
- H.323;
- Skinny;
- UNIStim.

Программное обеспечение Asterisk поддерживает следующие кодеки:

- G.711 (ulaw и alaw);
- G.722;
- G.723;
- G.729;
- GSM;
- iLBC;
- LPC-10;
- Speex.

В основу принципов построения универсального шлюза VRX-1010-E1 положены гибкость и масштабируемость как программных, так и аппаратных средств.

VoIP-шлюз VRX-1010-E1 подключается к аналоговым и цифровым офисным АТС практически любых производителей (Panasonic, LG, Samsung, Siemens и др.).

Универсальный VoIP VRX-1010-E1 шлюз реализован в виде законченного конструктива. Контроллер шлюза выполнен на основе мощного однокристального телекоммуникационного процессора и, по сути, представляет собой промышленный компьютер, функционирующий под управлением встроенной операционной системы Linux.

Программа управления шлюзом реализован как сервис (демоны) операционной системы Linux, что позволяет программе управления системой функционировать как на отдельно устанавливаемом специализированном сервере, так и непосредственно на плате универсального шлюза.

Между собой программы управления шлюзом и программа управления системой взаимодействуют через стек протоколов TCP-IP, что позволяет строить распределенные

системы любой степени сложности. Поддерживает следующие основные протоколы управления/сигнализации:
- поддержка протоколов SIP и H.323;
- расширенные функции QoS;
- функции безопасности (авторизация пользователей, списки доступа);
- прием/передача факсов (FAX over IP);
- конфигурирование через web-интерфейс.

Универсальный шлюз VRX-1010-E1 – модульное цифровое устройство, которое обладает мощным специализированным процессором для трансляции 2х мегабитных потоков E1 от АТС (УАТС) до SIP сервера (SIP АТС.

Универсальный VoIP шлюз позволит объединить в единое целое среды передачи для сетей передачи данных и традиционной телефонной сети.

5.3.2 Осуществите соединение сетевых устройств в соответствии схемы, представленной на рисунке 5.1.

5.3.3 Пропишите на ПК IP-адрес и маску в соответствии с вариантом (таблица 1.1). В качестве шлюза по умолчанию установите IP-адрес шлюза VRX-1010-E1.

5.3.4 Подключитесь к консоли шлюза VRX-1010-E1 через SSH-клиент

5.3.5 Приведите содержимое файла /etc/asterisk/asterisk.conf к следующему виду (рисунок 5.2):

