АО «ЎЗБЕКИСТОН ТЕМИР ЙЎЛЛАРИ»

ТАШКЕНТСКИЙ ИНСТИТУТ ИНЖЕНЕРОВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

*На правах рукописи*
УДК 656.25

**УБАЙДУЛЛАЕВ АБДУХАФИЗ МАРУФЖОНОВИЧ**

# «МОДЕРНИЗАЦИЯ ЛИНИИ ПЕРЕДАЧИ ДАННЫХ НА БАЗЕ МУЛЬТИСЕРВИСНОЙ СЕТИ»

5А350102 « Устройства и системы передачи информации »

Диссертация
написанная для получения академической степени магистра



Научный руководитель с.н.с НИЛ
«СЦБ и связь» к.т.н. доцент
И.К. Колесников

Ташкент-2019

1

АО «ЎЗБЕКИСТОН ТЕМИР ЙЎЛЛАРИ»

ТАШКЕНТСКИЙ ИНСТИТУТ ИНЖЕНЕРОВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

*На правах рукописи*
УДК 656.25

**УБАЙДУЛЛАЕВ АБДУХАФИЗ МАРУФЖОНОВИЧ**

# «МОДЕРНИЗАЦИЯ ЛИНИИ ПЕРЕДАЧИ ДАННЫХ НА БАЗЕ МУЛЬТИСЕРВИСНОЙ СЕТИ»

5А350102 « Устройства и системы передачи информации »

Диссертация
написанная для получения академической степени магистра

Научный руководитель с.н.с НИЛ
«СЦБ и связь» к.т.н. доцент
И.К. Колесников

Ташкент-2019

## АННОТАЦИЯ

Магистерская диссертационная работа состоит из введения, трех глав, заключения и приложения.

Во введения указана актуальность тема, Цель и задачи, объекта исследования, научная новизна, практическая значимость.

В первой главе исследуется архитектура мультисервисной сети, во второй даны методы анализа и диагностика локальных сетей.

Третья глава посвящена разработке схем мультисервисной сети передачи к их расчету.

Диссертационная работа имеет 93 страниц машинописного текста, 30 рисунков, 3 таблицы, литературы 15 наименований и приложения 4.

## ANNOTATION

The master's thesis work consists of introduction, three chapters, conclusion and application.

The introduction indicates the relevance of the topic, purpose and objectives, the object of study, scientific novelty, practical significance.

The first chapter examines the architecture of the multiservice network, the second gives methods for analyzing and diagnosing local networks.

The third chapter is devoted to the development of multi-service network transmission schemes to their calculation.

The dissertation work has 93 pages, 30 figures, 3 tables, 15 titles of literature, annex 4.

## ANNOTATSIYA

Magistrlik dissertatsiyasi kirish, uchta bob, xulosa va ilovalardan iborat.

Kirish mavzuning maqsadi, maqsad va vazifalari, o'quv maqsadi, ilmiy yangilik, amaliy ahamiyatga ega ekanligini ko'rsatadi.

Birinchi bo'lim multiservis tarmog'ining arxitekturasini o'rganish, ikkinchisi mahalliy tarmoqlarni tahlil qilish va tashxislash uchun usullari ko’rsatilgan.

Uchinchi qism ko'p tarmoqli tarmoq uzatish sxemalarini ularning hisoblashlari uchun rivojlantirishga bag'ishlangan.

Dissertatsiya ishida 93 ta varoq, 30 ta rasm, 3 ta jadval, 15 ta ilmiy adabiyot, 4-ilova mavjud.

**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

Проведенные за годы независимости широкомасштабные реформы заложили прочный фундамент национальной государственности и суверенитета, обеспечения безопасности и правопорядка, неприкосновенности государственных границ, верховенства закона, прав и свобод человека, межнационального согласия и религиозной толерантности в обществе, создали достойные условия жизни для населения и реализации созидательного потенциала граждан.

В Государственной программе по реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017 — 2021 годах говорится о коренном улучшении транспортного обслуживания населения, повышения безопасности пассажирских перевозок и сокращение вредных выбросов в атмосферу.

**Актуальность темы**. В последние годы процесс информатизации всех сфер государственной и общественной жизни Узбекистана определяется ростом и внедрением современных информационных технологий и средств телекоммуникаций. Существенным образцом он повлиял и на развитие железнодорожного транспорта. При этом открылись новые перспективы, возникли задачи, требующие принятие решений для модернизации всей системы железнодорожного транспорта. Эти изменения, в свою очередь, также касаются и цифровизации средств и связи, как части инфраструктуры отрасли.

Основным направлением технического развитие и совершенствования средств телекоммуникаций на железнодорожном транспорте является внедрение цифровой техники и, прежде всего интеллектуальную сетевую инфраструктуру на базе протокола IP, включающую в себя маршрутизаторы, коммутаторы, шлюзы и другое сетевое оборудование. IP инфраструктура является основой для дальнейшего внедрения пользовательских приложений и должна обеспечивать поддержку таких жизненно важных для сети

сервисов, как безопасность, сетевое управление и механизмов гарантии качества сервиса (QoS, - Quality of Service). Поэтому создание мультисервисной сети на железнодорожном транспорте является актуальным. В связи с этим возникает научно практический интерес к созданию инновационной интегральной цифровой сети связи на основе мультисервисных линий и связм для АО «Ўзбекистон темир йўллари»

**Цель, задачи и степень разработанности проблемы.** Целью работы является исследование и организация мультисервисной сети связи для участка железнодорожного транспорта на основе технологи Cisco IP телефонии. Для достижения поставленной цели решаются следующие задачи:

- анализ архитектуры мультисервисной сети передачи данных;
- основы построения моделей системы IP телефонии;
- разработка методов анализа и диагностики локальных сетей;
- построения групповых каналов с использованием Cisco;
- разработка методов анализа мультисервисных сетей;
- выбор способов диагностирования локальных сетей;
- разработка схемы построения каналов технологической связи с использованием IP телефонии;
- разработка схемы построения мультисервисной сети передачи данных;
- расчет мультисервисной сети связи.

Результаты решения этих задач представляют основное содержания диссертации.

**Объекты исследования.** Объектом исследования явилась организация первичной сети ОТС-Ц по потоком «E1» АО «Ўзбекистон темир йўллари». Развитие сети на базе Cisco IP телефонии открывает новые возможности мультисервисного применения для железнодорожного транспорта.

**Научная новизна.** Новыми результатами являются:

-предоставление методики расчета мультисервисной сети с использованием Cisco IP телефонии;

-разработка схем построения групповых каналов и каналов технологической связи с использованием Cisco IP телефонии;

-методика расчета мультисервисной сети связи.

**Практическая значимость.** Полученные в работе результаты являются основой для дальнейшего внедрения пользовательских приложений и должна обеспечивать поддержку таких жизненно важных для сети сервисов, как безопасность, сетевое управление и механизмов гарантии качества сервиса (QoS, - Quality of Service).

**Краткое содержание глав.** В введении указаны актуальность темы диссертации, цель и задачи, научная новизна, практическая значимость.

В первой главе исследуется архитектура мультисервисной сети передачи.

Во второй главе рассмотрены методы анализа и диагностика локальных сетей.

В третей главе даны схемы мультисервисной сети скоростного участка железнодорожного транспорта Узбекистана и приведен расчет этих сетей.

**Вклад автора и исследование проблемы.** Все основные результаты, изложенные в работе, получены автором самостоятельно. Обсуждение постановки задачи и внедрение результатов выполнялось совместно с авторами, фамилии которых указаны в списке опубликованных работ.

**Структура и объем работы.** Диссертация состоит из введения, трех глав, заключения, приложения и списка литератур.

Она содержит 93 страниц машинописного текста, 30 рисунков, 3 таблицы, литературы 15 наименований, приложения 4.

**Публикация и апробация работы.** Материалы диссертационной работы докладывались (и опубликованы) на научно - технических конференциях, проведенных в ТашИИТе в 2017-2019 г.

# 1. ИССЛЕДОВАНИЕ АРХИТЕКТУРА МУЛЬТИСЕРВИСНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

## 1.1. Архитектура мультисервисных сетей

Основа построения мультисервисных сетей - архитектура Cisco Architecture for Voice Video and Integrated Data [6, 9, 13]. Это всеобъемлющая архитектура, состоящая из трёх основных блоков (рис. 1.1):

1. Интеллектуальная сетевая инфраструктура на базе протокола IP, включающая в себя маршрутизаторы, коммутаторы, шлюзы и другое сетевое оборудование. IP инфраструктура является основой для дальнейшего внедрения пользовательских приложений и должна обеспечивать поддержку таких жизненно важных для сети сервисов, как безопасность, сетевое управление и механизмов гарантии качества сервиса (QoS, - Quality of Service).

2. Интеллектуальные клиентские места с поддержкой протокола IP, в том числе цифровые IP телефоны, персональные компьютеры со специализированным программным обеспечением для решения различных бизнес-задач, программные эмуляторы телефонов, видео клиенты и так далее.

3. Служебные серверные приложения, в том числе серверы Cisco CallManager, обеспечивающие управление корпоративной системой IP телефонии, корпоративная система директорий, видео серверы и т. д.


Рис. 1.1. Архитектура Cisco AVVID

Мультисервисные сети могут содержать следующие компоненты (рис.1.2)

1. IP Phones
2. Gatekeeper
3. Gateway
4. Multipoint control unit (MCU)
5. Call agent
6. Application servers
7. Прочие компоненты, голосовые приложения, системы автоматического ответа (Interactive Voice Response)

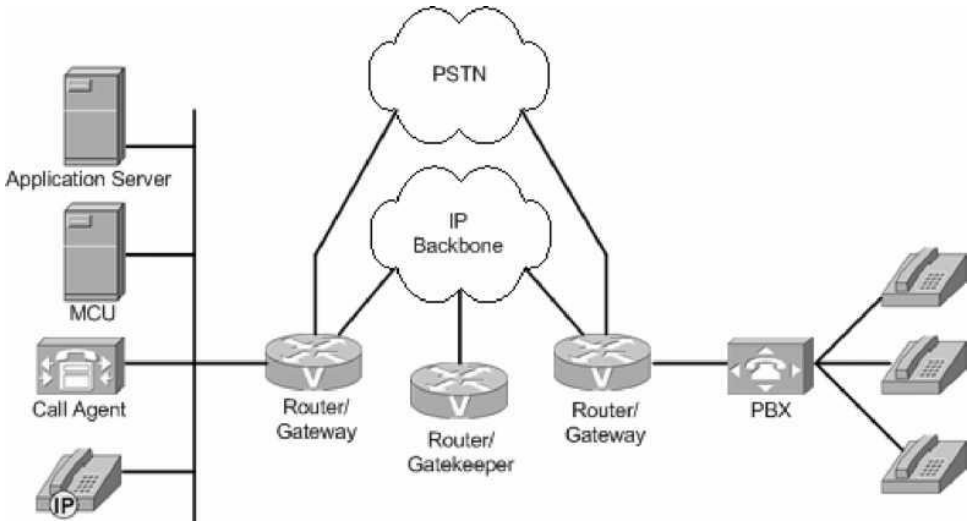


Рис.1.2. Основные компоненты мультисервисной сети

Характерной чертой рассматриваемой архитектуры являются ее распределенная природа, благодаря которой система легко масштабируема. Сеть на базе архитектуры Cisco AVVID может охватывать одно здание или несколько рядом стоящих зданий, объединенных кампусной сетью. Можно обеспечить сервисы телефонии, видео и данных для пользователей удаленных офисов и подразделений, объединенных корпоративной IP сетью.

Другая отличительная особенность архитектуры Cisco AVVID - это ее открытость, - ориентация на использование открытых стандартов (в частности, стандартных протоколов

н. 323, SIP и MGCP для передачи голоса и видео в сетях IP). Это позволяет обеспечить сопряжение с целым рядом других систем, как традиционной, так и пакетной телефонии, а также с системами передачи данных и видео приложениями, поддерживающими эти стандарты.

Поддержка открытых стандартных протоколов и открытых интерфейсов для разработки приложений (таких как TAPI и JTAPI), обеспечивает возможность написания новых приложений, интегрирующихся в системы на базе Cisco AVVID, а также возможность интеграции приложений, написанных сторонними производителями (рис.1.3).

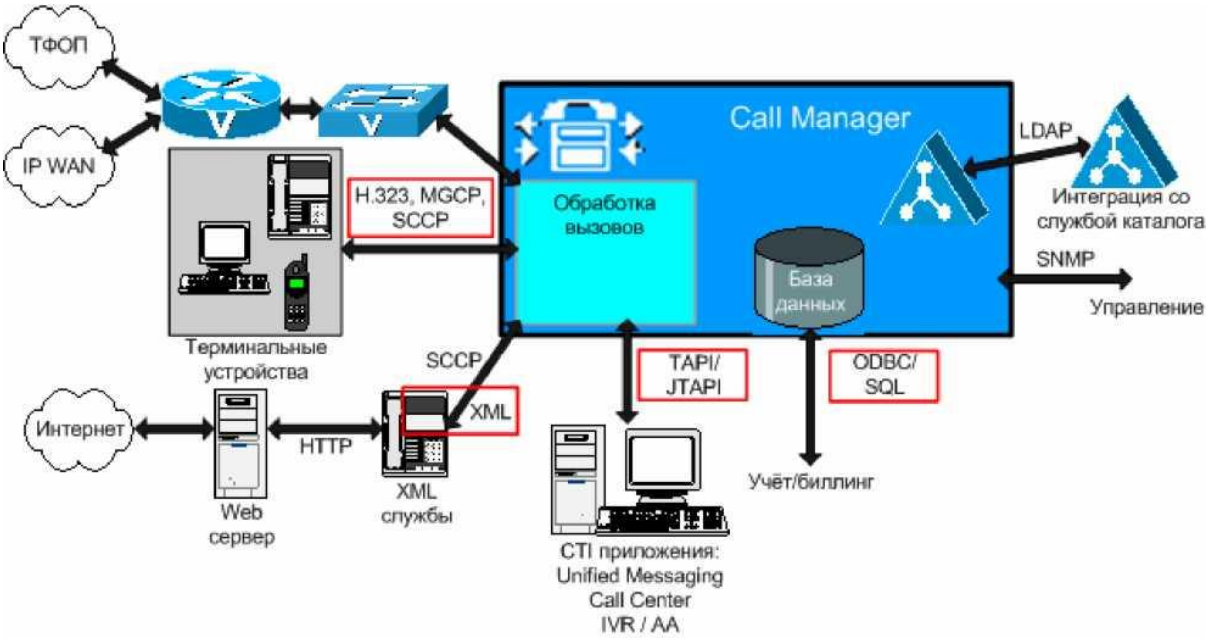


Рис.1.4. Интеграция с приложениями на основе открытых протоколов и интерфейсов

Как и всякая архитектура, Cisco AVVID имеет устойчивое основание, в виде трёхуровневой модели построения сетей.

Большинство современных сетей построено на основе трёхуровневой модели [4,10]. Как видно из рис.1.5, модель определяет три уровня: уровень ядра, уровень распределения и уровень доступа. Каждый уровень отвечает за реализацию определенных функций. Однако эти уровни являются логическими и не обязательно согласованы с физическими устройствами.

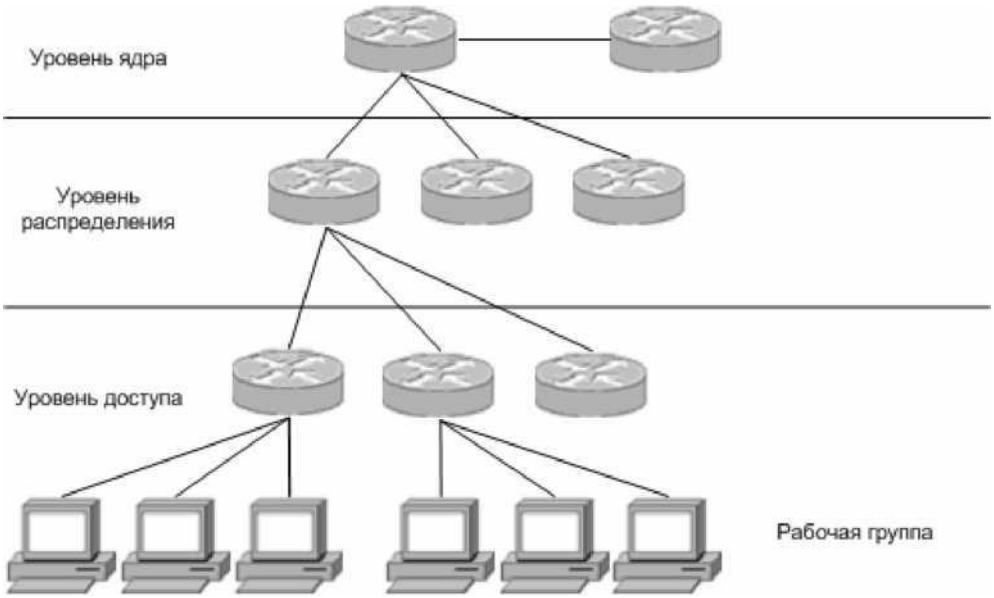


Рис.1.5. Дизайн сети: трёхуровневая модель

Следование данной модели позволяет значительно упростить построение сети и поиск неисправностей, а также обеспечивает предсказуемость и лучшую управляемость сети. Преимущества трёхуровневого построения, соответствующие требованиям к дизайну сети, либо недостижимы в других моделях, либо требуют значительных усилий для воплощения:

Масштабируемость. Разделение функциональности по слоям позволяет создать естественные точки расширения сети, не оказывая негативного влияния на остальные характеристики.

Лёгкость реализации. Поскольку иерархическая модель разделяет сеть на логическую и физическую составляющие, появляется возможность

постепенного построения и ввода в эксплуатацию отдельных участков сети.

Лёгкость поиска неисправности. Как правило, иерархическое построение сети облегчает задачу поиска неисправности, снижая количество возможных циклов.

Предсказуемость. Планирование пропускной способности существенно облегчается в иерархической модели, потребность в пропускной способности возрастают при приближении к ядру.

Управляемость. Предсказуемость потоков данных, масштабируемость, независимость реализации и лёгкость поиска неисправности существенно упрощают управление сетью.

На самом верху иерархии этот уровень отвечает за быструю и надежную пересылку больших объемов трафика. Единственным предназначением базового уровня является быстрая коммутация трафика.

Если происходит ошибка на уровне ядра, то она влияет на всех пользователей. Следовательно, весьма важно обеспечить высокую надежность на данном уровне. На этом уровне обрабатываются большие объемы трафика, поэтому не менее важно учитывать скорость и задержки.

Из указанных функций уровня ядра, следуют особенности его реализации:

- Ничто не должно замедлять трафик, в том числе списки доступа, маршрутизация между виртуальными локальными сетями VLAN и фильтрация пакетов;
- Не следует реализовывать функции доступа для рабочей группы;
- Следует избегать расширения уровня ядра при росте размеров объединенной сети (например, при добавлении маршрутизаторов). В случае нехватки производительности данного уровня, более предпочтительным выходом является модернизация, а не расширение.

Уровень распределения иногда называют уровнем рабочих групп. Он расположен между уровнем ядра и уровнем доступа. Основные функции уровня распределения состоят в маршрутизации, фильтрации и доступе к

региональным сетям, а также (если необходимо) в определении правил доступа пакетов к уровню ядра. Уровень распределения обязан устанавливать наиболее быстрый способ обработки запросов к службам (например, метод файлового обращения к серверу). После определения на данном уровне наилучшего пути доступа, запрос может быть передан на уровень ядра, где реализован скоростной транспорт запроса к нужной службе. На уровне распределения устанавливается политика сети, а также обеспечиваются возможности гибкого описания сетевых операций. На уровне распределения выполняется несколько функций:

- Реализация инструментов, подобных спискам доступа, фильтрации пакетов или механизму запросов;
- Реализация системы безопасности и сетевых политик, включая трансляцию адресов и установку брандмауэров;
- Перераспределение между протоколами маршрутизации, включая использование статических путей;
- Маршрутизация между сетями VLAN и другие функции поддержки рабочих групп;
- Определение доменов широковещательных и многоадресных рассылок.