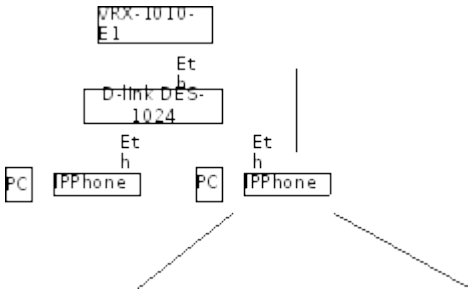


Рисунок 5.1 – Схема сети

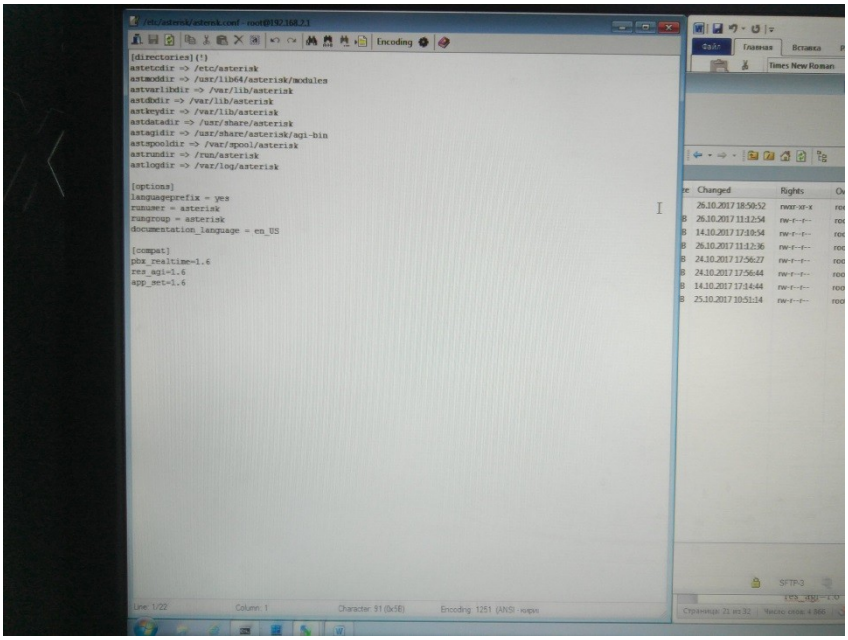


Рисунок 5.2 – Файл /etc/asterisk/asterisk.conf

5.3.6 Приведите содержимое файла /etc/asterisk/sip.conf к следующему виду (рисунок 5.3):

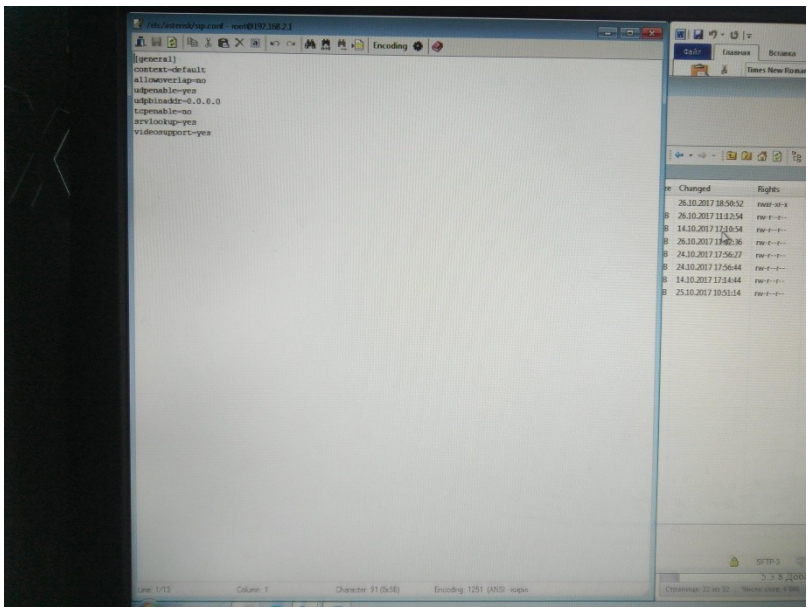


Рисунок 5.3 – Файл /etc/asterisk/sip.conf

5.3.7 Приведите содержимое файла /etc/asterisk/extensions.conf к следующему виду (рисунок 5.4):

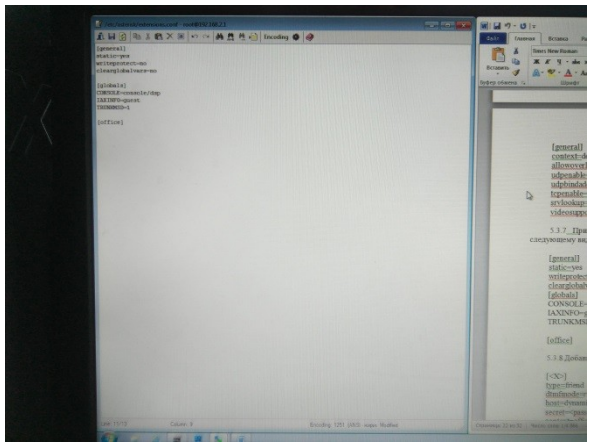


Рисунок 5.4 – Файла /etc/asterisk/extensions.conf

5.3.8 Добавьте в файл /etc/asterisk/sip.conf следующие строки (рисунок 5.5):

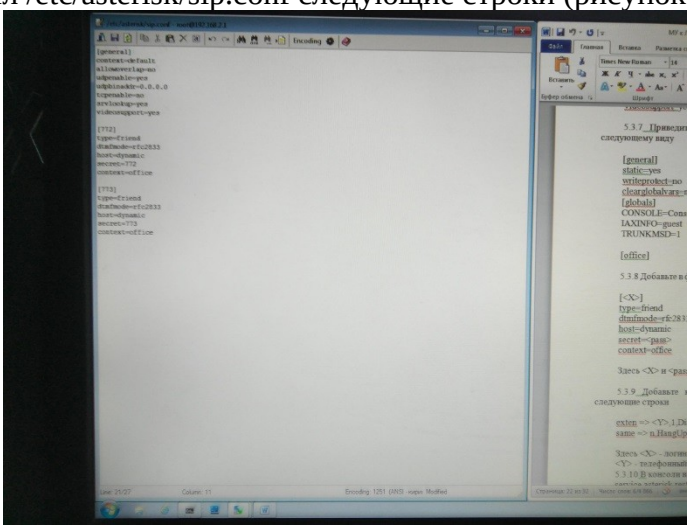


Рисунок 5.5 – Файл /etc/asterisk/sip.conf

Здесь [772]; [773] и secret=772; 773 - логин и пароль в соответственно.

5.3.9 Добавьте к содержимому файла /etc/asterisk/extensions.conf следующие строки (рисунок 5.6):

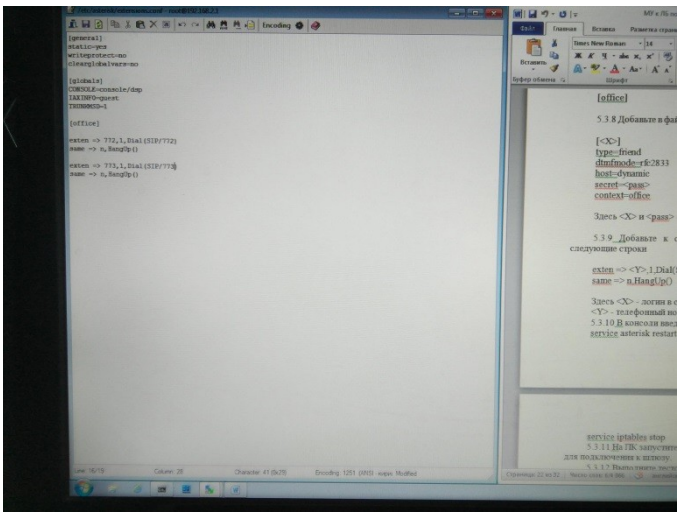


Рисунок 5.6 – Файл /etc/asterisk/extensions.conf

Здесь (SIP/772; 773)- логин

exten => 772; 773 - телефонный номер студента.

5.3.10. Запустите Putty и в консоли введите следующие команды (рисунок 5.7)