На уровне доступа реализовано управление пользователями и рабочими группами при обращении к ресурсам объединенной сети. Иногда уровень доступа называют уровнем настольных систем. Наибольшая часть необходимых пользователям сетевых ресурсов должна быть доступна локально - для небольших сетей предлагается сохранение отношения трафик локального сегмента/внешний трафик на уровне 80/20, для больших корпоративных сетей существует тенденция к увеличению объёма внешнего трафика - до соотношения 20/80. На уровне распределения выполняется перенаправление трафика к удаленным службам. Для уровня доступа характерны следующие функции:

- Постоянный контроль (из уровня распределения) за доступом и

политиками;

- Формирование независимых коллизионных доменов (сегментация);
- Соединение рабочих групп с уровнем распределения.

Для перехода от традиционной телефонии к мультисервисным сетям, должны быть обеспечены отказоустойчивость, качество обслуживания (QoS) и пропускная способность, необходимые для поддержки приложений мультисервисной сети, таких как передача потоковых голоса и видео [3, 8].

Например, должны выполняться следующие требования:

- Стандартный кодек G.729 для отсутствия ошибок воспроизведения требует, чтобы потеря пакетов, была значительно меньше 1 процента;
- Спецификация ITU G. 114 рекомендует, чтобы задержка при VoIP пакета при пересылке от абонента до абонента не превышала 150 миллисекунд (ms). Для международных звонков приемлемой считается задержка до 300 миллисекунд, особенно при использовании спутниковых каналов. При вычислении этой задержки также учитывается время распространения сигнала вдоль тракта передачи данных;
- Должны быть минимизированы колебания длительности задержки (jitter), для чего используют буферизацию данных. Данное решение увеличивает задержку передачи данных между абонентами и является эффективным только при колебаниях, не превышающих 100 миллисекунд.

Поэтому одним из необходимых условий для внедрения IP телефонии является замен широковещательной среды передачи данных на коммутируемую, однако, эта проблема не актуальна в настоящий момент, что обусловлено существенным падением цен на соответствующее оборудование и практически стопроцентным переходом на коммутируемую среду передачи данных (рис. 1.6).

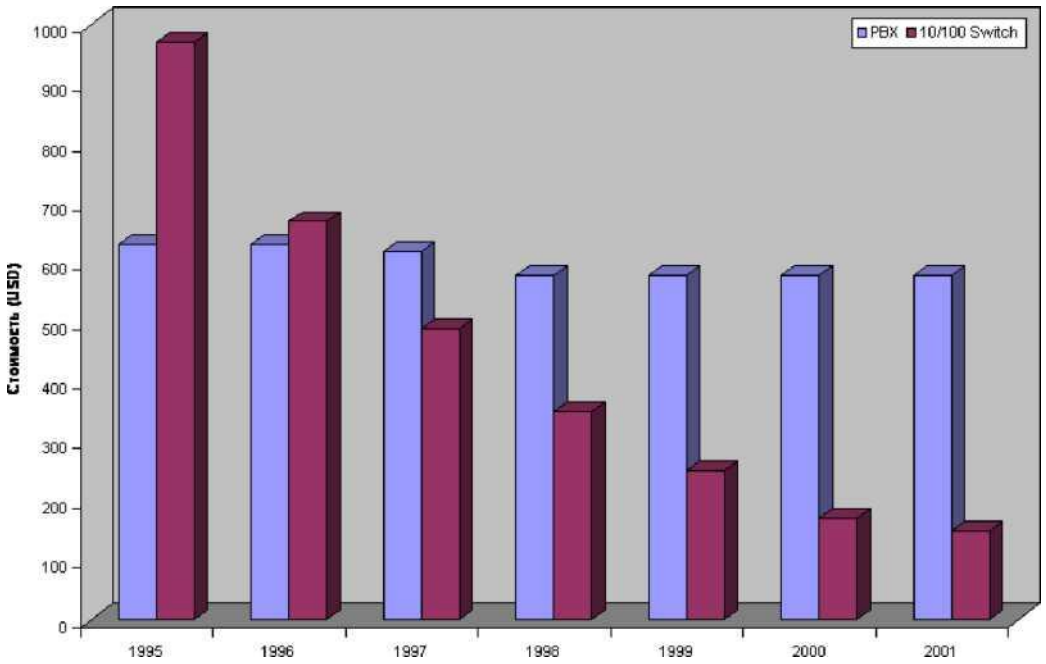


Рис.1.6. Сравнительный график средней стоимости оборудования в расчёте на один порт

Помимо этого для надёжной транспортировки голоса и видео требуется поддержка расширенной приоритизации трафика, многоадресных рассылок, буферизации и компрессии.

Для обеспечения высокого качество передачи голоса требуется, чтобы пакеты VoIP (как сигнального, так и аудио канала) имели приоритет по отношению к другим типам трафика. Необходимо удовлетворение требований по отказоустойчивости, пропускной способности, задержке и колебаниям величины задержки в сети.

Традиционная телефония обеспечивает надежное функционирование системы 99.999% времени, это соответствует 5.25 минуты простоя в год. Многие сети передачи данных не обеспечивают такого уровня надёжности. Поэтому одним из основных требований при внедрении VoIP является высокая надёжность и доступности сети.

Меры, направленные на обеспечение отказоустойчивости, могут включать:

• приобретение оборудования и программного обеспечения с высоким

показателем MTBF (mean time between failures) - среднее время между сбоями;

• установку дублирующего оборудования;

• прокладку дублирующих линий связи;

• обеспечение бесперебойного электропитания сетевого оборудования, включая оборудование конечных пользователей;

• упреждающее управление сетью и решение проблем до их проявления.

Для полной отказоустойчивости требуется дублирование следующих компонентов:

• серверы и CallManager-ы;

• устройства уровня распределения, такие как маршрутизаторы и многоуровневые коммутаторы;

• устройства уровня ядра, такие как многоуровневые коммутаторы;

• соединения с оператором телефонной связи, WAN, возможно даже через различных провайдеров, голосовые шлюзы;

• источники электропитания и UPS.

При переходе к мультисервисной сети требуется обеспечить необходимую пропускную способность для потокового голосового и видео трафика. Это накладывает ограничение на канал передачи данных и сетевое оборудование. Требуемая пропускная способность определяется используемой технологией сжатия аудио или видео данных,

Пропускная способность - это реальный объем полезных данных, переданный от источника до получателя. Предаваемый объём увеличивается за счёт накладных расходов - заголовков протокольных блоков данных различных уровней. Данные также подвержены ошибкам передачи. Объём передаваемых данных ограничен пропускной способность канала, при перегрузке сети возможны потери пакетов, что так же может привести к необходимости повторной передачи.

Для обеспечения требуемой пропускной способности применяются

следующие техники:

a. Использование очередей: основывается на передаче пакетов через конкретный интерфейс в соответствии с заданными приоритетами, позволяет обрабатывать интенсивные потоки, управлять нагрузкой сети, приоритизировать трафик, резервировать пропускную способность;

b. Сжатие заголовков: в IP сетях голос передаётся при помощи протокола реального времени Real-Time Transport Protocol (RTP), который переносится протоколом UDP, датаграммы UDP инкапсулируются в пакеты IP. Таким образом, составной заголовок RTP/UDP/IP достигает 40 байт. Это достаточно большая величина, поскольку объем данных, предаваемых в одном пакете, в большинстве случаев составляет 20 байт. Применение сжатия заголовков (CRTP) уменьшает размер заголовка до 2-4 байт.

c. Контроль установления вызова: данный механизм расширяет возможности обеспечения качества обслуживания, обеспечивая защиту голосового трафика от негативного влияния другого голосового трафика путём ограничения количества одновременно установленных вызовов.

d. Фрагментация и чередование: при фрагментации большие пакеты разбиваются на более мелкие, между которыми передаются голосовые пакеты, что позволяет избежать задержек, связанных с выводом больших пакетов в интерфейс.

В основе обеспечения качества обслуживания лежит возможность сетевых устройств распознавать и группировать специфические пакеты. Процесс распознавания получил название “классификация пакетов”. После классификации пакет должен быть помечен соответствующим образом, для чего выставляются соответствующие флаги в IP заголовке.

Для распознавания VoIP пакетов сетевые устройства используют адреса источника и получателя в заголовке IP и номера портов UDP источника и получателя в заголовке UDP.

Помимо статической классификации основанной на заголовках протокольных блоков данных 3 и 4 уровней, может быть использован

механизм динамической классификации, такой как Resource Reservation Protocol (RSVP).

Классификация пакетов - достаточно ресурсоёмкий процесс, поэтому классификация должна происходить как можно ближе к краю сети. В ядре классификация должна быть максимально упрощена, это достигается за счёт маркирования пакетов - установки байта типа сервиса (Type of Service) в заголовке IP.

Три старших бита байта (ToS) называются битами старшинства IP (IP Precedence). В настоящее время большинство приложений и производителей оборудования поддерживают установку и распознавание битов старшинства IP. Часто для определения дифференцированных классов сервиса (Differentiated Services classes) используются шесть старших битов, называемых Differentiated Services Code Point.

Маркирование пакетов может осуществляется установкой следующих флагов:

- Три бита IP Precedence байта ToS заголовка IP пакета;
- Шесть битов DSCP байта ToS заголовка IP пакета;
- Три бита MPLS Experimental (EXP);
- Три бита Class of Service Ethernet 802.1p;
- Один бит Cell Loss Probability (CLP) ATM.

В большинстве IP сетей, маркирование осуществляется установкой IP Precedence или DSCP, что вполне достаточно для идентификации VoIP трафика.

Классификация и маркирование Voice Dial Peers

Данная техника позволяет классифицировать пакеты VoIP в зависимости от номера, с которым осуществляется соединение.

Классификация и маркирование Committed Access Rate (CAR)

Committed access rate (CAR) - техника использующая лимитирование максимального значения уровня пропускной способности, используемого трафиком. CAR позволяет выставлять различные биты IP Precedence или

DSCP в зависимости от того, превышен ли установленный лимит. Однако техника классификации CAR чаще используется для пакетов данных, нежели для пакетов VoIP.

Применение политик маршрутизации (Policy-Based Routing)

Данная техника позволяет маршрутизировать трафик, основываясь на списках доступа (ACL), используемом протоколе, номере порта-источника и так далее. Поскольку данная технология позволяет изменять широкий круг полей пакета или кадра, её применение также возможно для классификации и маркирования пакетов.

Модульный интерфейс QoS командной строки (Mod QoS CLI или MQC)

Данный метод, основанный на применении шаблонов, является наиболее предпочтительным способом классификации и маркирования пакетов. Он позволяет отделить классификацию от политик, обеспечивая возможность конфигурирования различных средств обеспечения качества обслуживания для различных классов трафика. Для классификации трафика применяется class map, а для определения необходимых действий для каждого класса - policy map, которая применяется к входящему или выходяшему трафику конкретного интерфейса.

Call Admission Control (CAC) применяется к голосовому и видео трафику. В случае если сетевое соединение перегружено пакетами данных, выходом может стать применение очередей, буферизация и отбрасывание пакетов. Трафик задерживается до освобождения интерфейса или отбрасывается, а в последующем пользователь или протокол запрашивают повторную передачу.

Для трафика реального времени, чувствительного к задержке и потере пакетов, такой способ разрешения проблемы приведёт к падению качества обслуживания. В данном случае предпочитают ограничить возможность доступа в сеть, нежели потерять качество.

CAC представляет собой информированный способ принятия решения

о достаточности свободных ресурсов для обеспечения требуемого качества передачи голоса. Существует несколько различных механизмов контроля установления вызова:

- локальные - решение об установлении вызова принимается на основе состояния исходящего LAN или WAN интерфейса. Данные механизмы имеют возможность статически ограничить максимальное число одновременно установленных вызовов;
- основанные на измерениях - решение принимается на основе измерения текущего состояния сети, которое проводится посылкой пробных пакетов по заданному IP адресу (обычно это голосовой шлюз адресата). Получатель возвращает пакеты, на основании чего стоится некоторая статистика (обычно задержка и процент потери пробных пакетов), характеризующая состояние сети на данный момент;
- основанные на ресурсах - они делятся на два класса: определяющие количество запрашиваемых и/или свободных ресурсов, и резервирующие ресурсы. Ресурсы представляющие интерес включают пропускную способность соединения, загрузку ЦП, количество памяти.

Локальные механизмы CAC

*Физическое ограничение DS0* - задание количества временных слотов для Time Division Multiplexing интерфейсов. Обладает лёгкостью конфигурирования, но не применим к другим типам интерфейсов.

Достоинства:

- не требует нагрузки ЦП и дополнительной пропускной способности;
- позволяет экономить пропускную способность WAN соединения;
- широко используется.

Недостатки:

- невозможно использовать для IP телефонии в LAN;
- неприменимо для сложной топологии;
- не реагирует на изменения сети.

*Задание максимального числа соединений* - ограничивает максимальное число соединений с каждой группой абонентов (dial-peer). Обладает лёгкостью конфигурирования, но единственным способом ограничить число соединений через данный шлюз является задание определённого числа групп абонентов с ограничением максимального числа соединений для каждой.

Достоинства аналогичны предыдущей технологии.

Недостатки:

- можно использовать только при задании групп абонентов (dial-peer);
- неприменимо для сложной топологии;
- не реагирует на изменения сети.

*Задание максимальной используемой пропускной способности* - ограничивает максимальное использование пропускной способности, и используется только для VoFR. При достижении максимального значения всем последующим вызовам будет отказано в соединении.

*Проверка состояния транкового соединения (Trunk Conditioning)* - при выходе из строя транкового WAN соединения, информация об этом передаётся учрежденческой АТС - источнику вызова и вызов может быть направлен по альтернативному пути (рис. 1.7).

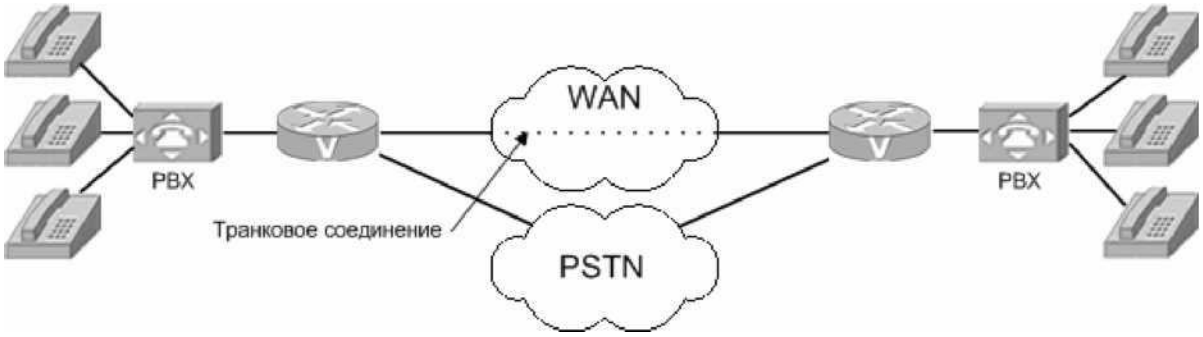


Рис.1.7. Trunk Conditioning

Особенность механизма является использование постоянного обмена небольшими сообщениями, отслеживающими как состояние WAN соединения между абонентами, так и состояния локальных соединений с

Plain Old Telephone System.

*Local Voice Busyout* - аналог механизма Trunk Conditioning, для коммутируемой среды передачи данных. LVBO позволяет объявить транковое соединение PBX со шлюзом как вышедшее из строя, если WAN соединение не обеспечивает приемлемое качество обслуживания. Сигнал Busyout посылается PBX в случае, если происходит сбой любого из отслеживаемых интерфейсов (рис.1.8).

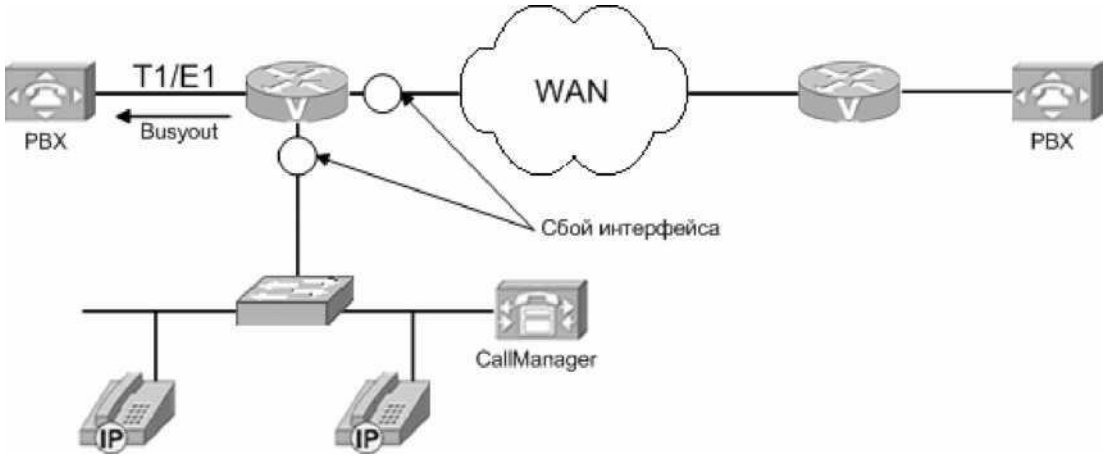


Рис.1.8. Local Voice Busyout

Достоинства:

• не требуется отвергать каждый запрос на соединение индивидуально, что уменьшает postdial задержку;

• не требуется возврата (hairpinning) отвергнутого вызова PBX-инициатору, что достигается использованием нескольких DS0 слотов для одного вызова;

• возможно перенаправление отвергнутых вызовов PBX, которые не поддерживают такой функциональности или не сконфигурированы должным образом.

Недостатки:

• отслеживает Ethernet LAN интерфейсы (не Fast Ethernet);

• используется только для аналоговых или CAS транков.

Механизмы CAC, основанные на измерениях

Данные механизмы опираются на Service Assurance Agent, который

обеспечивает измерения задержки и потерь пакетов для принятия решения о сбросе вызова. Хотя явных

измерений пропускной способности вдоль пути пакета не производится, в случае, если имеет место перегрузка сети, следует ожидать высокой задержки и потери пакетов.

SAA - это клиент-серверный протокол, использующий UDP. Клиент конструирует и посылает пробные пакеты. Для точности измерения пакеты SAA строятся также как и пакеты VoIP (IP Precedence и заголовок RTP/UDP/IP), что позволяет учитывать механизмы QoS, существующие в сети. Размер пакетов выбирается соответственно используемому кодеку. Адресат возвращает пакеты отправителю. Пробные пакеты SAA для контроля установления вызова отсылаются случайным образом на порт из верхней части портов UDP, отведенных для передачи аудио (с 16384 до 32767).

Для принятия решения используется показатель Calculated Planning Impairment Factor (ICPIF) - ITU G.113, который представляет задержку и процент потери пакетов в виде одного из чисел, приведённых в таблице 1.1.

Табл. 1.1. Интерпретация значений ICPIF (ITU G.113)

| Значение | Оценка качества |
|---|---|
| 5 | Very good |
| 10 | Good |
| 20 | Adequate |
| 30 | Limiting case |
| 45 | Exceptional limiting case |
| 55 | Customers likely to react strongly |

*Advanced Voice Busyout* - расширение LVBO. Как и LVBO обеспечивает подачу сигнала Busyout для PBX, основываясь на локальных данных шлюза, но также поддерживает посылку SAA пробных пакетов по одному или более IP адресам. Возвращаемая информация представляет собой ICPIF или

непосредственные величины задержки и процента потери пакетов и служит основанием для сигнализации о занятости сети учрежденческой АТС или отдельному голосовому порту (рис. 1.9).