service asterisk restart

service iptables stop

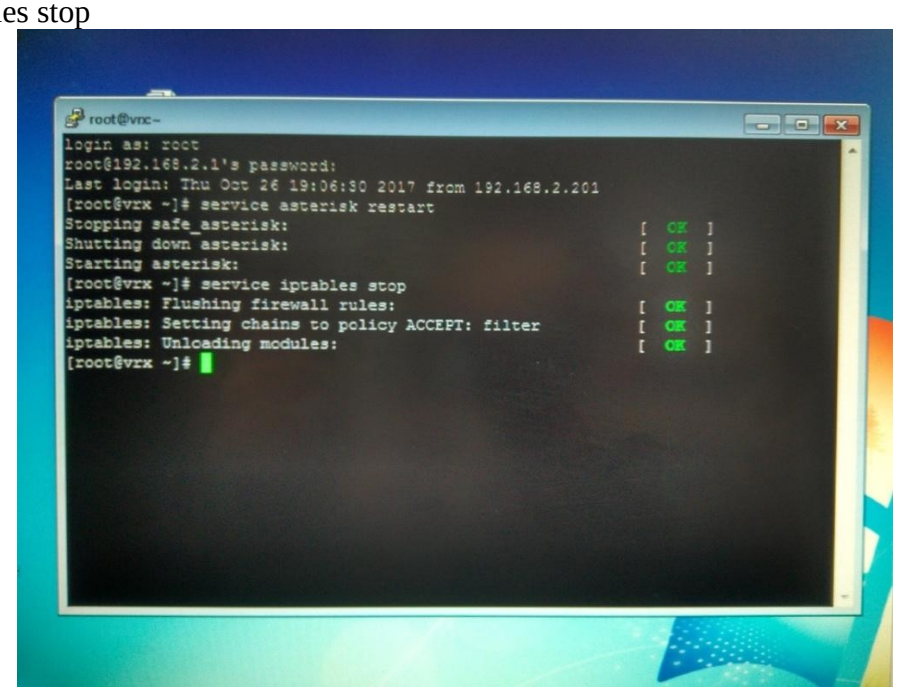


Рисунок 5.7 – Putty

5.3.11 На ПК запустите программу 3CX Phone и выполните её настройку для подключения к шлюзу (рисунок 5.8).

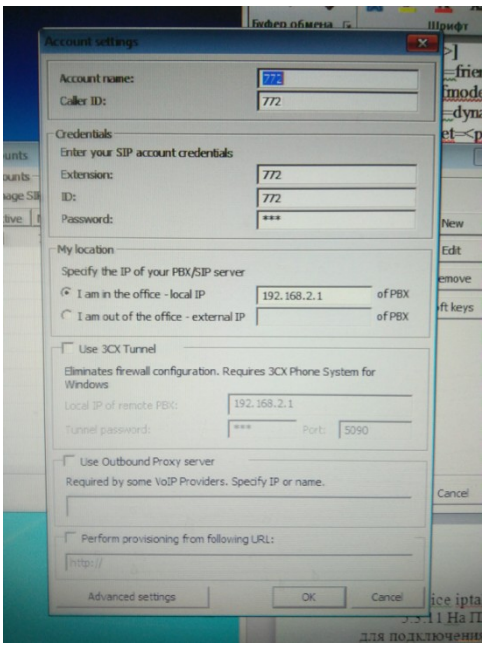


Рисунок 5.8 – 3CX Phone Account settings

5.3.12 Выполните тестовые вызовы между ПК (рисунок 5.9).