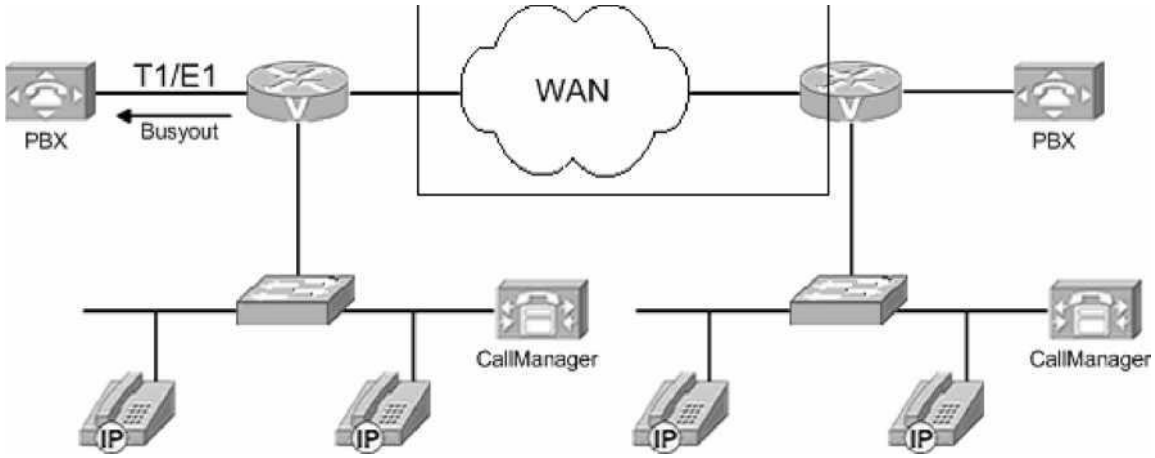


Рис.1.9. Advanced Voice Busyout

Недостатки:

- метод основан на пробах и даёт лишь статистическое, а не абсолютное, решение;
- IP адрес назначения пробных пакетов задан фиксировано и конфигурируется вручную;
- устройство, которому посылаются пробные пакеты должно поддерживать SAA responder;
- мониторинг включает только сети IP, невозможно отслеживать состояние удалённого телефонного транка;
- применение данного метода неэффективно в сетях, для которых характерны большие колебания объёма трафика в короткое время;
- используется только для аналоговых или CAS транков, CCS транки не поддерживаются.

*PSTN Fallback* - в отличие от Advanced Voice Busyout не блокирует транковые соединения и не обеспечивает никакой общей сигнализации PBX о том, что WAN соединение не способно обеспечить требуемое качество

обслуживания. Каждое CAC решение принимается по факту поступления запроса на вызов (рис.1.10). Данных механизм может принимать решение для любой IP сети, включая Internet. Хотя PSTN fallback нельзя напрямую использовать с IP телефонами и приложениями VoIP для PC, возможно косвенное использование, если данные устройства находятся за маршрутизатором, поддерживающим SAA responder.

Также PSTN fallback не требует статического конфигурирования IP адресов для SAA. Программное обеспечение использует кэш изменяемого размера для хранения последних IP адресов, по которым осуществлялись вызовы. При попадании в кэш CAC решение принимается немедленно, при промахе инициируется серии проб. Таким образом, увеличение postdial delay будет наблюдаться только для первого звонка по каждому заданному IP адресу.

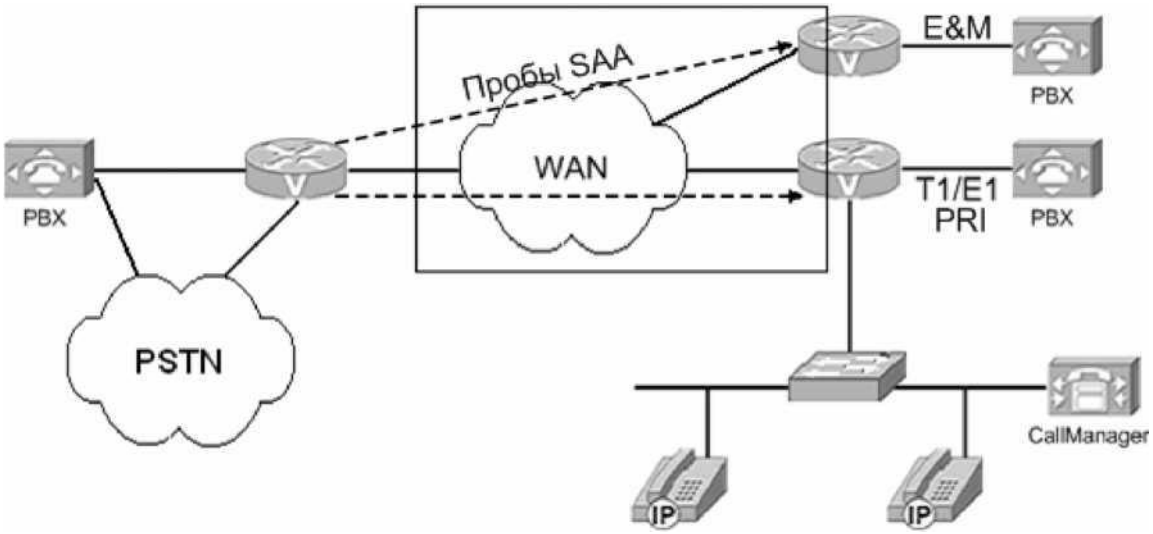


Рис.1.10. PSTN Fallback

Варианты действий в случае отрицательного решения CAC:

•вызов через другой IP адрес;

•перенаправление вызова через PSTN;

•отказ (reject) вызова PBX/PSTN (BRI/PRI/QSIG);

•возврат (hairpin) вызова PBX/PSTN (аналоговые и CAS протоколы);

•генерация коротких сигналов (reorder tone).

Недостатки:

•механизм применим только для IP сетей;

• при изменении нагрузки на сеть перемаршрутизации установленных соединений не происходит;

• для первого вызова по каждому новому IP адресу возникает увеличение postdial delay;

•метод основан на пробах и даёт лишь статистическое, а не абсолютное, решение;

• применение данного метода неэффективно в сетях, для которых характерны большие колебания объёма трафика в короткое время;

• невозможно измерение пропускной способности;

• возможно использование MD5 аутентификации.

Механизмы CAC, основанные на ресурсах

Существует два типа механизмы CAC, основанных на ресурсах:

• механизмы, отслеживающие использование определённых ресурсов и вычисляющих метрику, которая является основой принятия решения CAC;

• механизмы, резервирующие ресурсы необходимые для звонка.

Только механизмы второй категории способны обеспечить QoS на протяжении всего телефонного разговора, прочие механизмы принимают статистическое решение, опираясь на знание о текущем состоянии сети.

*Resource Availability Indication* - представляет собой опциальную функцию протокола

H. 323v2, обеспечивающую передачу RAS сообщения от конечного (terminating) шлюза gatekeeper-у (рис.1.11). Данное сообщение несёт информацию о способности или не способности данного шлюза принять новые звонки, при этом gatekeeper не имеет информации об имеющихся ресурсах шлюза.

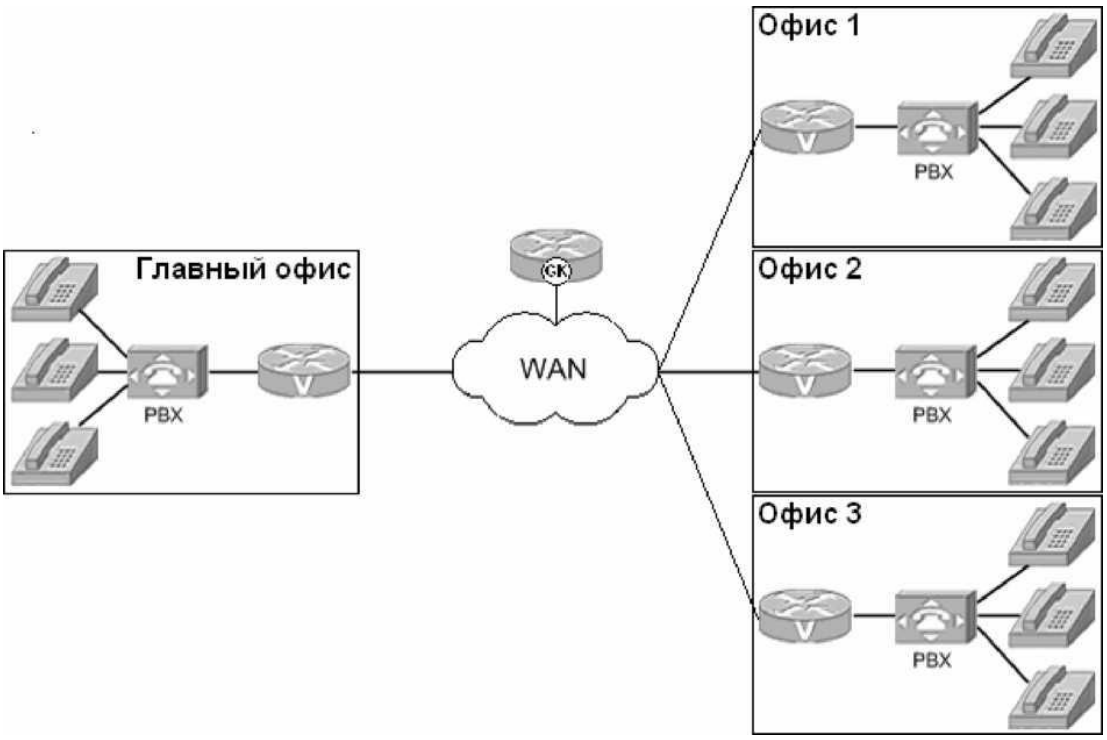


Рис.1.11. Resource Availability Indiecation

RAI единственный механизм, учитывающий состояние удалённого соединения.

Поскольку RAI обеспечивает передачу сообщения между шлюзом gatekeeper-ом, то данный механизм применим только в H.323 сетях, содержащих gatekeeper.

*Gatekeeper Zone Bandwidth* - этот механизм также специфичен для H.323 gatekeeper сетей, и позволяет устанавливать статические ограничения на используемую пропускную способность внутри определённой зоны, обслуживаемой данным Gatekeeper-ом, и между указанной зоной и любой другой внутри сети. Если запрашиваемый вызов превысит заданное максимальное значение используемой полосы пропускания, происходит отказ в вызове (рис. 1.12). При этом gatekeeper не имеет данных о топологии сети или реальном значении используемой различным трафиком пропускной способности.

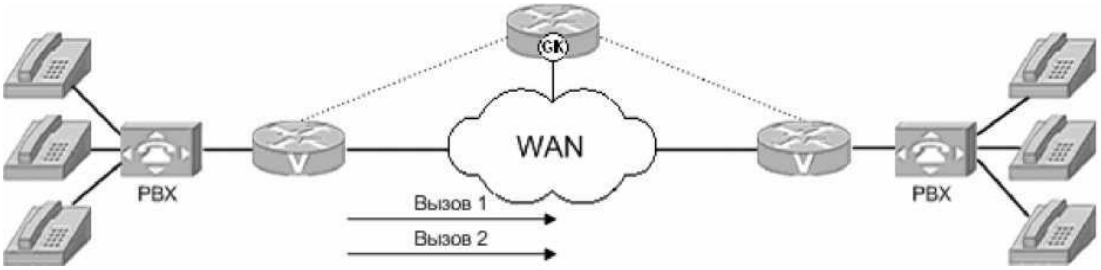


Рис. 1.12. Gatekeeper Zone Bandwidth

В сетях, где для отказоустойчивости применяется дублирование gatekeeper-ов с использованием Hot Router Standby Protocol, нет разделяемой информационной базы, таким образом, после отказа gatekeeper-а его преемник не будет иметь информации об используемой пропускной способности. И пока данная информация не соответствует действительности, существует возможность установления большего, чем разрешено, количества соединений.

*Resource Reservation Protocol* - единственный механизм CAC, осуществляющий резервацию требуемой полосы пропускания, что позволяет обеспечить не только принятие CAC решения, но и обеспечение QoS на протяжении всего телефонного звонка, независимо от изменяющихся условий функционирования сети.

Резервирование осуществляется в обоих направлениях, поскольку во время разговора информация передаётся в обоих направлениях, решение об установлении вызова принимается шлюзом вызываемого абонента, в зависимости от результатов резервирования.

Отличительными чертами RSVP является:

- возможность обеспечивать качество обслуживания на протяжении звонка;
- знание топологии. RSVP резервирование производится на каждом интерфейсе вдоль пути передачи голосовых пакетов, при этом нет необходимости знать реальную пропускную способность каждого интерфейса. Таким образом, RSVP автоматически учитывает изменения сети;

- для правильного функционирования требуется соответствующая настройка всех сетевых устройств;
- обеспечивая резервирование, данный протокол не учитывает количество уже установленных вызовов.

Если приоритетный пакет голосового трафика поступает в исходящую очередь в то время, когда передаётся пакет данных из зарезервированной очереди, неизбежна задержка (serialization delay). Учитывая, что пакет данных может иметь размер близкий к MTU (1500 байт для serial и 4470 байт для high-speed serial интерфейсов), величина задержки будет неприемлемой.

Например, для интерфейса со скоростью 64 kbps и MTU 1500 байт, задержка составит (1500 байт * 8 бит/байт) / (64,000 бит/с) = 187.5 мс. При необходимости обеспечить задержку передачи между абонентами не более 150 мс и ограничениями на колебания длительности задержки (jitter). Возникает необходимость уменьшения задержки вывода, что достигается путём рассечения больших пакетов на части, время передачи которых не превышает 10 мс. Размер фрагмента вычисляется (0.01 с * 64,000 бит/с) / (8 бит/байт) = 80 байт. При этом простого фрагментирования недостаточно, поскольку пакет VoIP будет находится в очереди позади фрагментов большого пакета, требуется переупорядочивание пакетов (рис.1.13).


Рис. 1.13. Фрагментация и чередование

## 1.2. Модели построения систем IP телефония

Встречается три основных модели построения сетей Cisco IP телефонии.

Простейший вариант представляет из себя локальную/кампусную сеть с интеграцией голоса и данных (а также, возможно, видео приложений).

В этом случае сетевая инфраструктура представлена коммутируемой сетью на базе технологий Ethernet / Fast Ethernet / Gigabit Ethernet. Пользовательские IP телефоны подключаются в пределах локальной/кампусной сети и работают под управлением сервера Cisco CallManager. Один сервер Cisco CallManager может поддерживать до 2500 IP телефонов. В целях масштабирования системы и для обеспечения отказоустойчивости серверы Cisco CallManager могут быть объединены в кластер.

В локальной/кампусной сети экономия полосы пропускания не является критичной, поэтому для голосовых звонков в пределах локальной сети сжатие голоса обычно не используется.

Серверы пользовательских приложений, таких как система голосовой почты или интерактивных голосовых меню, расположенные в пределах кампусной сети, обеспечивают дополнительные сервисы для абонентов системы.

Основные характеристики модели построения сети IP телефонии для одного здания или кампуса (нескольких зданий, объединенных высокоскоростной локальной сетью):

- для организации системы IP телефонии используется сервер Cisco CallManager или кластер серверов Cisco CallManager (для обеспечения масштабируемости и отказоустойчивости решения в пределах кампусной сети);
- на одном сервере Call Manager поддерживается до 2500 телефонов;
- поддерживается до 10000 IP телефонов на кластер Cisco CallManager;

• для дальнейшего масштабирования сети возможность использование нескольких кластеров Cisco CallManager;

• максимальное количество серверов Cisco CallManager в кластере - восемь (4 сервера для основной обработки вызовов, два для резервной обработки, один сервер базы данных и один TFTP сервер);

• для подключения к телефонной сети общего пользования (ТФОП), подключения аналоговых телефонов и факсовых аппаратов и стыковки с существующими учрежденческими АТС используются голосовые шлюзы;

• ресурсы голосовых сервисных модулей используются для организации аудиоконференций;

• для всех голосовых звонков используется кодек G.711 (несжатый голос);

• для обесепечение качественной работы различных приложений используются коммутаторы, поддерживающие необходимые средства обеспечения качества сервиса (QoS).

Один из наиболее распространенных вариантов построения системы IP телефонии представляет собой распределенную систему, обеспечивающую сервисы корпоративной IP телефонии не только для центрального офиса, но и для удаленных подразделений/офисов, подключенных к корпоративной IP сети с обеспечением необходимых механизмов качества сервиса (QoS).

В такой схеме сервер CallManager, расположенный в центральном отделении, управляет установлением телефонных соединений и функционированием телефонных аппаратов, расположенных в удаленных точках в пределах корпоративной IP сети (рис. 1.14).

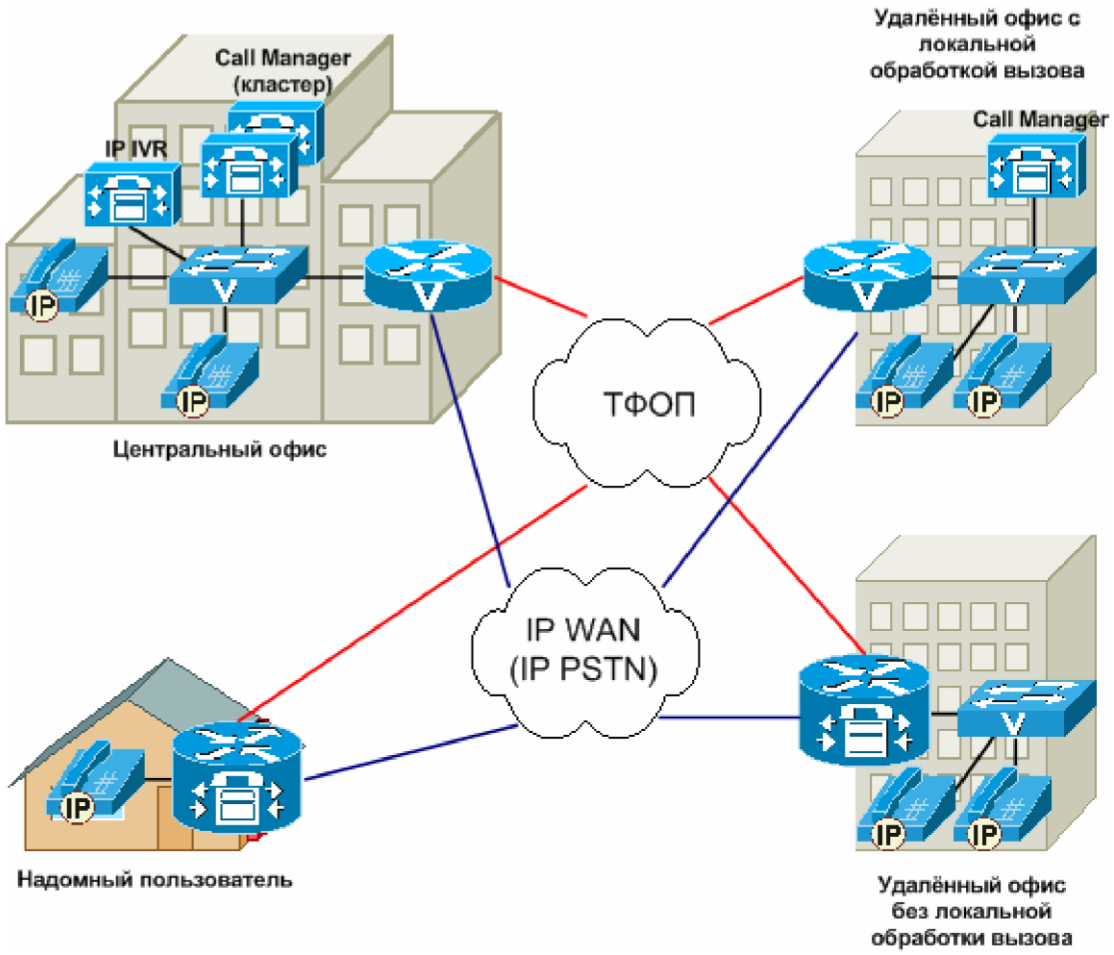


Рис.1.14. Распределённая схема построения систем IP телефонии

Подобная архитектура имеет ряд достоинств, среди них:

- простота и экономичность внедрения телефонии для небольших удаленных отделений;
- возможность централизованной настройки и управления телефонной системой;
- простота организации доступа удалённых абонентов к современным сервисам телефонии, развернутым в центральном отделении, таким как сервисы голосовой почты/унифицированной обработки сообщений, доступ к автоматическим телефонным справочникам с IP телефона и т.д.;
- возможность использования ресурсов корпоративной сети передачи данных для установления телефонных соединений между различными отделениями, объединенными сетью IP телефонии. При этом

возможна экономия на оплате междугородних телефонных разговоров между различными отделениями и повышение эффективности использования каналов WAN за счет использования единого набора каналов для передачи трафика голоса и данных;

- нет необходимости иметь опытный персонал службы технической поддержки в каждом удаленном подразделении/офисе.

При использовании подобной схемы построения сети должна быть обеспечена возможность локальной обработки вызовов в удаленном отделении на случай потери связи между удаленным и центральным отделением, например в случае сбоя канала WAN. Для этой цели можно использовать средства отказоустойчивой телефонии для удаленных офисов (Survivable Remote Site Telephony).

Основные характеристики распределенной модели построения сети IP телефонии с централизованной обработкой вызовов:

- сервер Cisco CallManager или кластер серверов Cisco CallManager, расположенный в центральной точке сети используется для управления локальными телефонами и телефонами, находящимися в удаленных офисах;
- на одном сервере Call Manager поддерживается до 2500 телефонов;
- удаленные офисы подключаются к корпоративной IP сети с обеспечением необходимых механизмов качества сервиса (QoS);
- для подключения к телефонной сети общего пользования (ТФОП), подключения аналоговых телефонов и факсовых аппаратов и стыковки с существующими УАТС используются голосовые шлюзы;
- голосовые шлюзы могут располагаться как в центральной, так и в удаленных точках сети IP телефонии;
- для организации конференций и транскодинга (перекодирования голоса из низкоскоростного кодека в высокоскоростной) можно использовать голосовые сервисные модули (расположенные в сети центрального офиса);

- в пределах локальной сети возможно использование кодека G.711 (несжатый голос);
- для экономного использования полосы пропускания на каналах WAN может быть использовано сжатие голоса (кодек G.729);
- Cisco CallManager контролирует использование полосы пропускания на каналах WAN между удаленными офисами и принимает решение о разрешении/запрете установления телефонного соединения на основе информации о наличии свободной полосы пропускания (call admission control);
- поддержка механизмов обеспечения качества сервиса (QoS) в пределах распределенной IP сети является критично важной для обеспечения качественной работы различных приложений (это особенно важно для голосовых приложений).

Третий вариант построения сетей IP телефонии предусматривает использование собственных управляющих серверов Cisco CallManager и серверов приложений в каждом офисе. Такая модель применяется для сетей, объединяющих крупные и средние офисы или в случае, когда имеются специфические требования к сервисам телефонии для конкретных офисов, их надежности и быстродействию.

В таком варианте построения сети для организации взаимодействия между серверами/кластерами серверов CallManager, расположенными в центральном и удаленных офисах компании, может использоваться H.323 gatekeeper. Gatekeeper может также использоваться в этой модели для целей контроля за установлением телефонных соединений (call admission control).

Один H.323 gatekeeper может обеспечить взаимодействие до 100 кластеров Cisco CallManager. Возможна также иерархическая модель с построения сети с использованием Directory gatekeeper’a. Это обеспечивает возможность масштабирования системы до многих сотен тысяч абонентов.

Возможно также использование смешанных моделей построения сети IP телефонии, включающих существующие учрежденческие АТС.

## 1.3. Протоколы для мультисервисной сети на базе IP телефония

Короткая, но богатая событиями история развития IP-телефонии привела к тому, что сегодня в реальных сетях VoIP сосуществуют и конкурируют между собой несколько семейств сигнальных протоколов, которые регламентируют управление мультимедиавызовами и передачу медиа-трафика в IP-сетях.

Помимо протокола сигнализации другой важной составляющей частью IP телефонии является протокол RTP (Real Time Protocol), который обеспечивает сквозной сетевой транспорт для приложений требующих передачи потоковых данных в реальном времени, таких как аудио и видео.

RTP является критическим компонентом VoIP, обеспечивая для получателя возможность переупорядочивания и хронометража пакетов перед воспроизведением. Заголовок RTP содержит временные отметки и последовательные номера, позволяющие буферизовать пакеты и устранять колебания длительности задержки.

Протокол RTCP отслеживает качество передачи данных и обеспечивает управляющую информацию. Для устройств вовлечённых в RTP сессию RTCP обеспечивает механизм обмена управляющей информацией и информацией о состоянии сессии. RTCP отслеживает такие показатели качества как: количество переданных и потерянных пакетов, задержка и колебание длительности задержки.

### 1.3.1. Сигнальные протоколы

На сегодняшний момент в реальных сетях VoIP представлены три основных семейства сигнальных протоколов - H.323, SIP и MGCP. Протоколы всех трех перечисленных семейств регламентируют управление мультимедиа-вызовами и передачу медиа-трафика в IP-сетях, но при этом реализуют три различных подхода к построению систем телефонной

сигнализации.

### 1.3.2. Набор рекомендаций H.323

Исторически первый и самый распространенный в настоящее время - это введенный Международным союзом электросвязи (МСЭ) набор рекомендаций H.323. H.323 стал плодом деятельности разработчиков протоколов мультимедийной связи в сетях ISDN (H.320). Первая версия этого протокола была принята МСЭ в 1996 году и, по сути, была попыткой перенести телефонную сигнализацию ISDN Q.931 на IP-соединения, "наложить" традиционную телефонию на сети передачи данных. Рекомендации H.323 достаточно подробно описывают способы организации мультимедийных конференций, охватывая сервисы передачи голоса, видео и компьютерных данных в пакетных сетях с негарантированной доставкой. К настоящему времени принята уже четвертая версия этого набора рекомендаций. К основным компонентам набора относятся описанные ниже протоколы.

H.225 - полный аналог протокола Q.931 в сетях ISDN; описывает процесс установления, поддержки и завершения соединения. Обмен сообщениями происходит по протоколу TCP.

RAS (Registration, Admission, Status) - отвечает за регистрацию устройств в сети, контроль доступа к ресурсам, контроль полосы пропускания, необходимой для сеанса связи, и контроль состояния устройств в сети. Работает по протоколу UDP. H.245 - отвечает за обмен информацией, необходимой для согласования параметров логических каналов для передачи медиа-потоков, то есть собственно голоса или видео. Сюда входит, к примеру, согласование кодеков, номеров UDP-портов и так далее. Обмен происходит по протоколу TCP.

H.450.x (появившийся в четвертой версии H.323) - отвечает за обеспечение таких дополнительных или интеллектуальных функций, как

Hold, Transfer и так далее.

Архитектура H.323 (рис.1.15) весьма проста и состоит всего из четырех функциональных компонентов, ни один из которых не является обязательным.

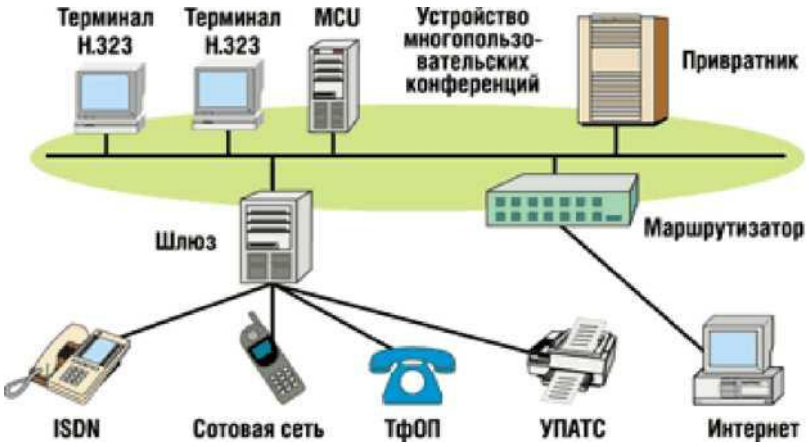


Рис.1.15. Архитектура H.323

Терминал (H.323 Terminal) - абонентское устройство, способное обеспечивать связь (голосовую, видео и т. д.) с другими терминалами, шлюзами или устройствами многопользовательских конференций.

Шлюз (H.323 Gateway) - центральное понятие IP-телефонии. Данное устройство обеспечивает взаимное сопряжение телефонной сети с IP-сетью. При этом предоставляется поддержка разных протоколов и интерфейсов сетей обоих типов. Если выход в телефонную сеть не требуется, то данный компонент не нужен, а терминалы могут связываться друг с другом напрямую.

Привратник (H.323 Gatekeeper, GK) - управляющий элемент H.323 сети, обеспечивающий ее масштабируемость, централизацию управления и настроек, а также трансляцию телефонных префиксов и идентификаторов (H.323 ID) в IP-адреса шлюзов или H.323 терминалов. Кроме того, привратник отвечает за управление доступом (Admission Control) при регистрации шлюзов и терминалов, контроль установления вызова (Call Admission Control), управление полосой пропускания и маршрутизацию вызовов. Привратник управляет подчиненной ему частью сети (зоной) через

RAS - протокол взаимодействия со шлюзами. Предусмотрено объединение привратников в группы, управлять которыми можно с помощью выделенного привратника - Directory Gatekeeper.

Устройство многопользовательских конференций (H.323 Multipoint Conference Unit, MCU) - управляет проведением многопользовательских конференций, согласует параметры соединения всех участников в режиме централизованной, децентрализованной или комбинированной конференции. Возможно переключение или смешивание медиа-потоков.

Обмен сообщениями между компонентами сети H.323 происходит в двоичном формате (ASN.1), для анализа которого нужен транслятор из двоичного формата в текстовый (ASN parser). В рекомендациях H.323 определено несколько различных способов адресации:

- телефонные номера в формате E.164, т. е. только символы из набора "0123456789#*,";
- H.323-идентификатор (H323-ID) - произвольный набор символов Unicode;
- универсальный идентификатор ресурса в формате URL (URL-ID);
- IP-адрес с номером порта, например, 10.2.3.4:1720;
- адрес электронной почты (Email-ID).

В наиболее общей форме сценарий соединения по протоколу H.323 выглядит как ряд последовательных шагов (рис.1.16). Вначале для установления соединения терминал обнаруживает привратника и регистрируется у него по протоколу RAS. Затем происходит установление сигнального канала по протоколам RAS и H.225. На следующем этапе выполняется согласование параметров оборудования, обмен информацией о его функциональных возможностях и открытие логических каналов по протоколу H.245. Только после этого происходит передача медиа-трафика по протоколам RTP/RTCP, а по ее окончании - завершение соединения.


Рис1.16. Сценарий соединения по протоколу H.323.

### 1.3.3. Протокол SIP

Следующий по распространенности протокол IP-телефонии - SIP (Session Initiation Protocol); он описан в рекомендациях RFC 2543. SIP регламентирует установление и завершение мультимедийных сессий - сеансов связи, в ходе которых пользователи могут говорить друг с другом, обмениваться видеоматериалами и текстом, совместно работать над приложениями и так далее. SIP и сопутствующие ему протоколы родились и развиваются в рамках IETF - главного органа стандартизации Интернета. Первая версия протокола SIP была принята в марте 1999 года, на три года позже, чем H.323, но благодаря интенсивному развитию этого направления сегодня набор рекомендаций RFC (базовых официальных документов IETF), имеющих отношение к SIP-архитектуре, насчитывает десятки, если не сотни документов.

SIP очень похож на протокол HTTP, поскольку разрабатывался по образу и подобию широко известных спецификаций HTTP и SMTP. По сути, это клиент-серверный протокол, работа которого состоит из череды запросов

и ответов, причем все SIP-заголовки передаются в формате ASCII-текста, а потому легко читаются. SIP позволяет использовать логическую адресацию (URL) на базе протокола TCP или UDP. Проще всего в качестве адреса в сети SIP задавать адреса электронной почты. При этом допускается применение разнообразных параметров, определяющих функциональность SIP-адреса или тип протокола связи. Например, можно указать, что соединение осуществляется с обычным телефонным номером сети общего пользования - sip:tel :+70957852525, и дополнить его добавочным номером postd=pp521, или определить параметры модемной связи - modem: +70957852526;type=v32b?7e1;type=v110.

SIP имеет несколько комплементарных протоколов, которые служат для реализации дополнительных возможностей. Наиболее важный из них - SDP (Session Description Protocol, RFC 2327), протокол согласования таких параметров сеанса связи, как виды кодеков, номера UDP-портов и так далее. SDP обеспечивает изменение параметров сеанса связинепосредственно во время сеанса. Перенос сообщений SDP основан на протоколе Session Announcement Protocol (SAP, RFC 2974).

Другой пример комплементарного протокола - SIMPLE (SIP for Instant Messaging and Presence Levering Extension). Фактически это расширение SIP, служащее для предоставления информации о событиях (presence) и для рассылки "мгновенных" сообщений (instant messaging).

Следует также упомянуть SIP-T (Trunk) - протокол переноса сообщений SS7 в виде MIME-объектов между контроллерами сигнализации, а также SIGTRAN (Signaling Transport)

- протокол переноса сообщений сигнализации SS7 через IP-сеть.

Архитектура SIP (рис.1.17) также очень проста и состоит из нескольких необязательных компонентов.

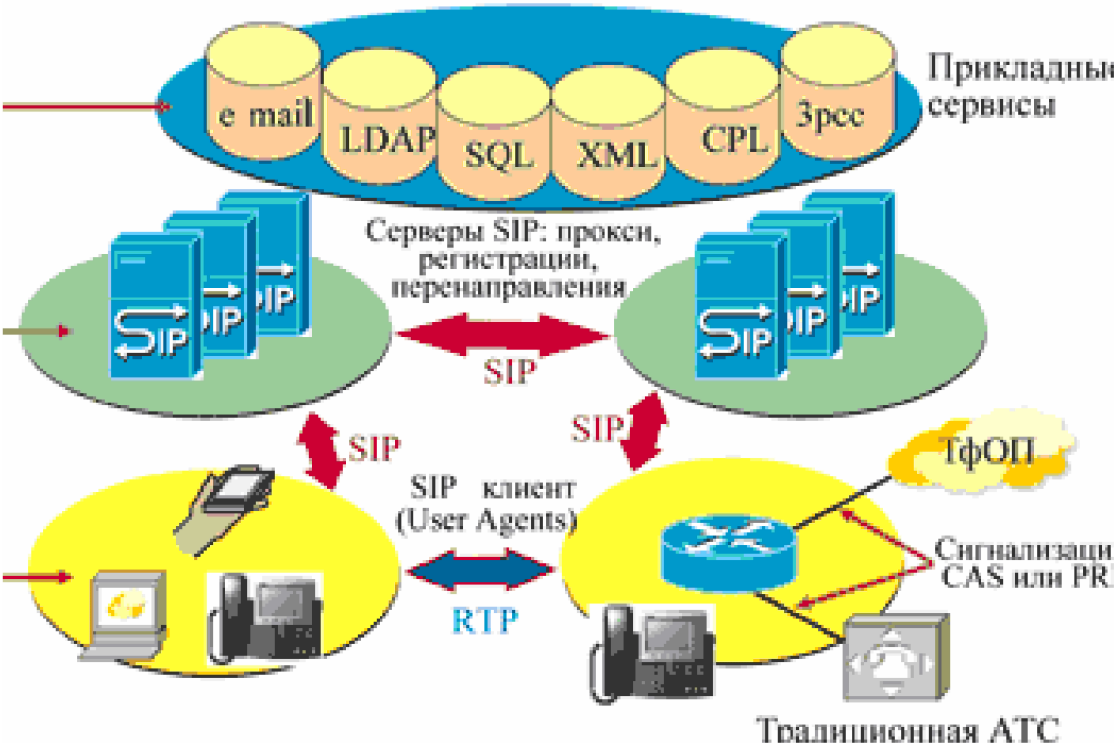


Рис.1.17. Архитектура SIP

Клиент SIP (SIP user agent) - может быть представлен как устройством (IP-телефон, шлюз или другой пользовательский терминал), так и программным приложением для ПК, PDA и т. д. Обычно SIP-клиент содержит и клиентскую, и серверную часть (User Agent Client, или UAC, и User Agent Server, или UAS). Основные функции данного компонента - инициирование и завершение вызовов.

Прокси-сервер SIP - управляет маршрутизацией вызовов и работой приложения. Прокси-сервер не может инициировать или терминировать вызовы.

Redirect-сервер SIP - перенаправляет звонки согласно заданным условиям.

Сервер регистрации SIP (registrar/location) - осуществляет регистрацию пользователей и ведет базу соответствия имен пользователей их адресам, телефонным номерам и так далее.

Еще один важный компонент реальных SIP-сетей, хотя и не входящий формально в архитектуру SIP, - Back-to-Back User Agent (B2BUA). Это

транслируется прокси-сервером. Вызываемому абоненту возвращается подтверждающее сообщение Ack.

своеобразный сервер, представляющий собой два соединенных друг с другом SIP-клиента и поэтому способный инициировать и завершать вызовы.

В наиболее общей форме сценарий соединения по протоколу SIP с участием прокси- сервера показан на рис. 1.18. Абонент посылает на прокси-сервер запрос на соединение, отправляя сообщение Invite. Прокси-сервер возвращает сообщение Trying и передает сообщение Invite вызываемому абоненту.

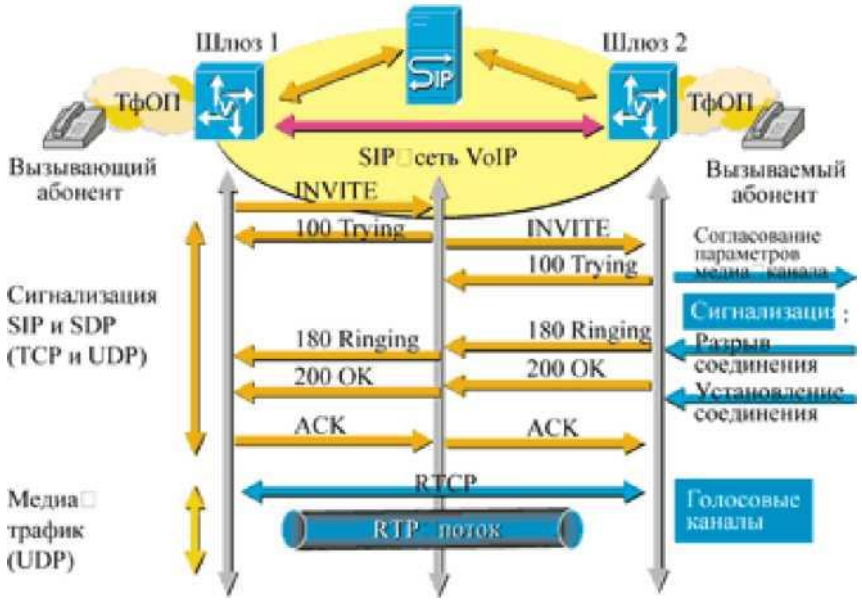


Рис1.18. Сценарий соединения по протоколу SIP

С этого момента соединение считается установленным и начинается обмен медиатрафиком по протоколам RTP/RTCP. Сторона, желающая завершить соединение, посылает сообщение Bye, и после получения подтверждающего OK соединение разрывается.

Этот сценарий очень прост, в нем не участвуют никакие другие серверы (Redirection, Registrar, Location), но он дает представление о схеме взаимодействия элементов SIP-сети.

### 1.3.4. Протокол MGCP

Последний из рассматриваемых протоколов IP-телефонии - MGCP (Media Gateway Control Protocol). Точнее, речь здесь идет не об одном протоколе, а о целой группе - SGCP, IPDC, MGCP, MEGACO, H.248. Эти спецификации не только очень схожи концептуально, но и являются "близкими родственниками".