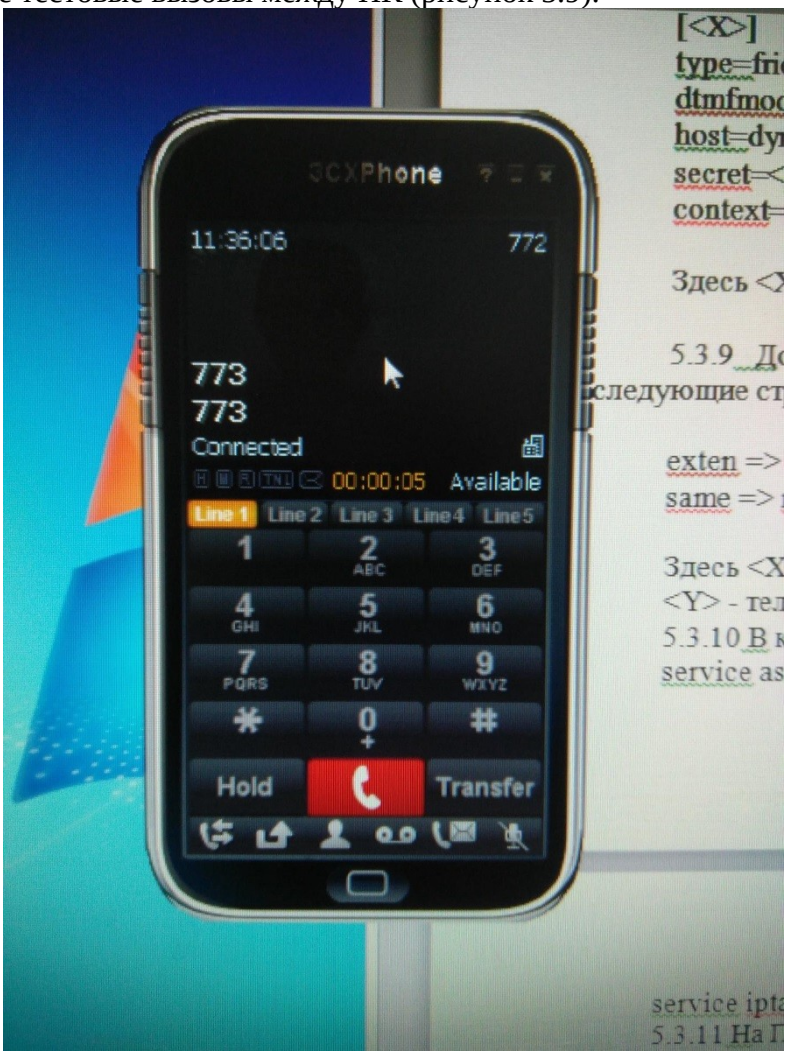


Рисунок 5.9 – Окно вызова 3CX Phone

Задание:

1 Соберите схему с использованием шлюза VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом 3CX Phone.
2 Присвоить ПК IP-адрес и маску подсети.
3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
4 Ознакомиться с выполнением различных процедур и команд.
5 Подключить мультимедийные приставки в ПК.
6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу. Осуществите тестовые звонки между ПК.
7 Составьте отчет о результатах выполнения работы.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 18

«Управление шлюзом»

Цель: Изучить роль и функциональность шлюза: Ознакомиться с концепцией шлюза как устройства, обеспечивающего связь между различными сетями или протоколами (например, между PSTN и VoIP, между локальной сетью и интернетом). Овладеть навыками базовой и расширенной настройки шлюза: Научиться проводить конфигурацию управляющего интерфейса, настройку маршрутизации, правил трансляции адресов (NAT), а также параметров безопасности. Освоить методы мониторинга и диагностики работы шлюза: Изучить инструменты для проверки состояния шлюза, анализировать логи, работать с диагностическими командами (например, проверка таблицы маршрутизации, просмотр статистики трафика, отладка SIP-сообщений для VoIP-шлюза). Получить практические навыки управления шлюзом: На примере выбранного устройства настроить базовые параметры, протестировать корректность работы, произвести настройку резервирования и определить потенциальные проблемы.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

2.1. Понятие шлюза и его задачи

- **Что такое шлюз:**
  Шлюз – это устройство, которое соединяет два или более различных сетевых сегментов, часто работающих на разных протоколах или стандартах. В телекоммуникациях шлюзы обеспечивают преобразование сигналов между традиционными телефонными сетями (PSTN) и IP-сетями (VoIP), а в компьютерных сетях – могут выполнять функции маршрутизатора, межсетевого экрана или VPN-концентратора.
- **Основные функции шлюза:**
  - **Маршрутизация трафика:** Определение оптимальных путей для передачи пакетов между сетями.
  - **Трансляция адресов (NAT):** Преобразование внутренних IP-адресов в публичные (и наоборот) для обеспечения доступа к ресурсам внешней сети.
  - **Преобразование протоколов:** Обеспечение взаимодействия между сетями, использующими различные протоколы (например, SIP-телефония и аналоговая телефония).
  - **Обеспечение безопасности:** Фильтрация трафика, контроль доступа и защита от внешних угроз.

2.2. Основные компоненты и архитектура шлюза

- **Управляющий интерфейс:**
  Интерфейс для доступа к настройкам устройства (консоль, веб-интерфейс, SSH/Telnet). Здесь администратор выполняет базовую и расширенную конфигурацию.
- **Модули обработки трафика:**
  Внутренние компоненты, обеспечивающие маршрутизацию, NAT, преобразование протоколов и обработку сигнализации (например, SIP-преобразование для VoIP-шлюза).
- **Логирование и мониторинг:**
  Механизмы, позволяющие регистрировать события, ошибки и статистику работы для последующего анализа и диагностики.

2.3. Основы управления и диагностики

- **Настройка через CLI и/или веб-интерфейс:**
  Большинство современных шлюзов поддерживают командную строку (CLI) для детальной настройки, а также графический веб-интерфейс для базового администрирования.
- **Диагностические команды и утилиты:**
  Использование команд для просмотра конфигурации (например, `show running-config`, `show ip route`, `show nat translations`), проверки логов и мониторинга состояния интерфейсов.
- **Механизмы резервирования и отказоустойчивости:**
  В некоторых случаях шлюзы поддерживают настройку резервных маршрутов, балансировку нагрузки и автоматическое переключение при отказе основного канала.

Задание:

3.1. Подготовка оборудования и рабочего окружения

- **Оборудование:**
  - Физический шлюз (например, специализированное устройство для VoIP или маршрутизатор с функциями NAT и VPN) или его эмуляция в виде виртуальной машины.
  - Компьютер для подключения по консоли (через USB/COM-порт) или через сетевой доступ (SSH/Telnet, веб-интерфейс).
- **Программное обеспечение:**
  - Терминальный эмулятор (PuTTY, SecureCRT, терминал Linux).
  - Браузер для доступа к веб-интерфейсу (если предусмотрено).
  - Дополнительные утилиты для диагностики сети (ping, traceroute, Wireshark для анализа трафика).

3.2. Этапы практической работы

Шаг 1. Начальная настройка и подключение к шлюзу

1. **Подключение к устройству:**
   Подключитесь к шлюзу через консоль или по сети. При необходимости используйте консольный кабель для первоначальной конфигурации.
2. **Первичная настройка:**
   - Задайте уникальное имя (hostname) устройства.
     Пример для CLI:

     plaintext Копировать Редактирова

     ```
     Gateway> enable
     Gateway# configure terminal
     Gateway(config)# hostname MyGateway
     ```

   - Настройте IP-адрес для управления (например, на интерфейсе управления или VLAN-интерфейсе):

     plaintext Копировать Редактирова

     ```
     MyGateway(config)# interface vlan 1
     MyGateway(config-if)# ip address 192.168.10.1 255.255.255.0
     MyGateway(config-if)# no shutdown
     MyGateway(config-if)# exit
     ```

Шаг 2. Настройка маршрутизации и NAT

1. **Настройка базовой маршрутизации:**

   Укажите маршруты для внутренних и внешних сетей. Например, настройка дефолтного маршрута:

   plaintext Копировать Редактир

   ```
   MyGateway(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.254
   ```

2. **Конфигурация NAT (если требуется):**

   Настройте трансляцию адресов для подключения внутренней сети к внешней.

   - Задайте внутренний интерфейс:

     plaintext Копировать Редактир

     ```
     MyGateway(config)# interface GigabitEthernet0/1
     MyGateway(config-if)# ip nat inside
     MyGateway(config-if)# exit
     ```

   - Задайте внешний интерфейс:

     plaintext Копировать Редактир

     ```
     MyGateway(config)# interface GigabitEthernet0/2
     MyGateway(config-if)# ip nat outside
     MyGateway(config-if)# exit
     ```

Создайте правило NAT:

plaintext Копировать Редактировать

```
MyGateway(config)# access-list 10 permit 192.168.10.0 0.0.0.255
MyGateway(config)# ip nat inside source list 10 interface GigabitEthernet0/2 overload
```

Шаг 3. Настройка специфических функций (например, VoIP-шлюза)

Если шлюз используется для преобразования между PSTN и VoIP:

1. **Настройка SIP параметров:**
   Задайте параметры регистрации SIP, IP-адреса для голосового трафика и преобразование сигналов.

```plaintext
MyGateway(config)# voice service voip
MyGateway(conf-voice)# ip address trusted 192.168.10.100 255.255.255.0
MyGateway(conf-voice)# registrar server timeout 10
MyGateway(conf-voice)# exit
```

2. **Настройка преобразования кодеков и маршрутизации звонков:**
   Определите правила для обработки входящих/исходящих вызовов, используя соответствующий синтаксис (зависит от модели устройства).