История формирования MGCP началась с создания двух протоколов - SGCP (Simple Gateway Control Protocol, разработка Bellcore и Cisco Systems) и IPDC (Internet Protocol for Device Control, разрабатывался компанией Level 3 при участии многих производителей). Затем SGCP и IPDC были объединены в один протокол, получивший название MGCP. В дальнейшем эволюция MGCP привела к появлению протоколов MEGACO (в рамках IETF) и

H. 248 (в рамках МСЭ).

Первая версия протокола MGCP (RFC 2705) датирована октябрем 1999 года. Интересно отметить, что MGCP - единственный из трех описываемых здесь протоколов, в работе над которым IETF и МСЭ сотрудничают; именно в результате этого взаимодействия и были созданы протоколы MEGACO и H.248. В то же время существуют и другие реализации MGCP-подобных протоколов, например, собственный протокол Cisco Systems SSCP (Skinny Station Control Protocol), с помощью которого УАТС Cisco Call Manager управляет IP- телефонами.

Основная идея MGCP состоит в том, что управление сигнализацией (Call Control) сосредоточено на центральном управляющем устройстве, называемом контроллером сигнализаций (Call Agent, CA), и полностью отделено от медиа-потоков (bearer). Эти потоки обрабатываются шлюзами или абонентскими терминалами, которые способны исполнять лишь ограниченный набор команд, исходящих от управляющего устройства. Архитектура протокола MGCP-сети также очень проста (рис. 1.19), в ней

выделяются всего два функциональных компонента. Первый может быть представлен шлюзом (Media Gateway, MG) или IP-телефоном, а второй - устройством управления вызовами, которое может называться контроллером сигнализаций (CA), контроллером шлюза (Media Gateway Controller, MGC) или программным контроллером (Softswitch, SS). Иногда контроллер сигнализаций представляют в виде двух компонентов - собственно контроллера (Call Agent), выполняющего функции управления шлюзами, и шлюза сигнализации (Signaling Gateway), обеспечивающего обмен сигнальной информацией и согласование между традиционной телефонной сетью и сетью IP.

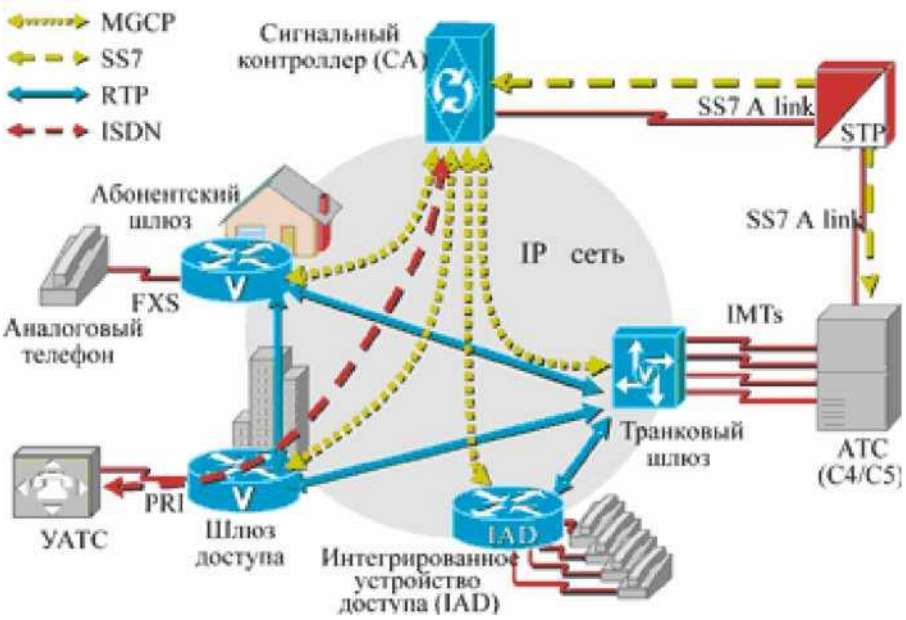


Рис1.19. Архитектура MGCP

Контроллеры обмениваются со шлюзами (или IP-телефонами) данными в простом текстовом формате (в случае H.248 возможен и бинарный обмен), а функциональное назначение каждого шлюза определяется набором команд, которые он "понимает". Манипулируя наборами команд, можно получать специализированные шлюзы: транковые (Trunking gateways, TGW), абонентские (Residential gateways, RGW), шлюзы доступа (Access gateways, AGW) и так далее.

Контроллер сигнализаций CA воспринимает сеть как набор двух

логических элементов

- устройств (end-points) и соединений (connections) между ними. Устройства могут быть физическими (например, IP-телефоны или линии на шлюзах) или виртуальными (например, линии к серверам голосовых сообщений). Соединения могут быть ориентированы на передачу голоса, факс-сообщений или данных. Управление этими элементами, т. е. организация соединений между устройствами, происходит путем посылки команд в виде текстовых (ASCII) сообщений по протоколу UDP - при этом может использоваться протокол SDP. Как правило, управляющие воздействия контроллера CA инициируются какими-то событиями (events).

Простейший сценарий соединения в концепции MGCP (рис. 25) будет выглядеть следующим образом. Пользователь телефона, подключенного к MGCP-шлюзу, снимает трубку, после чего шлюз сообщает контроллеру об этом событии, а CA дает команду шлюзу включить в телефонную линию сигнал готовности (dial-tone). Теперь пользователь слышит в трубке непрерывный гудок. Набор телефонного номера - тоже последовательность событий для контроллера. Анализируя эти события, CA может установить соединение с другим абонентом в IP-сети или в телефонной сети. Централизованная обработка сигнализации дает возможность контроллеру прозрачно транслировать сигнализацию SS7 или ISDN из телефонной сети в IP-сеть и, наоборот, получать соответствующие сигнальные сообщения, упакованные в IP-пакеты, а затем анализировать их и манипулировать голосовыми каналами на шлюзах.

### 1.3.5. Сравнение сигнальных протоколов

Сравнивая особенности развития и функциональные особенности трех видов протоколов (таблица 1.2), можно сделать вывод, что их различияобусловлены историческими причинами, в частности, изменениями представлений о пути развития телекоммуникаций в разное время. При этом

H.323 - это технологически устоявшийся, широко распространенный протокол IP-телефонии для операторских сетей и межоператорского обмена, "транзитный" протокол. В свою очередь, SIP - протокол предоставления расширенных голосовых услуг в IP-сетях, который продолжает быстро развиваться, "абонентский" протокол. Что касается MGCP, то он ориентирован, прежде всего, на организацию больших операторских узлов сопряжения IP-сетей с ТфОП и сетями SS7.

Табл. 1.2. Сравнение протоколов VoIP-сети

| Показатель | H.323 | SIP | MGCP |
|---|---|---|---|
| Клиент | Thick | Thick | Thin |
| Компонент, определяющий функциональность сети и сетевые сервисы | Привратник | Прокси-сервер | Сигнальный контроллер CA |
| Используемая модель | Телефонная (Q.931) | Интернет (WWW) | Централизованная |
| Протокол передачи сигнализации | TCP или UDP | TCP или UDP | UDP |
| Протокол передачи медиа-трафика | RTP | RTP | RTP |
| Формат сообщений | Двоичный (ASN.1) | Текстовый (ASCII) | Текстовый (ASCII) или двоичный |
| Стандартизирующая организация | ITU | IETF | IETF/ITU |

# 2. МЕТОДЫ АНАЛИЗА И ДИАГНОСТИКА ЛОКАЛЬНЫХ СЕТЕЙ

Очень часто под диагностикой локальной сети подразумевают тестирование только ее кабельной системы. Это не совсем верно. Кабельная система является одной из важнейших составляющих локальной сети, но далеко не единственной и не самой сложной с точки зрения диагностики. Помимо состояния кабельной системы на качество работы сети значительное влияние оказывает состояние активного оборудования (сетевых плат, коммутаторов и маршрутизаторов), качество оборудования сервера и настройки сетевой операционной системы. Кроме того, функционирование сети существенно зависит от алгоритмов работы эксплуатируемого в ней прикладного программного обеспечения.

Под термином "сеть" здесь подразумевается весь комплекс указанных выше аппаратных и программных средств; а под термином "диагностика сети" - процесс определения причин неудовлетворительной работы прикладного программного обеспечения (ПО) в данной сети. Именно качество работы прикладного ПО в сети оказывается определяющим с точки зрения пользователей [2]. Все прочие критерии, такие как число ошибок передачи данных, степень загруженности сетевых ресурсов, производительность оборудования и тому подобное, являются вторичными.

## 2.1. Методы анализа мультисервисных сетей

Основных причин неудовлетворительной работы прикладного ПО в сети может быть несколько: повреждения кабельной системы, дефекты активного оборудования, перегруженность сетевых ресурсов (канала связи и сервера), ошибки самого прикладного ПО. Часто одни дефекты сети маскируют другие. Таким образом, чтобы достоверно определить, в чем

причина неудовлетворительной работы прикладного ПО, локальную сеть требуется подвергнуть комплексной диагностике.

При возникновении неполадок работы сети поиск неисправности и ее устранение происходит в строгом соответствии с семиуровневой моделью сети ISO OSI. Последовательно проверяются на наличие ошибок уровни начиная с физического, после проверки каждого уровня проверяется вышележащий.

### 2.1.1. Организация диагностики локальной сети

В рамках предлагаемой методики не рассматривается ставшая хрестоматийной методика упреждающей диагностики сети. Не подвергая сомнению, важность упреждающей диагностики, следует заметить, что на практике она используется редко. Чаще всего (хотя это и неправильно) сеть анализируется только в периоды ее неудовлетворительной работы. В таких случаях локализовать и исправить имеющиеся дефекты сети требуется быстро. В данной работе основное внимание уделено диагностике канального уровня сети - поскольку это является первоочередной задачей при диагностике сети передачи данных.

Алгоритм поиска и устранения неисправности в общем виде состоит из восьми шагов (рис.2.1):

1. Определение проблемы;
2. Сбор необходимой информации;
3. Оценка возможных сценариев решения проблемы и определение наиболее вероятных причин неисправности;
4. Разработка плана решения проблемы;
5. Осуществление действий в соответствии с составленным планом;
6. Оценка результатов;
7. Повторение последовательности шагов, в случае, если неисправность не была устранена;

8. Документирование изменений после успешного устранения неисправности.


Рис. 2.1. Последовательность устранения неполадок в сети

### 2.1.2.Тестирование физического уровня

Полноценно кабельная система может быть протестирована только специальным прибором - кабельным сканером. Другого способа не существует. Не имеет смысла заниматься трудоемкой процедурой выявления дефектов сети, если их можно локализовать одним нажатием клавиши на кабельном сканере. При этом прибор выполнит полный комплекс тестов на соответствие кабельной системы сети выбранному стандарту. Следует учитывать, что стандартное тестирование не позволяет проверить уровень шума создаваемого внешним источником в кабеле. Это может быть шум от люминесцентной лампы, силовой электропроводки, сотового телефона,

мощного копировального аппарата и др. Для определения уровня шума кабельные сканеры имеют, как правило, специальную функцию. Поскольку кабельная система сети полностью проверяется только на этапе ее инсталляции, а шум в кабеле может возникать непредсказуемо, нет полной гарантии того, что шум проявится именно в период полномасштабной проверки сети на этапе ее инсталляции.

При проверке сети кабельным сканером вместо активного оборудования к кабелю подключаются с одного конца - сканер, с другого - инжектор. После проверки кабеля сканер и инжектор отключаются, и подключается активное оборудование: сетевые платы, концентраторы, коммутаторы.

### 2.1.3.Тестирование канального уровня

Любая методика тестирования сети существенно зависит от имеющихся в распоряжении системного администратора средств. В большинстве случаев необходимым и достаточным средством для обнаружения дефектов сети (кроме кабельного сканера) является анализатор сетевых протоколов.

Анализаторы могут быть подключены к коммутатору двумя способами.

При первом способе (рис.2.2) анализатор подключается к специальному порту (порту мониторинга или зеркальному порту) коммутатора, если таковой имеется, и на него по очереди направляется трафик со всех интересующих портов коммутатора.

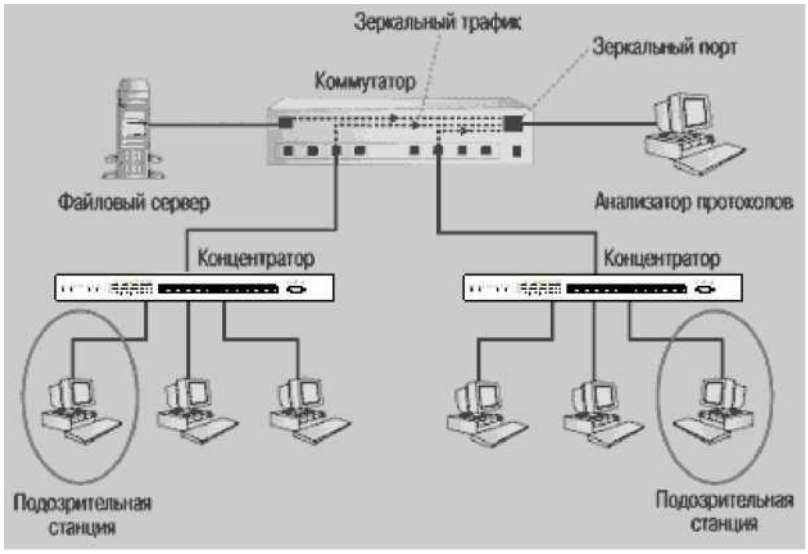


Рис.2.2. Подключение анализатора к порту мониторинга

Если в коммутаторе специальный порт отсутствует, то анализатор (или агент) следует подключать к портам интересующих доменов сети в максимальной близости к наиболее подозрительным станциям или серверу (рис.2.3). Иногда это может потребовать использования дополнительного концентратора. Однако такой способ практически не используется в настоящее время, поскольку современное оборудование предоставляет подробную информацию и позволяет применять первый способ подключения анализатора.

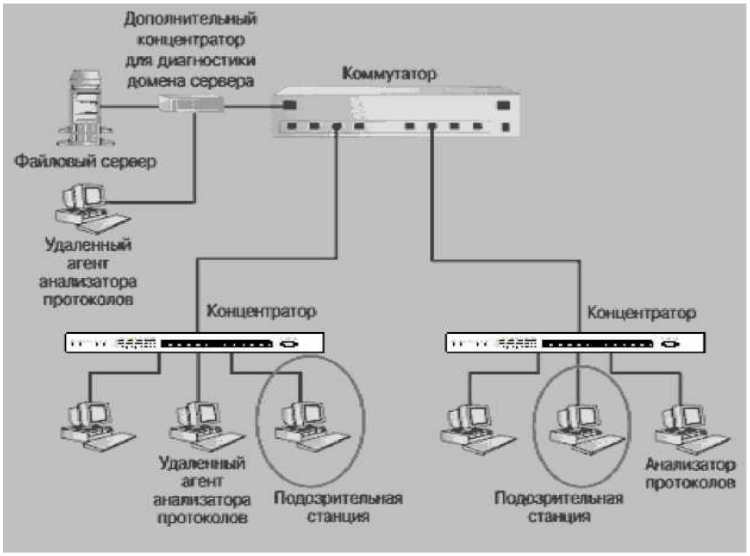


Рис.2.3. Подключение анализатора при отсутствии порта мониторинга

На рынке имеется множество разнообразных анализаторов протоколов от чисто программных до программно-аппаратных. Несмотря на функциональную идентичность большинства анализаторов протоколов, каждый из них обладает теми или иными достоинствами и недостатками. В связи с этим следует обратить внимание на две важные функции, без которых эффективную диагностику сети провести будет затруднительно. Во- первых, анализатор протоколов должен иметь встроенную функцию генерации трафика. Во- вторых, анализатор протоколов должен уметь отфильтровывать принимаемые кадры, то есть принимать не все кадры подряд, а, например, кадры определённого протокола. Если эта функция отсутствует, то при сильной загруженности сети, какой бы производительностью ни обладал компьютер, на котором установлен анализатор, последний будет терять кадры. Это особенно важно при диагностике быстрых сетей типа Fast Ethernet, FDDI и особенно Gigabit Ethernet.

### 2.1.4. Измерение утилизации сети и установление корреляции между замедлением работы сети и перегрузкой канала связи

Утилизация канала связи сети - это процент времени, в течение которого канал связи передает сигналы, или иначе - доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами. Параметр "Утилизация канала связи" характеризует величину загруженности сети.

Загруженность канала связи может влиять на время реакции прикладного программного обеспечения. И первоочередная задача состоит в определении наличия взаимозависимости между плохой работой прикладного программного обеспечения и утилизацией канала связи сети.

Многие источники упоминают о стандарте де-факто, в соответствии с которым для удовлетворительной работы сети Ethernet с общей шиной, утилизация канала связи "в тренде" (усредненное значение за 15 минут) не

должна превышать 20%, а "в пике" (усредненное значение за 1 минуту) - 35-40%. Приведенные значения объясняются тем, что в сети Ethernet при утилизации канала связи, превышающей 40%, существенно возрастает число коллизий и, соответственно, время реакции прикладного ПО. Несмотря на то, что такие рассуждения в общем случае верны, безусловное следование подобным рекомендациям может привести к неправильному выводу о причинах медленной работы программ в сети.

Если в сети Ethernet в любой момент времени обмен данными происходит не более чем между двумя компьютерами, то любая сколь угодно высокая утилизация сети является допустимой.

Высокая утилизация канала связи сети только в том случае замедляет работу конкретного прикладного ПО, когда именно канал связи является "узким местом" для работы данного конкретного ПО.

Кроме канала связи узкие места в системе могут возникнуть из-за недостаточной производительности или неправильных параметров настройки сервера, низкой производительности рабочих станций, неэффективных алгоритмов работы самого прикладного ПО.

В какой мере канал связи ответственен за недостаточную производительность системы, можно выяснить следующим образом. Выбрав наиболее массовую операцию данного прикладного ПО (например, для банковского ПО такой операцией может быть ввод платежного поручения), следует определить, как утилизация канала связи влияет на время выполнения такой операции.

Проще всего это сделать, воспользовавшись функцией генерации трафика. С помощью этой функции интенсивность генерируемой нагрузки следует наращивать постепенно, и на ее фоне производить измерения времени выполнения операции. Фоновую нагрузку целесообразно увеличивать от 0 до 50-60% с шагом не более 10%.

Если время выполнения операции в широком интервале фоновых нагрузок не будет существенно изменяться, то узким местом системы

является не канал связи. Если же время выполнения операции будет существенно меняться в зависимости от величины фоновой нагрузки (например, при 10% и 20% утилизации канала связи время выполнения операции будет значительно различаться), то именно канал связи, скорее всего, ответственен за низкую производительность системы, и величина его загруженности критична для времени реакции прикладного ПО. Зная желаемое время реакции ПО, легко можно определить, какой утилизации канала связи соответствует желаемое время реакции прикладного ПО.

В данном эксперименте фоновую нагрузку не следует задавать более 60%. Даже если канал связи не является узким местом, при таких нагрузках время выполнения операций может возрасти вследствие уменьшения эффективной пропускной способности сети.

### 2.1.5. Измерение числа коллизий в сети

Такой показатель как число коллизий становится неактуальным в настоящее время, поскольку практически повсеместно осуществлён переход на коммутируемую полнодуплексную среду передачи данных.

Если две станции коллизионного домена сети одновременно ведут передачу данных, то в домене возникает коллизия. Коллизии бывают трех типов: местные, удаленные, поздние.

Местная коллизия (local collision) - это коллизия, фиксируемая в коллизионном домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда источник передачи находится в домене.

В сетях 100BaseT (а также 10BaseT) станция определяет, что произошла локальная коллизия, если во время передачи кадра она обнаруживает активность на приемной паре $^{(Rx)}$.

Удаленная коллизия (remote collision) - это коллизия, которая возникает в другом физическом сегменте сети. Станция, работающая в полудуплексном

режиме, узнает, что произошла удаленная коллизия, если она получает неправильно оформленный короткий кадр с неверной контрольной последовательностью CRC, и при этом отсутствует одновременная активность на приемной и передающей парах (Tx и Rx).

Поздняя коллизия (late collision) - это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи первые 64 байт кадра. В сетях 10BaseT/100BaseT поздние коллизии часто фиксируются измерительными устройствами как ошибки CRC.

Даже если канал связи не является узким местом системы, коллизии несущественно, но замедляют работу прикладного ПО. Причем основное замедление вызывается не столько самим фактом необходимости повторной передачи кадра, сколько тем, что каждый компьютер сети после возникновения коллизии должен выполнять алгоритм отката (backoff algorithm): до следующей попытки выхода в канал связи ему придется ждать случайный промежуток времени, пропорциональный числу предыдущих неудачных попыток.

Следует учитывать, что не все измерительные приборы правильно определяют общее число коллизий в сети.

Практически все чисто программные анализаторы протоколов фиксируют наличие коллизии только в том случае, если они обнаруживают в сети фрагмент, то есть результат коллизии. При этом наиболее распространенный тип коллизий - происходящие в момент передачи преамбулы кадра (то есть до начального ограничителя кадра (SFD)) - программные измерительные средства не обнаруживают, так устроен набор микросхем сетевых плат Ethernet. Наиболее точно коллизии обнаруживают аппаратные измерительные приборы, например LANMeter компании Fluke.

Долю коллизий в общем числе кадров имеет смысл анализировать в момент активности подозрительных (медленно работающих) станций и только в случае, когда утилизация канала связи превышает 30%.

Коллизии в сети могут быть следствием перегруженности входных

буферов коммутатора. Следует помнить, что коммутаторы при перегруженности входных буферов эмулируют коллизии, искусственно понижая скорость передачи рабочих станций сети. Этот механизм называется "управление потоком" (flow control).

### 2.1.6. Измерение числа ошибок на канальном уровне сети

В сетях Ethernet наиболее распространенными являются следующие типы ошибок.

- Короткий кадр - кадр длиной менее 64 байт (после 8-байтной преамбулы) с правильной контрольной последовательностью. Наиболее вероятная причина появления коротких кадров - неисправная сетевая плата или неправильно сконфигурированный или испорченный сетевой драйвер;
- Ошибки контрольной последовательности (CRC error) - правильно оформленный кадр, но с неверной контрольной последовательностью (ошибка в поле CRC);
- Ошибка выравнивания (alignment error) - кадр, содержащий число бит, не кратное числу байт.
- Блики (ghosts) - последовательность сигналов, отличных по формату от кадров Ethernet, не содержащая разделителя (SFD) и длиной более 72 байт. Впервые данный термин был введен компанией Fluke с целью дифференциации различий между удаленными коллизиями и шумами в канале связи.

Блики являются наиболее коварной ошибкой, так как они не распознаются программными анализаторами протоколов по той же причине, что и коллизии на этапе передачи преамбулы. Выявить блики можно специальными приборами или с помощью метода стрессового тестирования сети.

Следует заметить, что степень влияния ошибок канального уровня сети на время реакции прикладного ПО сильно преувеличена.

В соответствии с общепринятым стандартом де-факто число ошибок канального уровня не должно превышать 1% от общего числа переданных по сети кадров. Как показывает опыт, эта величина перекрывается только при наличии явных дефектов кабельной системы сети.

Прежде чем анализировать ошибки в сети, следует выяснить, какие типы ошибок могут быть определены сетевой платой и драйвером платы на компьютере, где работает программный анализатор протоколов.

Работа любого анализатора протоколов основана на том, что сетевая плата и драйвер переводятся в режим приема всех кадров сети (promiscuous mode). В этом режиме сетевая плата принимает все проходящие по сети кадры, а не только широковещательные и адресованные непосредственно к ней, как в обычном режиме. Анализатор протоколов всю информацию о событиях в сети получает именно от драйвера сетевой платы, работающей в режиме приема всех кадров.

Не все сетевые платы и сетевые драйверы предоставляют анализатору протоколов идентичную и полную информацию об ошибках в сети. Сетевые платы 3Com вообще не выдают никакой информации об ошибках. Если установить анализатор протоколов на такую плату, то значения на всех счетчиках ошибок будут нулевыми.

EtherExpress Pro компании Intel сообщают только об ошибках CRC и выравнивания. Сетевые платы компании SMC предоставляют информацию только о коротких кадрах. NE2000 выдают почти полную информацию, выявляя ошибки CRC, короткие кадры, ошибки выравнивания, коллизии.

Сетевые карты D-Link и Kingstone сообщают полную, а при наличии специального драйвера - даже расширенную, информацию об ошибках и коллизиях в сети.

Для выявления ошибок на канальном уровне сети измерения необходимо проводить на фоне генерации анализатором протоколов собственного трафика. Генерация трафика позволяет обострить имеющиеся проблемы и создает условия для их проявления. Трафик должен иметь

невысокую интенсивность (не более 100 кадров/с) и способствовать образованию коллизий в сети, то есть содержать короткие (<100 байт) кадры.

При выборе анализатора протоколов или другого диагностического средства внимание следует обратить, прежде всего, на то, чтобы выбранный инструмент имел встроенную функцию генерации трафика задаваемой интенсивности.

При первом проведении диагностике и наличии в ней проблем, не следует ожидать, что дефектен только один компонент.

Отсутствие ошибок на канальном уровне еще не гарантирует того, что информация сети не искажается. В начале данного раздела уже упоминалось, что влияние ошибок канального уровня на работу сети сильно преувеличено. Следствием ошибок нижнего уровня является повторная передача кадров. Благодаря высокой скорости сети Fast Ethernet и высокой производительности современных компьютеров, ошибки нижнего уровня не оказывает существенного влияния на время реакции прикладного ПО.

Таким образом, основная задача диагностики канального уровня сети - выявить наличие повышенного числа коллизий и ошибок в сети и найти взаимосвязь между числом ошибок и степенью загруженности канала связи. Все измерения следует проводить на фоне генерации анализатором протоколов собственного трафика.

Методика упреждающей диагностики заключается в следующем. Администратор сети должен непрерывно или в течение длительного времени наблюдать за работой сети. Такие наблюдения желательно проводить с момента ее установки. На основании этих наблюдений администратор должен определить, во-первых, как значения наблюдаемых параметров влияют на работу пользователей сети и, во-вторых, как они изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и так далее.

Наблюдаемыми параметрами обычно являются:

- параметры работы канала связи сети - утилизация канала связи,

число принятых и переданных каждой станцией сети кадров, число ошибок в сети, число широковещательных и многоадресных кадров и так далее;

- параметры работы сервера - утилизация процессора сервера, число отложенных (ждущих) запросов к диску, общее число кэш-буферов, число "грязных" кэш-буферов и так далее.

Зная зависимость между временем реакции прикладного ПО и значениями наблюдаемых параметров, администратор сети должен определить максимальные значения параметров, допустимые для данной сети. Эти значения вводятся в виде порогов (thresholds) в диагностическое средство. Если в процессе эксплуатации сети значения наблюдаемых параметров превысят пороговые, то диагностическое средство проинформирует об этом событии администратора сети. Такая ситуация свидетельствует о наличии в сети проблемы.

Наблюдая достаточно долго за работой канала связи и сервера, можно установить тенденцию изменения значений различных параметров работы сети (утилизации ресурсов, числа ошибок и тому подобное). На основании таких наблюдений администратор может сделать выводы о необходимости замены активного оборудования или изменения архитектуры сети .

## 2.2. Способы диагностирования локальных сетей.

На протяжении ряда лет большинство вопросов повышения производительности и надежности сетей решалось закупкой новой техники. Не всегда подобное решение было технически и экономически обоснованно, но почти всегда оно позволяло достигнуть желаемой цели — сеть начинала работать быстрее и лучше. При наличии 200% запаса пропускной способности практически все "узкие места" можно без труда "расширить", а приобретая только самое дорогое оборудование лидеров сетевых технологий, вы можете с большой степенью вероятности обезопасить себя от "скрытых

дефектов". Сегодня ситуация изменилась, и экономическое обоснование проектов по модернизации сетей становится актуальным. Мировой опыт показывает, что инвестиции в профессионализм специалистов дают большую отдачу, чем инвестиции в "железо", даже очень хорошее. Необходимую пропускную способность сети или ее надежность нельзя оценить без детального анализа ее нынешнего состояния. Это можно сделать только посредством диагностических средств и методов тестирования компьютерных сетей.

Диагностические средства, предназначенные для компьютерных сетей, можно классифицировать по двум основным признакам:

- Средство, предназначенное для диагностики сети или для тестирования сети;

- Средство, предназначенное для реактивной диагностики или для упреждающей диагностики.

Под диагностикой сети принято понимать измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы операторов). Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки (утилизации) ресурсов сети или времени реакции прикладного ПО, которую администратор сети должен осуществлять ежедневно.

Диагностика бывает двух типов: упреждающая (proactive) и реактивная (reactive). Упреждающая диагностика должна проводиться в процессе эксплуатации сети ежедневно. Основная цель упреждающей диагностики — предотвращение сбоев в работе сети. Реактивная диагностика выполняется, когда в сети уже произошел сбой и надо быстро локализовать источник и выявить причину.

Для того чтобы проверить соответствие качества кабельной системы требованиям стандартов, определить максимальную пропускную способность сети или оценить время реакции прикладного программного обеспечения (ПО) при изменении параметров настройки коммутатора или

операционной системы (ОС), то такие измерения можно сделать только при отсутствии в сети работающих пользователей. В этом случае правильно употреблять термин "тестирование" сети. Таким образом, тестирование сети — это процесс активного воздействия на сеть с целью проверки ее работоспособности и определения потенциальных возможностей по передаче сетевого трафика.

Тестирование можно условно разделить на несколько видов в зависимости от цели, ради которой оно проводится. Это тестирование системы сети в соответствии со стандартами TIA/EIA TSB-67 состоит из стрессового тестирование конкретных сетевых устройств. Оно проводится с целью проверки устойчивости их работы при различных уровнях нагрузок, и различных типах сетевого трафика. Тестирование ПО осуществляется для определения его требований к пропускной способности сетевых ресурсов. Стрессовое тестирование сети (конкретных сетевых конфигураций) проводится с целью выявления "скрытых дефектов" в оборудовании и "узких мест" в архитектуре сети, а также с целью определения пороговых значений трафика, допустимых в данной сети.

Тестирование прикладного ПО, с целью определения требований к пропускной способности сетевых ресурсов, проводят компании-разработчика ПО. Такое тестирование осуществляется в рамках комплексной проверки ПО. Оно проводится перед выпуском его на рынок, и называется тестированием на соответствие качеству (Quality Assurance Test, QAT)

Стрессовое тестирование сетевых устройств обычно проводится независимыми специализированными лабораториями. Примерами таких лабораторий являются организации LANQuest и Data Communications. Чаще всего стрессовое тестирование устройств проводится с целью проверки заявленных технических характеристик и выявления различного рода дефектов.

Средства, предназначенные для диагностики сетей, можно условно разделить на две категории в зависимости от принципа их работы: средства

мониторинга и управления работой сети (далее средства мониторинга — monitoring software) и анализаторы сетевых протоколов (далее анализаторы протоколов — analyzers).

Принцип работы средств мониторинга основан на взаимодействии консоли оператора с так называемыми агентами, которые, собственно, и занимаются мониторингом и управлением работой устройств сети. Примерами средств мониторинга являются программы Transcend компании 3Com, Optivity компании Bay Networks (ныне Nortel), HP OpenView Net Metrix. Агенты могут быть встроены в оборудование или загружены программным образом. Поскольку наиболее распространенным протоколом общения консоли оператора и агентов является SNMP, такие агенты часто называют SNMP-агентами. SNMP- агенты могут выполнять самые различные функции, в зависимости от типа баз управляющей информации (Management Information Base, MIB), которые они поддерживают. Эти функции могут включать в себя управление конфигурацией устройства, в которое агенты встроены (configuration management), управление контролем доступа к информации (security management), анализ производительности устройства (perfomance management), измерение числа ошибок при передаче данных (fault management) и другие.

При реактивной диагностике сети с помощью средств мониторинга измерительным прибором является SNMP-агент самого диагностируемого устройства. Однако при появлении сбоев показания SNMP-агента нельзя считать достоверными. Это особенно актуально, когда сбои происходят в самом устройстве с установленным SNMP-агентом. В таких случаях наблюдатель должен быть "независим" от диагностируемого устройства. SNMP-агент устройства наблюдает за коллизионным доменом сети всегда только из одной точки и, что особенно важно, для реактивной диагностики, не имеет возможности производить генерацию тестового трафика. В результате если не все оборудование имеет встроенные агенты, то часть ошибок канального уровня в домене сети может не фиксироваться.

С точки зрения реактивной диагностики, т. е. возможности быстрой локализации дефектов в сети, применение анализаторов сетевых протоколов оказывается предпочтительным. Они представляют собой значительно более мощное средство по сравнению со средствами мониторинга сети, так как лишены всех перечисленных выше недостатков. Именно возможность эффективного проведения реактивной диагностики является сегодня актуальной задачей для администраторов сетей Принцип работы анализатора протоколов отличается от принципа работы средства мониторинга сети. Анализатор сетевых протоколов исследует весь проходящий мимо него сетевой трафик. Локальные сети по своей природе являются широковещательными, т. е. каждый кадр от любой станции в пределах коллизионного домена видят все станции этого домена сети. Подключая анализатор к любой точке коллизионного домена сети, вы будете видеть весь трафик в этом домене.

Анализаторы протоколов предоставляют возможность собирать данные о работе протоколов всех уровней сети и, в большинстве случаев, способны производить генерацию тестового трафика в сеть. Имея большой буфер для сбора пакетов, анализаторы протоколов позволяют быстро локализовать причину сбоя в сети: например, обнаружить факт перегрузки конкретного сервера, бесследное исчезновение пакетов транспортного уровня на неисправных сетевых платах, коммутаторах и маршрутизаторах, IP-пакеты с неправильной контрольной суммой, дубликаты IP- адресов и многое другое.

Анализаторы протоколов можно разделить на две категории: программные и аппаратные (или программно-аппаратные). Программный анализатор

— это программа, которая устанавливается на компьютер с обычной сетевой платой. Анализатор протоколов переводит сетевую плату компьютера в режим приема всех пакетов (promiscous mode). Примерами программных анализаторов протоколов являются Observer и Distributed Observer компании Network Instruments, NetXray компании Network

Associates, LANalyzer for Windows компании Novell и многие другие.

Использование всевозможных методов тестирования и диагностирования компьютерных сетей позволяет своевременно выявить ошибки в работе сети, что позволит значительно повысить эффективность работы компьютерных сетей, а также увеличить эксплуатационный срок.

## 2.3. Построения мультисервисной сети передачи данных.

### 2.3.1. Схема сети. Оборудование. Настройки.

В соответствии с необходимостью составления исходных документов для обеспечения работ по построению корпоративной мультисервисной сети пресс-центра Российско- Германского саммита, первоочередной задачей было построение логической схемы сети передачи данных.

При построении сети имели место следующие исходные требования:

1. Обеспечение 30 рабочих мест журналистов пресс-центра стационарным компьютерным оборудованием с доступом к сети Internet;
2. Обеспечение возможности беспроводного (WiFi) подключения портативных компьютеров к локальной сети с возможностью доступа к сети Internet;
3. Обеспечение резерва проводных подключений для портативных компьютеров, не оборудованных соответствующими адаптерами беспроводных сетей;
4. Обеспечение проводной и беспроводной (WiFi) телефонной связи для технических сотрудников с сохранением их рабочих телефонных номеров;
5. Простота и удобства подключения новых хостов к сети;
6. Обеспечение высокой надёжности и производительности сети.

В соответствии с требуемой функциональностью было принято

решение использовать следующее оборудование:

- маршрутизатор - Cisco 2811 Integrated Services Router
- коммутатор - Cisco 2960 Catalyst Switch
- точки приема - Cisco Aironet 1231 Access Point

### 2.3.2.Cisco 2811 Router

Она обеспечивает производительность различных услуг, таких как, передача потокового голоса. Обеспечивает безопасность на скорости носителя. Обладает высокой производительностю системы. Поддерживает информацию более 90 существующих и вновь создаваемых, модулей. Имеет 2 интегрированных порта 10/100 Fast Ethernet; опциональную поддержку PoE (Power over Ethernet - питание по Ethernet). Обладает встроенным шифрованием, осуществляет поддержку SDM (Security Device Manager), обеспечивает простоту управления. Осуществляет поддержку до 1500 VPN туннелей при использовании модуля AIM-EPII-PLUS. Антивирусная защита происходит с помощью NAC (Network Admission Control); функции обнаружения и предотвращения вторжения - система IPS (Intrusion Preventing System); ункции программного межсетевого экрана (IOS Firewall); поддержка аналоговых и цифровых голосовых звонков; опциональная поддержка голосовой почты; опциональная поддержка Cisco CME (CallManager Express) для локальной обработки вызовов (до 36 IP-телефонов); опциональная поддержка SRST (Survivable Remote Site Telephony) для локальной поддержки голосовых вызовов (до 36 IP-телефонов).

### 2.3.3. Cisco 2960 Catalyst Switch

- интегрированная безопасность, включая NAC (Network Admission Control); поддержка QoS; 48 интегрированных портов 10/100 Fast Ethernet;
- 2 интегрированных порта Gigabit Ethernet.

Cisco AiroNet 1231 Access Point:

поддержка стандартов IEEE 802.11a/b/g; поддержка питания по Ethernet; поддержка средств управления; интегрированные функции безопасности.

В соответствии с приведёнными требования была разработана сеть, схема которой представлена на рис2.4.

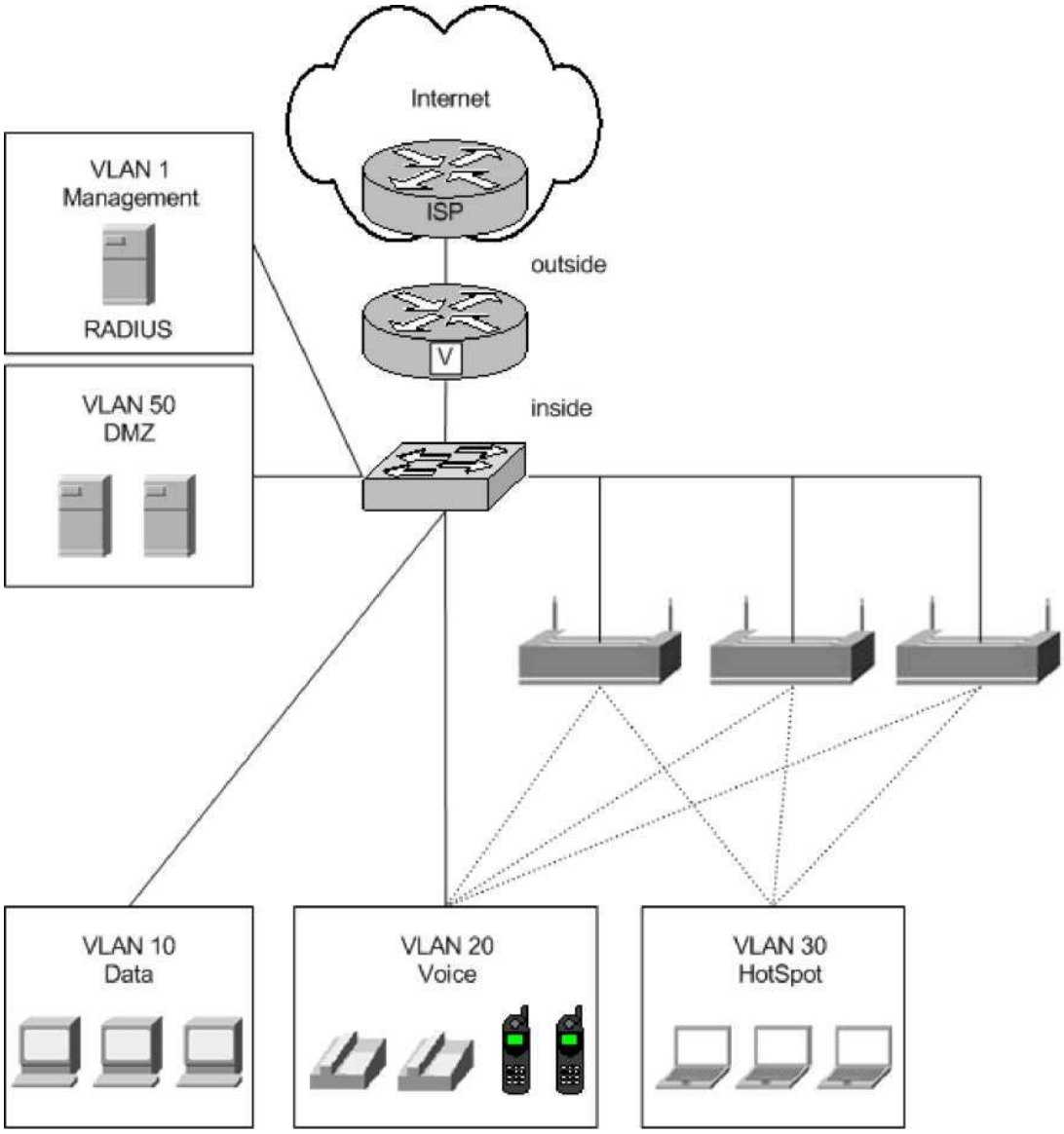


Рис.2.4. Схема сети Российско-Германского саммита

Маршрутизатор выполняет функции маршрутизации трафика между VLAN-ами, отвечает за управление установлением соединения телефонных вызовов, является межсетевым экраном и обеспечивает контроль внутреннего и внешнего трафика.

Коммутатор осуществляет подключение точек приема, устройств уровня доступа (рабочие станции и IP-телефоны), организует виртуальные ЛВС, предоставляет функции QoS, обеспечивает безопасность на уровне портов.

Точки приема осуществляют подключение устройств уровня доступа (рабочие станции и IP-телефоны), предоставляет функции QoS и безопасности.

Схема адресации сети приведена в таблице 2.1.

Табл. 2.1. Схема адресации сети

| № | Название | Адрес | Описание |
|---|---|---|---|
| VLAN 1 | Management | 192.168.0.0/24 | Управляющий доступ к оборудованию производится только из Management VLAN, здесь же располагается RADIUS сервер. |
| VLAN 10 | Data | 192.168.10.0/24 | Сеть для стационарных рабочих станций по кабельному подключению |
| VLAN 20 | Voice | 192.168.20.0/24 | Сеть для голосового трафика (кабельные и радио IP-телефоны) |
| VLAN 30 | HotSpot | 192.168.30.0/24 | Сеть беспроводного доступа для журналистов с портативными компьютерами |
| VLAN 40 | Unused | | VLAN для неиспользуемых портов коммутатора (как составной компонент системы безопасности) |

| | | | |
|---|---|---|---|
| VLAN 50 | DMZ | 217.80.159.0/29 | Сеть для серверов публичного доступа (в частности, Proxy-сервер). |

В соответствии с данной схемой, на локальном маршрутизаторе устанавливается программное обеспечение, осуществляющее маршрутизацию звонков. Данная модель маршрутизатора позволяет устанавливать Cisco Call Manager Express, который поддерживает до 36 IP-телефонов.

Таким образом, схема представляет собой распределенную систему, обеспечивающую локальную обработку вызовов с обеспечением необходимых механизмов качества сервиса (QoS).

В такой схеме единственный сервер CallManager, управляет установлением телефонных соединений и функционированием телефонных аппаратов, расположенных в пределах локальной IP сети.

Основные характеристики предложенной модели построения сети IP телефонии:

• для подключения к телефонной сети общего пользования (ТФОП), подключения аналоговых телефонов и факсовых аппаратов и стыковки с существующими УАТС могут использоваться голосовые шлюзы;

• в пределах локальной сети возможно использование кодека G.711 (несжатый голос);

• для экономного использования полосы пропускания на каналах WAN может быть использовано сжатие голоса;

• Cisco CallManager контролирует использование полосы пропускания на каналах WAN между удаленными офисами и принимает решение о разрешении/запрете установления телефонного соединения на основе информации о наличии свободной полосы пропускания (call admission control);

• поддержка механизмов обеспечения качества сервиса (QoS) в

пределах распределенной IP сети является критично важной для обеспечения качественной работы различных приложений (это особенно важно для голосовых приложений).

Подключение проводных IP телефонов к сети передачи данных осуществляется посредством одного кабеля (рис. 16), что обеспечивает простоту установки, отсутствие дополнительного расхода портов коммутатора и необходимости изменение кабельной инфраструктуры. При этом предполагается разнесение рабочих станций и телефонных аппаратов в различные виртуальные локальные сети, что позволит обеспечивать требуемое качество обслуживания и увеличит безопасность.

Для подключения проводных IP телефонов к электрической сети предполагается использовать технологию Inline Power, что обеспечит следующие преимущества: во-первых, не потребуется локальная розетка электропитания для каждого телефонного аппарата, и, во- вторых, этот способ также позволяет централизовать средства управления и обеспечения надёжности электропитания.

Поскольку требуется обеспечение надёжной работы телефонной сети при сбоях электропитания (до 4 часов работы в автономном режиме), используются источники бесперебойного питания (UPS); при этом UPS могут использоваться только для коммутаторов, поддерживающих технологию Inline Power и других важных сетевых устройств и серверов (в том числе сервера Call-Manager).

После установки и подключения оборудования, потребовалось провести его настройку, в соответствии с требования к сети. Помимо базовых настроек первоочередное значение имели настройки безопасности [7].

В рамках обеспечения безопасности были отключены все неиспользуемые службы. В том числе различные TCP и UDP сервисы, служба finger (по которой можно получить некоторую конфиденциальную информацию), отключен протокол bootp, отключен snmp, так как его использование не предполагалось: no service finger no service pad no service

tcp-small-servers no service udp-small-servers no snmp-server no ip bootp server

Также была отключена маршрутизация по адресу источника - no ip source-route.

Ряд служб следовало включить:

- Шифрование паролей;
- Входящие и исходящие TCP keepalive сообщения;
- Службу временных отметок (необходимо для датирования лог-информации);
- Службу простановки sequence number в лог сообщениях;
- CEF (Cisco express forwarding - необходимо для работы RPF - reverse pass forwarding).

service password encryption service tcp-keepalives-in service tcp-keepalives-out

service timestamps debuf datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec service sequence-numbers ip cef

Были настроены информационные баннеры, появляющиеся при входе на устройство: banner # <message> # banner motd # <message> # banner login # <message> #

В качестве сообщения, выводимого в баннере, было использовано одно из рекомендуемых: “Authorized access only! This system is the property of <company name>. Disconnect IMMEDIATELY as you are not an authorized user! Contact <administrator email address> <administrator phone number>”.

Так же были наложены ограничения на возможные пароли и включен учет ошибочных попыток аутентификации:

security passwords min-length 8

security authentication failure rate 3 log

Заданы параметры сбора лог-информации: logging on

logging 192.168.5.100 ! log-server logging console critical logging trap debugging logging buffered 32000

На интерфейсной базе:

- Отключены направленные широковещания.
- Отключен proxy-arp.
- Отключены перенаправления.
- Включена опция обратной проверки (RPF - reverse pass forwarding).

no ip directed-broadcast no ip proxy-arp no ip redirects

ip verify unicast reverse-path

Использования RPF является крайне важным моментом, так как это частично помогает бороться со спуффингом IP адресов. Суть данной технологии заключается в том, что маршрутизатор проверяет, на правильном ли интерфейсе получен пакет с данным адресом источника. Если согласно маршрутизирующей информации сеть источника находиться за другим интерфейсом, пакет отбрасывается. Проверка происходить не по таблицам маршрутизации, так как это требует значительных временных затрат, а по специальной базе данных, созданной CEF.

Также требовалось настроить IP телефонию. Поскольку телефоны в данной сети должны были получать IP адреса автоматически, первоочередной задачей было создание адресного пула для IP телефонов (данный пул создаётся для VLAN Voice отдельно от адресных пулов для клиентских рабочих станций - VLAN Data, HotSpot): ip dhcp excluded-address 192.168.20.0 192.168.3.10 ip dhcp excluded-address 192.168.20.250 192.168.3.254 ip dhcp pool IpPhones network 192.168.20.0 255.255.255.0 option 150 ip 192.168.20.254 default-router 192.168.20.254

Данный пул DHCP, помимо информации об адресе, выделенном клиенту, предоставляет клиентскому телефону информацию об адресе tftp-сервера, содержащего конфигурационные файлы для телефонов и файлы firmware для проводных IP телефонов.

Для доступа к телефонам за пределами локальной сети были определены правила трансляции номеров:

voice translation-rule 10

rule 1 /^3822\( \)/ /\1/

rule 2 /\(... \)/ /8\1/

voice translation-rule 20 rule 1 /^3822555555/ /103/ rule 2 /^3822777777/ /105/ voice translation-profile Filter_3822 translate calling 10 translate called 20

translate redirect-called 20

### 2.3.4. Настройка сервисов IP-телефонии

Включение IP телефонии - telephony-service.

Определение firmware файлов для различных моделей телефонов: load 7960-7940 P00307010200 load 7914 S00104000100

Указание максимального числа телефонов и максимального числа номеров директорий: max-ephones 30 max-dn 150

Задание адреса интерфейса и порта, использующегося Cisco Call Manager-ом: ip source-address 192.168.20.254 port 2000

Определение форматы даты и системного сообщения:

time-format 24

date-format dd-mm-yy

system message Elecs.Com Ltd.

Создание конфигурационных файлов - create cnf-files version-stamp 7960 Apr 21 2006 16:54:19.

Задание максимального числа одновременно идущих конференций - max-conferences 4. Определение музыкальной заставки проигрываемой при удержании звонка - moh music- on-hold.au.

Кроме этого достаточно было задать номера директорий для телефонов (ephone-dn) и определить сами IP телефоны (ephone): ephone-dn 1 dual-line number 101 label XXX

description XXX-phone transfer-mode consult

ephone 1 username "xxx" mac-address 000F.8FFB.A548 type 7960 button 1:11 2m1

# 3. СОЗДАНИЕ МУЛЬТИСЕРВИСНОЙ СЕТИ СКОРОСТНОГО УЧАСТКА ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА УЗБЕКИСТАНА

## 3.1. Построение групповых каналов E1 с использованием технологи Cisco MLPPP(Multi Link PPP)

Построение групповых каналов E1 основанная на использования технологи Cisco MLPPP(Multi Link PPP) предусматривает применение аппаратуры оперативно-технологической связи типа ДСС. Такая аппаратура предназначена для построения цифровой сети ОТС на магистральном, дорожном, отделенческом и станционном уровнях административного управления технологическими процессами всех подразделений железнодорожного транспорта. Аппаратура ДСС обеспечивает взаимодействие с аналоговыми сетями ОТС. На базе аппаратуры ДСС можно строить коммутационные станции ОТС (КС) распорядительного (КС-Р), исполнительного (КС-И) и комбинированного (КС-РИ) типов. КС, построенная на базе аппаратуры ДСС, включает в себя мультиплексор выделения и транзита каналов (МВТК), устройство коммутации (УК) и пульты оперативной связи (ПОС). В крупных узлах (например, в узлах с ЕДЦУ) в состав КС входит устройство коммутации и синхронизации (УКС), объединяющее несколько УК.

В работе составляется схема участков, на которой, в дополнении к приведенной в задании топологии участков железной дороги, предусматриваются промежуточные ж.д. станции на каждом участке. Промежуточные ж.д. станции расставляются через 5…15 км. Каждой промежуточной ж.д. станции присваивается наименование, состоящее из наименования одной из крупных станций участка и некоторого числа. Наименования промежуточных ж.д. станций не должны совпадать. На всех

участках на схеме указывается длина перегонов. Пример схемы участков железной дороги приведён на рис.3.1.

При проектировании должны быть предусмотрены следующие виды ОТС:

диспетчерская связь:

– поездная диспетчерская (ПДС) вместе с поездной радиосвязью (ПРС);

– энергодиспетчерская (ЭДС);

– служебная диспетчерская (СДС);

– линейно-путевая (ЛПС);

– перегонная связь (ПГС);

– межстанционная связь (МЖС);

– станционно-распорядительная связь (СРТС), включая стрелочную связь.

Все поездные диспетчеры (ДНЦ) находятся в ЕДЦУ. Для каждого ДНЦ организуются два круга: ПДС и ПРС. На рабочем месте одного ДНЦ устанавливаются два пульта оперативной связи распорядительного типа – ПОС-Р для ПДС и ПРС. При организации ПДС на каждой ж.д. станции у дежурного по станции (ДСП) следует предусмотреть установку одного пульта исполнительного типа – ПОС-И и одного базового модуля (БМ) с мобильным телефоном (ТА-М). В круг ПРС на каждой ж.д. станции включается стационарная радиостанция (Р/ст).

Круги ЭДС, СДС и ЛПС организуются самостоятельно. СДС и ЛПС организуются на всех участках железной дороги. ЭДС организуется на электрифицированных участках железной дороги. Электрифицированные участки задаются самостоятельно. Электрифицированными принимаются обязательно участки магистрали. Рекомендуется внутри отделения железной дороги организовать по два-три круга ЭДС, СДС и ЛПС. Диспетчеры ЭДС, СДС и ЛПС находятся в отделениях дороги. У каждого диспетчера

устанавливается пульт ПОР-Р. Поскольку места нахождения исполнительных абонентов ЭДС, СДС и ЛПС заданием не определены, они задаются самостоятельно. Допускается, чтобы на каждой ж.д. станции находилось по одному абоненту ЭДС, СДС и ЛПС. Каждый исполнительный абонент ЭДС, СДС и ЛПС пользуется аналоговым телефонным аппаратом с тангентой (ТА-Т).

ПГС и МЖС организуются на каждом перегоне для связи двух смежных станций. МЖС служит для связи между ДСП смежных станций. При проектировании ПГС и МЖС на каждом участке должны быть использованы по две физических цепи электрического кабеля, включаемых в коммутационные станции. При соединениях по цепям ПГС и МЖС ДСП пользуются пультами ПОС-И. Кроме того, в качестве резерва должна быть запроектирована МЖС, с организацией одного коммутируемого канала между каждой парой смежных ж.д. станций. Для коммутируемого канала внутри канала Е1 выделяется один канальный интервал (КИ).

При проектировании СРТС в проекте следует самостоятельно задаться количеством исполнительных абонентов и руководителей СРТС для каждой ж.д. станции. На промежуточной станции руководителем является только ДСП. На других станциях, кроме ДСП, могут быть иные руководители, не относящиеся к диспетчерским видам связи. У каждого исполнительного абонента СРТС устанавливается один аналоговый телефонный аппарат без тангенты, а у руководителя – пульт ПОС-И.

На цифровой сети связи постанционная связь не проектируется, так как предполагается, что на всех ж.д. станциях организована общетехнологическая телефонная связь (ОбТС).

В работе предусматривается включения следующих схем:

- схема установки оборудования ОТС-Ц на ж.д. станциях проектируемых участков и организации колец нижнего и верхнего уровней;

- схема прохождения колец нижнего и верхнего уровней через мультиплексоры дорожной транспортной сети и выделения каналов для участков с аналоговыми системами ОТС;

- схема со структурой диспетчерских кругов и распределением канальных интервалов каналов Е1 по диспетчерским кругам.

На схеме показывается размещение коммутационных станций: по одной на всех ж.д. станциях, кроме Управления ж.д. На всех ж.д.станциях, не относящихся к Управлению и отделениям железной дороги, устанавливаются КС исполнительного типа (КС-И). В Управлении дороги одна КС, обслуживающая ЕДЦУ, должна быть распорядительной (КС-Р), вторая – обычно бывает комбинированной (КС-РИ).

На схеме показывается организация колец, образованных каналами Е1. Вначале планируются кольца нижнего уровня, а затем - кольцо верхнего уровня. В одно кольцо нижнего уровня в среднем должно входить 8…10 КС. Рекомендуется в одно кольцо включать не более 18 КС. Следует избегать образования колец с числом менее 5. Теперь образуется кольцо верхнего уровня, которое объединяет кольца нижнего уровня. Это кольцо должно проходить через минимальное число КС и к нему должен быть доступ от каждого кольца нижнего уровня. Коммутационные станции, через которые проходит кольцо верхнего уровня, называются мостовыми. Структура колец не зависит от структуры диспетчерских кругов. Любое кольцо должно проходить через КС только один раз.

На рис.3.2 показан пример организации пяти колец нижнего уровня на участках, соответствующих рисунку 1. В коммутационные станции, на которых происходит переход с цифровой сети на аналоговую сеть, включаются каналы ТЧ кругов ПДС, ПРС, ЛПС, СДС и ЭДС (на рис.2.2

предполагается, что участок от станции В до станции Ж – не электрифицирован и ЭДС на нём не организуется).

На данной схеме показывается организация каналов Е1 сети ОТС-Ц с применением плезиохронных и синхронных систем передачи, работающих по волоконно-оптическим кабелям. Каналы Е1 предназначены для образования колец нижнего и верхнего уровней. Каналы Е1 выделяются в пунктах установки коммутационных станций с помощью мультиплексоров первичной сети и подключаются к КС через электрические интерфейсы. Для повышения надежности связи каналы Е1, образующие в первую очередь кольцо верхнего уровня рекомендуется организовать по независимым путям.

В проекте следует самостоятельно запланировать линии передачи магистрального и дорожного уровня. На магистральном уровне используется систему передачи STM4, а на дорожном – STM1 или плезиохронной иерархии. Линия передачи магистрального уровня организуется на участках, относящихся к магистрали. Мультиплексоры STM4 устанавливаться только в Управлении и в отделениях дороги. На дорожном уровне линии передачи должны охватывать все участки цифровой сети. Мультиплексоры смежных ж.д. станций соединяются волоконно-оптическим кабелем.

На рис.2.3 приведён пример схемы организации каналов Е1 сети ОТС-Ц на участках. На дорожном уровне на всех ж.д. станциях устанавливаются мультиплексоры STM1. Образованы четыре линии передачи STM1: А-Б-В-Г; Д-В-Е; А-З-И-Л и И-М-Н, причём первые две линии продолжаются на других участках. Мультиплексоры магистрального уровня находятся на ст. А и В и являются частью линии передачи, уходящей влево за ст.А и вправо за ст.В. В соответствии с запланированными ранее кольцами (см.рис.2) показывается прохождение каналов Е1 внутри линий передачи, их выделение в местах подключения к КС и транзитные соединения между мультиплексорами. На схеме приводится нумерация колец, аналогичная предыдущей схеме (см.рис.3.2).

Также делается нумерация каналов Е1, включаемых в КС мостовых станций (например на ст. А – номера от 1 до 6). Аналогично рисунку 2, на схеме показывается включение в коммутационные станции групповых каналов ТЧ ПДС, ПРС, СДС, ЛПС и ЭДС (ст. Е и И).

На схеме показываются диспетчерские круги ПДС, ПРС, СДС, ЛПС и ЭДС.

За каждым диспетчерским кругом внутри каналов Е1, образующих кольца нижнего и верхнего уровней, закрепляется один канальный интервал (КИ). Можно использовать любые канальные интервалы кроме КИ0 и КИ16, причём номера канальных интервалов в кольцах нижнего и верхнего уровня могут не совпадать.

Для каждого круга диспетчерской связи показываются места нахождения пульта диспетчера и исполнительных устройств. Обозначение пультов и исполнительных устройств показано на рис.4. Тип исполнительного устройства зависит от диспетчерской связи: ПДС – ПОС-И и БМ с ТА-М; ПРС – Р/ст; ЭДС, СДС и ЛПС – ТА-Т. Одно исполнительное устройство показывается на требуемой ж.д. станции одной точкой на пересечении соответствующего группового канала. В виде точки также показывается подключение одного канала ТЧ, служащего для ответвления диспетчерского круга.

На рис.3.2 показана организация: по четыре круга ПДС и ПРС, по три круга ЭДС и ЛПС, два круга СДС. Каждому кругу соответствует канальный интервал. Допускается для кругов ПДС и ПРС два канальных интервала обозначать одной линией с указанием кругов и номеров КИ, например: ПДС1/ПРС1 КИ13/18.

Подробная конфигурация диспетчерских кругов по форме, приведена рисунке 3.4.

Также делается нумерация каналов Е1, включаемых в КС мостовых станций (например на ст. А – номера от 1 до 6). Аналогично рисунку 2, на схеме показывается включение в коммутационные станции групповых каналов ТЧ ПДС, ПРС, СДС, ЛПС и ЭДС (ст. Е и И).

На схеме показываются диспетчерские круги ПДС, ПРС, СДС, ЛПС и ЭДС.

За каждым диспетчерским кругом внутри каналов Е1, образующих кольца нижнего и верхнего уровней, закрепляется один канальный интервал (КИ). Можно использовать любые канальные интервалы кроме КИ0 и КИ16, причём номера канальных интервалов в кольцах нижнего и верхнего уровня могут не совпадать.

Для каждого круга диспетчерской связи показываются места нахождения пульта диспетчера и исполнительных устройств. Обозначение пультов и исполнительных устройств показано на рис.4. Тип исполнительного устройства зависит от диспетчерской связи: ПДС – ПОС-И и БМ с ТА-М; ПРС – Р/ст; ЭДС, СДС и ЛПС – ТА-Т. Одно исполнительное устройство показывается на требуемой ж.д. станции одной точкой на пересечении соответствующего группового канала. В виде точки также показывается подключение одного канала ТЧ, служащего для ответвления диспетчерского круга.

На рис.3.4 показана организация: по четыре круга ПДС и ПРС, по три круга ЭДС и ЛПС, два круга СДС. Каждому кругу соответствует канальный интервал. Допускается для кругов ПДС и ПРС два канальных интервала обозначать одной линией с указанием кругов и номеров КИ, например:

ПДС1/ПРС1 КИ13/18.

ПДС1: А-А1-А2-А3-Б-Б1-Б2-Б3; Г3-Г2-Г1-Г

ПДС2: Д-Д1-Д2-В-В2-В3-В4-В5-Е

ПДС3: А4-А5-А6-З-З1; К-К1-К2-К3

ПДС4: Н-М2-М1-М-И-И2-И3-Л

ЭДС1: А-А1-А2-А3-Б-Б1-Б2-Б3; А-А4-А5-А6-З-З1

ЭДС2: И-И1-М-М1-М2-Н; И-И2-И3-Л; И-К3-К2-К1-К

ЭДС3: В-Г3-Г2-Г1; В-В1-Д2-Д1-Д

СДС1: А-А1-А2-А3-Б-Б1-Б2-Б3; А-А4-А5-А6-З-З1;

И-И1-М-М1-М2-Н; И-И2-И3-Л; И-К3-К2-К1-К

СДС2: В-Г3-Г2-Г1; В-В1-Д2-Д1-Д; В-В2-В3-В4-В5-Е-Е1-Е2-Ж

ЛПС1: А-А1-А2-А3-Б-Б1-Б2-Б3; А-А4-А5-А6-З-З1

ЛПС2: И-И1-М-М1-М2-Н; И-И2-И3-Л; И-К3-К2-К1-К

ЛПС3: В-Г3-Г2-Г1; В-В1-Д2-Д1-Д; В-В2-В3-В4-В5-Е-Е1-Е2-Ж

На схеме диспетчерских кругов указываются номера каналов Е1 в соответствии со схемой организации каналов Е1 (см.рис.3.3).

Нумерация делается для всех абонентских устройств заданных участков за исключением участков с АСП. Номер абонентского устройства состоит из номеров кольца нижнего уровня, ж.д. станции внутри кольца и номера внутри ж.д. станции.

Вначале задаются двузначные номера колец нижнего уровня, в которых вторая цифра может принимать значения от 1 до 9. Если на заданных участках колец не более 9, то первая цифра номера одинаковая для всех колец. В противном случае каждому множеству из девяти и менее колец присваивается своя первая цифра. Затем внутри кольца для каждой ж.д. станции задаётся номер, состоящий из номера кольца и дополнительной одной (если в кольцо включено не более 10-ти ж.д. станций) или двух цифр.

Для каждой ж.д. станции определяется количество абонентских устройств ОТС, которое делится на две составляющие: для диспетчерской и станционной распорядительной связи (СРТС).

К абонентским устройствам диспетчерской связи относятся: пульты диспетчеров ПОС-Р; исполнительные пульты ПОС-И; аналоговые телефонные аппараты с тангентами – ТА-Г, устанавливаемые у исполнительных абонентов диспетчерской связи; стационарные

радиостанции поездной радиосвязи Р/ст. Требуемое количество абонентских устройств диспетчерской связи было определено ранее. Каждому абонентскому устройству диспетчерской связи, за исключением устройств ДСП, присваивается один номер. Пульту ПОС-И и мобильному телефону ТА-М дежурного по станции присваивается один общий номер.

Количество абонентов СРТС можно принять исходя из следующих рекомендаций. Для ЕДЦУ и Управления дороги – диспетчеры ПДС, ЭДС, СДС и ЛПС; ДСП и исполнительные абоненты ЭДС, СДС и ЛПС; 4…8 иных руководителей и 25…45 иных исполнительных абонентов; для отделения дороги и крупной ж.д. станции – диспетчеры ЭДС, СДС и ЛПС; ДСП и исполнительные абоненты ЭДС, СДС и ЛПС; 1…3 иных руководителя и 10…25 иных исполнительных абонентов; для промежуточных станций.

ДСП и исполнительные абоненты ЭДС, СДС и ЛПС; 2…8 иных исполнительных абонентов. Каждому абоненту СРТС присваивается один номер.

При этом диспетчеры и дежурные по станциям входят в обе группы абонентов. Поскольку пульт диспетчера по одному из каналов В постоянно подключён к групповому каналу, за его пультом следует закрепить два номера – для диспетчерской связи и СРТС. Для пульта ДСП можно закрепить один номер.

Номера следует присвоить для МЖС и ПГС. За МЖС закрепляются два номера – один для соединения по физической цепи, другой для соединения по выделенному канальному интервалу внутри канала Е1. Для ПГС номер присваивается на случай организации связи с местом аварии.

Количество номеров для одной ж.д. станции может быть определено по следующей формуле:

$N = К_{участ.} + К_{станц.}$ ,

где: $К_{участ.}$ – число абонентских устройств диспетчерской, межстанционной и перегонной связи.

$К_{станц.}$ – число абонентских устройств внутри станции за исключением тех, что вошли в число $К_{участ.}$ ;

$К_{участ.} = 2*К_{дисп.} + К_{ПРС-Р} + К_{ПРС-И} + К_{ДСП} + К_{испол} + 2*К_{МЖС} + К_{ПГС,}$

где: $К_{дисп.}$ – число диспетчеров; $К_{ПРС-Р}$ – число пультов ПРС (только для ЕДЦУ); $К_{ПРС-И}$ – число стационарных радиостанций ПРС на станции ($К_{ПРС-И}$ = 1); $К_{ДСП}$ – число ДСП на станции (в большинстве случаев $К_{ДСП}$ = 1); $К_{испол}$ – число исполнительных абонентов ЭДС, СДС и ЛПС; $К_{МЖС}$ – число линий МЖС, включаемых в КС; $К_{ПГС}$ – число линий ПГС, включаемых в КС.

$К_{станц.} = К_{СРТС-Р} + К_{СРТС-И}$ ,

где: $К_{СРТС-Р}$ – число руководителей СРТС, кроме диспетчеров и ДСП (иные руководители); $К_{СРТС-И}$ – число исполнительных абонентов СРТС, кроме исполнительных абонентов ЭДС, СДС и ЛПС (иные исполнительные абоненты).

Внутри каждой ж.д. станции, должна быть предусмотрена сокращенная нумерация для всех абонентских устройств, кроме радиостанций ПРС. Сокращенные номера состоят из двух или трех последних цифр полного номера абонентских устройств. Например, для ж.д. станции А1 (см.таблицу 3.1) используются следующие сокращенные номера: 31…45.

Нумерация для групп абонентов делается только для кругов поездной диспетчерской связи.

Для каждого круга ПДС задаётся количество групп абонентов, число которых рекомендуется принимать от двух до четырёх. В группу обычно входят ДСП, находящиеся на ж.д.станциях одного участка. Число ДСП в одной группе варьируется от 2 до 10.

В третьем главе приведён пример нумерации для групп абонентов двух кругов ПДС. Для каждой группы указаны ж.д. станции, где находятся ДСП. У каждой ж.д. станции записывается абонентский номер, присвоенный для данного ДСП (например, А2 (21331)). Этот номер берётся в соответствии с номерами, записанными в таблице 3.1.

Далее для каждой группы задаётся групповой номер, служащий для вызова всех абонентов данной группы. Такой номер состоит из четырёх цифр. Первая (старшая) цифра должна совпадать с первой цифрой номеров колец нижнего уровня. Вторая цифра должна быть равна нулю, что указывает на групповой номер. Предпоследняя цифра является номером круга ПДС, а последняя – номером группы абонентов в этом круге.

## 3.2. Построение групповых каналов технологической связи с использованием IP телефонии.

Построения групповых каналов с использованиях IP телефонии основана на концепции Cisco, объединяющая системы передачи данных, телефония и видео (рис.3.1). Современная технология обеспечивает потребности информационной системы и диктует растущие требование к таким системам. Интеграция телефонии видео и данных позволяет расширить возможности, доступные пользователю такой сети. Целью интегрированную систему есть обеспечение сотрудников удобными средствами, который помогает решать стоящие задачи.

Рис. 3.1. Единая сеть концепции Cisco

Возможность внедрения этой сети на железнодорожный транспорт позволит обеспечить сетевую безопасность, управление качеством услуг, обеспечиваемым сетевой инфраструктурой.

Появление нового интегрированного решение Cisco IP видео телефонии позволяет преодолеть основные проблемы существующих видео систем – сложность использования для конечных абонентов и трудоемкость поддержки и управления видеорешениями для администрации системы. Это система может использоваться для видео звонка, при этом устанавливается видеосоединения в результате набора номера со своего IP телефона. Видеоизображение будет выведена на экран персонального компьютера с помощью видеоустройства Cisco VT Advantage.

Сети Cisco IP телефонии основано на использования моделей Cisco AVVID и предназначено для решения следующих задач: построение современной многофункциональной системы цифровой телефонии; подключение системы IP телефонии к телефонной сети общего пользования и стыковка с существующими участками традиционной телефонной сети; обеспечение широкого круга современных сервисов.

Решение Cisco IP телефонии состоит из следующих основных компонентов:

Управляющий сервер Cisco Call Manager обеспечивает управление установлением телефонных соединений и видеосоединений в системе. CallManager также управляет предоставлением дополнительных функций абонентам, использующим как IP телефоны, так и видеоустройства.

Специализированные цифровые IP телефоны Cisco подключаются в коммутируемую локальную сеть Ethernet 10/100 и обеспечивают как традиционную функциональность цифровых телефонов, так и ряд новых возможностей, присущих IP телефонам Cisco. Для стыковки с существующими системами традиционной телефонии ( в том числе с установленными ранее УАТС) и подключения к телефонной сети общего пользования, применяются голосовые шлюзы. Данная функциональность реализована на базе целого ряда мультисервисных маршрутизаторов Cisco. Существуют также голосовые модули для некоторых моделей коммутаторов

Cisco Catalyst и самостоятельные устройства, обеспечивающие функциональность голосовых шлюзов.

Дополнительные компоненты входят в состав видеотелефонной составляющей интегрированного решения (наряду с управляющим компонентом решения – Cisco CallManager): абонентские видеоустройства Cisco VT Advantage; AVTA позволяет расширить возможности абонентского IP телефона за счет передачи видео на ПК абонента при установлении телефонного соединения; видеотерминалы сторонних производителей, поддерживающие протоколы H.323 и SCCP; дополнительным компонентом решения Cisco видеотелефонии являются устройства Cisco IP/VC MCU серии 3500 (IP/VC 3540 и 3511), обеспечивающие аудио- и видеоконференции в системе; также необязательным компонентом являются H.323 гейткиперы, использующиеся для интеграции с H.323 аудио- и видеосетями; ISDN шлюзы семейства IP/VC обеспечивают интеграцию с существующими системами H. 320 видеоконференций.

Показана на рисунке 3.2 простейший вариант телефонная сеть, охватывающая абонентов, находящихся в одном здании или группе близко расположенных зданий.

Рис.3.2. Интегрированная сеть IP телефонии: одно здания

Внедрение видеотелефонии достигается простым расширением описанной выше системы. В простейшем случае достаточно оснастить персональные компьютеры абонентов системой Cisco VT Advantage или подключить видеотерминалы (такие, как, например, устройства Tandberg 1000) к системе Cisco IP телефонии. Используемый в системе Cisco CallManager будет осуществлять управление установлением как обычных телефонных соединений, так и видеозвонков. Для обеспечения функциональности видеоконференций (т. е. при необходимости участия в

одном видеосоединении более двух абонентов) потребуется дополнительно использовать устройства MCU из семейства продуктов Cisco IP/VC (рис.3.3).

Рис.3.3. Интегрированная система IP видеотелефонии

Один из наиболее распространенных вариантов построения системы IP телефонии представляет собой распределенную систему, обеспечивающую сервисы корпоративной IP телефонии не только для центрального офиса, но и для удаленных подразделений/офисов, подключенных к корпоративной IP сети с обеспечением необходимых механизмов качества сервиса (QoS).

При использовании подобной схемы построения сети необходимо предусмотреть возможность локальной обработки вызовов в удаленном отделении на случай потери связи между удаленным и центральным отделениями, например, в случае сбоя канала WAN. Для этой цели можно использовать средства отказоустойчивой телефонии для удаленных офисов (Survivable Remote Site Telephony) на базе целого ряда моделей маршрутизаторов Cisco (рис.3.4).

Рис.3.4. Распределенная система IP телефения и видеотелефонии

Обеспечение услуг телефонии на базе сети передачи данных позволяет избавиться от необходимости эксплуатации раздельных сетей для передачи данных и телефонной связи и обеспечивает возможность более полного удовлетворения потребностей предприятий в услугах телефонии. Продукция Cisco IP телефонии позволит уменьшить расходы на внедрение, поддержку и расширение объединенной сети и, как следствие, повысить рентабельность телекоммуникационной сети. Вот лишь некоторые достоинства использования IP телефонии: возможность построения единой

телекоммуникационной инфраструктуры на базе IP сети, обеспечивающей функциональность системы телефонии, а также видеотелефонии; интегрированное сквозное решение, обеспечивающее возможность внедрения единой сетевой политики в рамках всей сети (политики обеспечения качества сервиса, безопасности, сетевого управления и т. д.). IP телефонию отличается простотой построения географически распределенных телефонных и видеотелефонных систем (за счет распределенной природы архитектуры решения); гибкие возможности масштабирования и функционального расширения системы. Используемая компанией Cisco политика защиты инвестиций дает сокращение расходов на каналы за счет возможности эффективного использования каналов для совместной передачи голосового трафика, данных и трафика видеоприложений; сокращение расходов на оплату междугородных переговоров; упрощение настройки, поддержки и администрирования телекоммуникационной инфраструктуры; снижение общей стоимости владения системой; возможность использования современных приложений, использующих преимущества интеграции голоса, видео и данных в рамках единой телекоммуникационной инфраструктуры; ориентация на поддержку открытых протоколов и интерфейсов для разработки приложений (API), обеспечивающая возможность интеграции с широким спектром современных приложений, предлагаемых в настоящее время различными производителями; возможность разработки собственных приложений, интегрирующихся с сетями IP телефонии.

### 3.3. Расчет мультисервисной сети связи

Расчет интенсивности нагрузки и распределение её по направлениям в сети. Этот расчет состоит из расчетов нагрузки мультисервисной сети, анализа исходных данных, пиковых обменов потоков, расчет потока данных между отделами - серверами и отделами - сетью Internet.

Расчет мультисервисной сети связи данного предприятия включает несколько этапов: составление структурной схемы ЛВС; расчет трафика для каждого отдела и сетью Internet; расчет трафика между отделами; расчет интернет трафика; расчет трафика сервер - сервер; расчет трафика отдел - сервер. Общее число пользователей (ПЭВМ) 40; Общее количество VoIP - телефонных аппаратов 12 шт. Общее число серверов 5;

## Заключение

По результатам магистерской диссертационной работа можно сделать следующее заключение:

Мультисервисная сеть Cisco IP телефония поддерживает безопасность сетевого управления и гарантирует качество сервиса.

При возникновении неполадок работа мультисервисной сети, поиск неисправностей происходит в строгом соответствии с семиуровневой моделью сети ISO OSI, алгоритм которого состоит из восьми шагов.

Построения групповых потоков Cisco предусматривает применение аппаратуры оперативно- технологической связи типа ДСС.

Разработана схема группового канала технологической связи с использованием IP телефонии.

Произведен расчет мультисервисной сети, состоящей из расчета нагрузки, пиковых обменов потоков, потока данных между отделами, отделами – сетью Internet.

## СПИСОК ЛИТЕРАТУРЫ


1. Мирзияев Ш.М. «Обеспечение верховенства закона и интересов человека - гарантия развития страны и благополучия народа». Т.: «Узекистан» - 2016

2. Диагностика и анализ локальных сетей [Электронный ресурс]: — Электрон. дан. — КомпьютерМастер, 2004. — Режим доступа: http://www.computermaster.ru/articles/landiagnost.html., свободный.

3. Balenson D. Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers [Электронный ресурс]: — Электрон. дан. - RFC 1423, TIS, IAB IRTF PSRG, IETF PEM WG, 1993.

4. Braden R. Requirements for Internet Hosts - Application and Support [Электронный ресурс]: — Электрон. дан. - STD 3, RFC 1123, Internet Engineering Task Force, 1989.

5. Busse I., Deffner B., SchulzrinneH. Dynamic QoS control of multimedia applications based on RTP [Электронный ресурс]: — Электрон. дан. - Computer Communications, 1996.

6. Cadzow J. A. Foundations of digital signal processing and data analysis [Электронный ресурс]: — Электрон. дан. - N.-Y.: Macmillan, 1987.

7. Cisco Voice Over IP Version 4.2 [Электронный ресурс]: — Электрон. дан.

— Cisco Systems Inc, 2004. — 1 электрон. опт. диск (CD-ROM)

20. Clark D. D., Tennenhouse D. L. Architectural considerations for a new generation of protocols in SIGCOMM Symposium on Communications Architectures and Protocols // Computer Communications Review. — 1990. — №— С. 200-208.

8. Crocker D. Standard for the Format of ARPA Internet Text Messages [Электронный ресурс]: — Электрон. дан. - STD 11, RFC 822, UDEL, 1982

9. Eastlake D., Crocker S., Schiller J. Randomness Recommendations for Security [Электронный ресурс]: — Электрон. дан. - RFC 1750, DEC, Cybercash, MIT, 1994.

10. Feller W. An Introduction to Probability Theory and its Applications - N.-Y.: John Wiley and Sons, 1968 — T. 1.

11. Floyd S., Jacobson V. The synchronization of periodic routing messages in SIGCOMM Symposium on Communications Architectures and Protocols // Computer Communications Review. — 1993. — № 20. — С. 33-44.

12. International Standards Organization, "ISO/IEC DIS 10646-1:1993 information technology -- universal multiple-octet coded character set (UCS) -part I: Architecture and basic multilingual plane," 1993.

13. Mills D. Network Time Protocol Version 3 [Электронный ресурс]: — Электрон. дан. - RFC 1305, UDEL, 1992.

14. Mockapetris P. Domain Names - Concepts and Facilities [Электронный ресурс]: — Электрон. дан. - STD13, RFC 1034, USC/Information Sciences Institute, 1987.

15. Mockapetris P. Domain Names - Implementation and Specification [Электронный ресурс]: — Электрон. дан. - STD 13, RFC 1035, USC/Information Sciences Institute, 1987.

# ПРИЛОЖЕНИЯ