Шаг 4. Настройка безопасности и мониторинга

1. **Фильтрация трафика и контроль доступа:**
   Настройте ACL для ограничения доступа к шлюзу:

```plaintext
MyGateway(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 any
MyGateway(config)# access-list 101 deny ip any any
MyGateway(config)# interface vlan 1
MyGateway(config-if)# ip access-group 101 in
MyGateway(config-if)# exit
```

2. **Включение логирования и диагностики:**
   Настройте сбор логов и мониторинг состояния устройства.

```plaintext
MyGateway(config)# logging buffered informational
MyGateway(config)# logging host 192.168.10.5
```

   Просмотрите состояние устройства:

```plaintext
MyGateway# show ip route
MyGateway# show ip nat translations
MyGateway# show running-config
```

Шаг 5. Тестирование и диагностика работы шлюза

1. **Проверка маршрутизации и NAT:**
   - Используйте команду `ping` с шлюза к внешнему ресурсу.
   - Проверьте таблицу NAT:

     plaintext Копировать Редактировать

     ```
     MyGateway# show ip nat translations
     ```

2. **Тестирование SIP/VoIP (если применимо):**
   - Инициируйте тестовый звонок между устройствами в локальной сети и через шлюз.
   - Проанализируйте SIP-сообщения с помощью Wireshark, чтобы убедиться в корректном прохождении сигнализации.
3. **Анализ логов:**

   Просмотрите логи и отладочную информацию для выявления возможных ошибок или сбоев в работе шлюза.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 19

«CLI. Работа со шлюзом в терминальном режиме»

Цель: Овладение навыками работы с CLI: Научиться работать с сетевым оборудованием (шлюзом) через командную строку, используя терминальный режим. Освоение базовой и расширенной конфигурации шлюза: Получить практический опыт настройки базовых параметров (имя устройства, IP-адресация, маршрутизация, NAT) и управления шлюзом посредством CLI. Развитие навыков диагностики и мониторинга: Научиться использовать диагностические команды для проверки состояния шлюза, просмотра таблицы маршрутизации, NAT, а также анализа конфигурации.

Время выполнения: 4 часа.

Ход работы:

Теоретические сведения:

2.1. Понятие CLI и терминального режима

- **CLI (Command Line Interface):**
  CLI – это интерфейс командной строки, позволяющий администратору напрямую взаимодействовать с устройством посредством ввода текстовых команд. Работа в терминальном режиме обеспечивает быстрый и детальный контроль над настройками оборудования.
- **Режимы работы в CLI:**
  Современные сетевые устройства (например, маршрутизаторы и шлюзы) обычно работают в нескольких режимах:
  - **User Mode (пользовательский режим):** базовый режим, позволяющий выполнять ограниченный набор команд (обычно для просмотра информации).
  - **Privileged Mode (привилегированный режим):** режим, предоставляющий доступ к командам диагностики и управления (переход осуществляется командой `enable`).
  - **Configuration Mode (режим конфигурации):** режим для внесения изменений в рабочую конфигурацию устройства (вход через команду `configure terminal`).

2.2. Роль шлюза в сети

- **Функциональность шлюза:**
  Шлюз – это устройство, которое соединяет две или более сетевых сред, выполняет маршрутизацию трафика, трансляцию адресов (NAT), а также может осуществлять фильтрацию и преобразование протоколов (например, между VoIP и PSTN).
- **Преимущества работы через CLI:**
  Благодаря CLI администратор получает возможность детально настроить устройство, быстро изменить параметры и выполнить диагностику в режиме реального времени.

2.3. Основные команды и процедуры работы

- **Переход между режимами:**
  - Переход в привилегированный режим:

```shell
Router> enable
Router#
```

  - Переход в режим глобальной конфигурации:

```arduino
Router# configure terminal
Router(config)#
```

- **Основные команды настройки:**
  - **Hostname:** изменение имени устройства.
  - **Interface:** выбор и настройка конкретного сетевого интерфейса (IP-адрес, маска, команда `no shutdown` для активации).
  - **IP Route:** настройка статических маршрутов.
  - **NAT:** настройка трансляции адресов.
- **Диагностические команды:**
  - `show running-config` – просмотр текущей конфигурации.
  - `show ip route` – отображение таблицы маршрутизации.
  - `show ip nat translations` – просмотр активных записей NAT.
  - `ping` – проверка доступности узлов сети.

Задание:

3.1. Подготовка рабочего окружения

- **Оборудование:**
  Физический шлюз (например, маршрутизатор с функционалом NAT) или его эмуляция (например, Cisco Packet Tracer, GNS3, EVE-NG).
- **Программное обеспечение:**
  Терминальный эмулятор (PuTTY, SecureCRT или встроенный терминал в Linux/Windows) для подключения по консоли, Telnet или SSH.
- **Доступ:**
  Наличие административных прав для внесения изменений в конфигурацию устройства.

3.2. Шаги выполнения практической работы

Шаг 1. Подключение и начальная настройка

1. **Подключение к шлюзу:**
   - Подключитесь к устройству через консольный кабель или удалённо (SSH/Telnet).
   - Запустите терминальный эмулятор и установите соединение.
2. **Переход в привилегированный режим:**
   После входа в устройство (в режиме User) введите:

   shell Копировать Редактировать

   ```
   Router> enable
   Router#
   ```

   Примечание: Если требуется, введите пароль для привилегированного режима.

3. **Вход в режим глобальной конфигурации:**

```arduino
Router# configure terminal
Router(config)#
```

4. **Настройка имени устройства (hostname):**

```scss
Router(config)# hostname MyGateway
MyGateway(config)#
```

Комментарий: Новое имя помогает идентифицировать устройство в сети.

5. **Настройка IP-адреса на интерфейсе управления:**

Пример настройки интерфейса VLAN (для управления):

```arduino
MyGateway(config)# interface vlan 1
MyGateway(config-if)# ip address 192.168.10.1 255.255.255.0
MyGateway(config-if)# no shutdown
MyGateway(config-if)# exit
```

6. **Сохранение конфигурации:**

Выйдите из режима конфигурации и сохраните изменения:

```arduino
MyGateway# write memory
```

или

```lua
MyGateway# copy running-config startup-config
```

Шаг 2. Настройка маршрутизации и NAT

1. **Настройка статического маршрута (дефолтного маршрута):**

```arduino
MyGateway(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.254
```

Комментарий: Данный маршрут направляет весь исходящий трафик к шлюзу по умолчанию.

2. **Настройка NAT (если требуется):**

- **Определение внутренних и внешних интерфейсов:**
  Назначьте интерфейсу, подключенному к внутренней сети, статус «inside», а интерфейсу, подключенному к внешней сети, – статус «outside».

```arduino
MyGateway(config)# interface GigabitEthernet0/1
MyGateway(config-if)# ip nat inside
MyGateway(config-if)# exit

MyGateway(config)# interface GigabitEthernet0/2
MyGateway(config-if)# ip nat outside
MyGateway(config-if)# exit
```

- **Создание правила NAT с перегрузкой (PAT):**

```arduino
MyGateway(config)# access-list 10 permit 192.168.10.0 0.0.0.255
MyGateway(config)# ip nat inside source list 10 interface GigabitEthernet0/2 overload
```

Шаг 3. Диагностика и мониторинг

1. **Проверка таблицы маршрутизации:**

   Из привилегированного режима выполните:

   ```arduino
   MyGateway# show ip route
   ```

   Комментарий: Команда отобразит все активные маршруты.

2. **Просмотр активных NAT записей:**

   ```arduino
   MyGateway# show ip nat translations
   ```

   Комментарий: Позволяет убедиться, что трансляция адресов работает корректно.

3. **Просмотр текущей конфигурации:**

   ```lua
   MyGateway# show running-config
   ```

   Комментарий: Команда позволяет проверить внесённые изменения и убедиться, что они сохранены.

4. **Проверка доступности (ping):**

   Выполните команду для проверки связи с внешним ресурсом:

   ```arduino
   MyGateway# ping 8.8.8.8
   ```

Шаг 4. Работа с подсказками и справкой CLI

- **Использование контекстной справки:**

  Введите `?` после набора команды, чтобы получить список доступных опций, например:

  ```arduino
  MyGateway(config)# interface ?
  ```

  Комментарий: Это помогает быстро ознакомиться с доступными командами и аргументами.

Шаг 5. Завершение работы

- **Выход из сессии CLI:**

  После проверки и внесения изменений сохраните конфигурацию и выйдите из сеанса:

  ```shell
  MyGateway# exit
  ```

- **Анализ результатов:**

  Проверьте корректность работы устройства, убедитесь, что все изменения вступили в силу, и выполните повторное тестирование при необходимости.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий