Съдържание

1. Увод

1.1. Въведение в областта

Съвременният бизнес не може да съществува без телефонни комуникации, това е факт. От огромно значение са не само връзките в реално време с клиенти, но и тези с бизнес партньори, производители, както и между служителите на всяка компания. Традиционните телефонни комуникации, както стационарни, така и мобилни, са считани за даденост от повечето техни потребители. Въпреки непрестанното им развитие, многобройните им технологични промени остават незабелязани, тъй като телефоните запазват своите основни функции – да инициират и приемат обаждания.

В ранните етапи на развитие на компютърните комуникации и Интернет за транспортна среда при обмен на данни е била използвана предимно традиционната телефонна мрежа. За връзка към Интернет са използвани модеми, даващи възможност за получаване и предаване на данни през съществуващи телефонни линии. Увеличаването на броя на Интернет потребителите и разработването на множество мрежови приложения водят до многократно нарастване на обема на предаваните данни, които заемат основната част от честотната лента. Необходимостта от все по-голяма честотна лента налага създаването на технологии за високоскоростно предаване на данни. Изграждат се две физически отделни мрежи за предаване на глас и данни.

В средата на деветдесетте години на миналия век телефонните комуникации навлизат в изцяло нов етап от своето развитие. Настъпващите промени не се отразяват на начините за извършване на обаждания, те засягат начините на организиране и структуриране на бизнес комуникациите. Телефонните мрежи, до скоро използвани за предаване на компютърни данни, биват заменяни от мрежите за данни, предаващи гласови сигнали в цифров вид. VoIP е поредното технологично нововъведение, навлизащо с бързи темпове и оказващо голямо влияние върху съвременните бизнес комуникации. Терминът VoIP, накратко от

Voice over Internet Protocol, е метод за предаване на гласови данни в цифров вид, енкапсулирани в IP пакети. VoIP мрежите не само улесняват телефонните комуникации, но и предоставят редица нови функции, променящи изцяло концепцията за телефонно обаждане. Основна предпоставка за успеха на VoIP е широкото разпространение на IP базираните мрежи, каквито са почти всички корпоративни, частни, обществени, кабелни и безжични компютърни мрежи.

За първи път моделът за VoIP комуникации е представен през 1995 година от компанията Vocaltec Inc. с разработения от нея софтуерен продукт „Internet Phone". Необходимият за неговото използване хардуер включвал персонален компютър с процесор 486 работещ на 33 MHz, звукова карта, високоговорител и модем за връзка към IP мрежата [21]. Задачата, изпълнявана от приложението, се свежда основно до компресиране на гласовия сигнал в IP пакети и предаването им до търсен потребител. Изискване за осъществяване на обаждане е било използването на един и същи софтуер и от двамата участници в разговора. Друго ограничение на този продукт е възможността за осъществяване на връзки единствено между персонални компютри, но не и с абонати на традиционни телефонни компании.

Днес терминът Voice over Internet Protocol е приет като нарицателно за различни комуникационни модели и обхваща голям набор от технологии. Като цяло, VoIP превръща в цифров вид и компресира гласовия трафик, който след това бива енкапсулиран в IP пакети и транспортиран през обществени или частни IP мрежи. Използвайки този метод, гласовият трафик може да бъде пренесен между всеки две точки на IP мрежа, имащи валидни IP адреси. Важно при предаване на гласови данни в реално време е използването на механизми, осигуряващи качество на услугите.

Най-общо VoIP технологията може да бъде разделена на два основни вида [16]. Първият от тях използва мрежи за данни за пренос на VoIP пакети, единствено с цел намаляване на разходите за провеждане на телефонни обаждания. Това е най-лесният начин за имплементиране на VoIP, осигуряващ и най-бърза възвращаемост на инвестициите. Този метод е често прилаган от публични телефонни компании, предлагащи атрактивни цени на разговори на далечни разстояния, вследствие на

занижените си разходи. Вторият вид VoIP използва IP телефони, които са директно свързвани към Етернет мрежа, вместо към отделна физическа телефонна мрежа. При използването на IP телефони гласовият трафик бива предаван в цифров вид по цялата верига, което позволява да бъде използван пълният потенциал на IP телефонията и приложенията, свързани с нея.

Честа заблуда е, че VoIP комуникациите все още се използват единствено за връзка между персонални компютри. Към настоящия момент потребителите на VoIP услуги могат да се свържат с всеки телефонен номер, достъпен за абонатите на обществените телефонни компании. VoIP обединява служителите във всички корпоративни офиси, както и мобилните служители, свързвайки ги с единна комуникационна среда за обмен на глас и данни.

VoIP е бързоразвиваща се технология, показателен за което е фактът, че през 2005 година са били произведени и доставени на пазара по-голям брой IP телефонни апарати, отколкото традиционни телефонни апарати. Все повече традиционни телефонни компании преминават към VoIP технологиите за пренос на гласови данни с цел намаляване на разходите си. Многобройните нови възможности и гъвкавостта при изграждане на бизнес комуникациите след имплементиране на VoIP са предпоставки за по-добро обслужване на клиенти, по-ефективна работа на служителите, както и за намаляване на разходите.

1.2. Цели на дипломната работа

Целта на настоящата дипломна работа е задълбочен анализ на VoIP технологиите, сферите на тяхната употреба, надеждност, преимуществата им пред традиционните телефонни мрежи и методите за тяхното прилагане. Изготвен е цялостен проект за преминаване към единна IP среда за пренос на глас и данни, заменяща традиционните телефонни централи и премахваща необходимостта от обслужването на две отделни мрежи. Поставената цел е не само разглеждане на конкретен пример за имплементиране на VoIP, а обстоен анализ на процеса на миграция към IP телефония. Началният етап при осъществяване на така дефинираната цел изисква представяне на критериите и последователността при

оценяване на съществуващата IP мрежа за пренос на данни, както и на потребителските изисквания. Тъй като дипломната работа не е конкретно решение на дадено задание, а дава общ поглед върху проблемната област, то нейната цел включва разглеждане на схеми за избор на хардуерни решения и стратегии за тяхното имплементиране. Последна, но не по-малко съществена цел, придаваща завършеност на проекта, е разработването на конкретни конфигурации за мрежовите устройства, осигуряващи необходимата сигурност и функционалност в съответствие със зададена политика Цел при тяхното съставяне е обхващане на едни от най-често използваните технологии за предаване на данни, изграждане на връзка към традиционна телефонна централа, както и прилагане на разгледаните в дипломната работа методи за осигуряване качество на услугите.

1.3. Структура на дипломната работа

Настоящата дипломна работа е организирана в осем основни глави. Приложени са също списък с използваната литература, както и речник на термините и съкращенията.

Глава 1 съдържа кратко въведение в разглежданата област и дефинира основните цели на дипломната работа.

Глава 2 представя принципите в работата на IP телефонните системи, тяхната архитектура и основните им компоненти. Разгледани са също и традиционните телефонни мрежи, които са основоположни на IP телефонните комуникации.

Глава 3 разглежда предимства на VoIP телефонните мрежи, като вниманието е насочено към икономическите стимули за преминаване към единна мрежа за глас и данни, възможностите за създаване на приложения, влияещи положително на работния процес и предпоставките, допринасящи за намаляване на периода за възвръщане на инвестициите.

Глава 4 е посветена на технологиите, използвани при VoIP комуникациите. Направен е обзор на най-често използваните кодеци, протоколите, служещи за

сигнализация и пренос на гласовия трафик, а също и на методите за оценяване качеството на гласовия сигнал.

Глава 5 описва факторите, влияещи върху качеството на предаване на гласови данни през IP мрежа. Анализирани са проблемите, свързани с предаването на глас през мрежа за данни и са представени решения за всеки от тях.

Глава 6 разисква нужните стъпки при създаване и имплементиране на VoIP решения. Дискутирани теми са инфраструктурния анализ на съществуващата мрежа за данни, възможните стратегии при миграция към единна мрежа и критериите за избор на хардуерно оборудване.

Глава 7 описва конфигурирането на мрежовите устройства за предаване на гласови данни. Засегнати са различни технологии за пренос на данни и са представени конкретни решения на разгледаните в предходните глави методи за осигуряване качество на услугите. Направено е детайлно описание на синтаксиса на използваните команди. Представени са цялостни конфигурации на мрежовите устройства, изграждащи примерна VoIP мрежа.

Глава 8 представлява кратко резюме, включващо и направените изводи и възможности за бъдещо развитие на текущия проект.

2. Архитектура на IPT мрежите

2.1. VoIP или IPT

Терминът IPT или IP телефония не трябва да бъде бъркан с по-общото наименование Voice over IP или VoIP. Една VoIP мрежа може да включва хибридни решения със съвместно работещи IPT и традиционни телефонни системи. Пример за това е използването на IP-PBX централи. Гласовите данни, обменяни между тях, се предават в цифров вид, енкапсулирани в IP пакети. Въпреки това, крайните устройства - телефонни апарати и факсове, свързани към тях са аналогови, и данните, обменяни между тях и IP-PBX централите са в аналогов вид.

За разлика от това, една IPT мрежа в чист вид се базира изцяло на цифрово предаване на гласовите данни с помощта на IP пакети от произволен потребителски телефон до всеки друг в мрежата или до медиа шлюза, служещ за връзка с външни телефонни мрежи. Цифровия вид на данните дава възможност да бъдат реализирани всички предимства на IP базираните телефонни системи. Въпреки тези различия, по-общия термин VoIP, включващ в себе си и частния случай IPT, често бива използван за описание и на двата вида мрежи [7].

2.2. Традиционни телефонни мрежи

За успешното планиране и имплементиране на VoIP система са необходими основни познания върху структурата и функционирането на традиционните телефонни системи.

В началото на развитието си, телефонните мрежи започват като системи от медни жици, свързващи потребителите един с друг. В продължение на десетилетия, електричеството, преминаващо по тези жици, бива използвано единствено за предаване на аналогови сигнали. В средата на миналия век се слага началото на разработването на технологии за предаване на глас през цифрови мрежи. В днешно време почти всички обаждания биват пренасяни през телефонната мрежа във вид

на цифрова информация. Единствено в частта между потребителския телефон и телефонната централа все още се използват аналогови сигнали.

В ранните етапи на телефонните комуникации е било необходимо използването на отделни физически връзки за всяко обаждане. С въвеждането на честотното разделяне (Frequency Division Multiplexing - FDM) става възможно използването на една аналогова линия за едновременно предаване на множество обаждания. Следващият етап настъпва с откриването на механизми за цифровизиране на гласовия поток и предаването му в цифров вид. Постепенното преминаване на аналоговата телефонна мрежа към цифрова започва през шестдесетте години на двадесети век. Тези промени са в отговор на нуждите от пренасяне не само на по-големи количества гласов трафик, но и на данни за появилите се тогава компютърни мрежи. В цифровите телефонни мрежи разговорите на домашните абонати най-често биват цифровизирани в телефонната централа, към която е свързан абоната. В по-големите организации цифровата връзка продължава до частната УТЦ, като в зависимост от нейния вид, може да достигне и до телефонните апарати на крайните потребители. В последния случай, единствената част от телефонната верига, в която гласът се предава в аналогов вид, е от устата на говорещия до микрофона на слушалката.

Съществуват четири основни функции на обществената комутируема телефонна мрежа (PSTN), необходими за осъществяване на едно телефонно обаждане [6]. Останалите предлагани от PSTN услуги, като конферентни връзки, пренасочване на повикванията, ограничаване на изходящите повиквания и други, се осъществяват също на базата на тези функции, които са:

- Сигнализиране
- Услуги, свързани с бази данни
- Свързване и прекратяване на обаждане
- Преобразуване на гласа в цифров вид

Телефонните обаждания по своята природа са връзково-ориентирани. Това означава, че връзката между двете страни трябва да бъде осъществена преди

началото на разговора. Телефонните централи, които са основните компоненти на PSTN мрежата, са отговорни за създаването на тези връзки. Множеството от връзки между централите, свързващи страните участващи в едно обаждане, образуват верига, пренасяща гласовите данни. Тази верига се създава преди началото на разговора и съществува физически до неговото прекратяване от някой от участниците. Телефонните централи са свързани по между си с комуникационни трънк линии, вариращи по капацитет от E1 до OC-192c/STM-64. Всяка една от тези линии е разделена на отделни DS-0 канали, осигуряващи капацитета, необходим за едно телефонно обаждане – 64 Kbps.

Сигнализацията се използва за да се бъдат известявани както мрежовите елементи, така и потребителите на телефонната мрежа, за настъпването на определени събития. Примери за такива събития са активирането на телефонния звънец, уведомяващо потребителите за постъпило повикване, както и набирането на цифрите на телефонен номер. Сигнализацията между мрежовите елементи се използва за създаване на връзки в мрежата.

Системата за сигнализация Signaling System Seven (SS7) е пакетно-базирана, безвръзково-ориентирана мрежа, служеща за транспортна среда при преноса на сигнализиращ трафик, обменян между отделните телефонни централи, участващи в едно обаждане. Нейните задачи са да изгражда, разпада, наблюдава и маршрутизира повиквания в PSTN мрежата. Заявките за превод на телефонни номера в инструкции за създаване на вериги се изпълняват от устройствата за управление на услугите (SCP) с помощта на техните бази данни. Точките за комутация на сигнализацията (SSP) са интерфейсите между телефонните централи и сигнализиращата мрежа SS7. В тях SS7 съобщенията се превеждат в инструкции за изграждане на съединителни линии за свързване на дадено обаждане.

Съобщенията на SS7 не се пренасят през връзките, служещи за обмен на гласови данни. Те се предават през самостоятелна мрежа, изградена паралелно на PSTN от специализирани устройства за трансфер на сигнала (STP). Устройствата са аналогични като функционалност на маршрутизаторите в мрежите за данни и пренасят съобщенията в пакети, наречени MTP. Тези съобщения могат да

предизвикат телефонно звънене, индикация за зает сигнал, за приключване на обаждане и други.

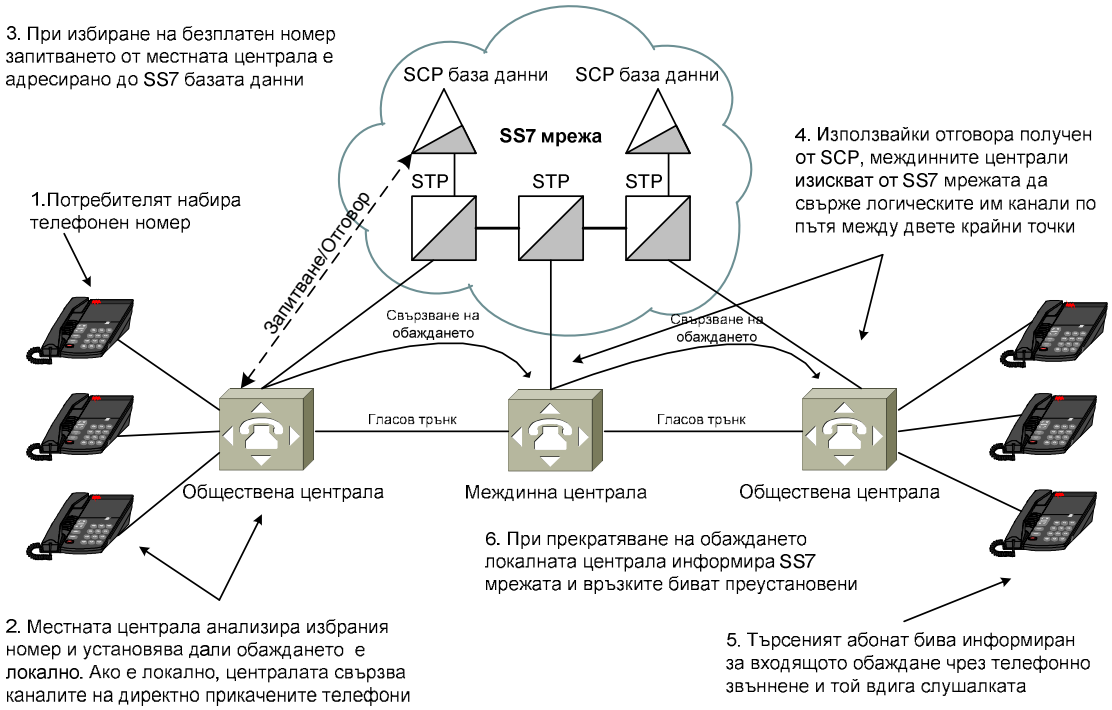
Мрежовата система SS7 е съвкупност от мрежи, която обхваща значителна част от държавите от развития свят. Съществуват множество технически и исторически причини за отделянето на сигнализиращия трафик от мрежата за пренос на глас. Най-съществената от тях е предоставянето на възможност за добавяне и променяне на мрежовата интелигентност и предлаганите услуги, без това да зависи от преносната среда на мрежата за гласови данни.

Когато някой абонат вдигне телефонната слушалка, телефонната централа разпознава това и се подготвя за последващото набиране на цифрите, съставящи търсения номер (Фиг. 2.1). Централата може да бъде както частна УТЦ, намираща се в същата сграда с телефона, инициращ обаждането, така и обществена централа, отдалечена на километри от него. По време на набирането на цифрите, телефонната централа проверява валидността на избрания номер и дали търсения абонат е директно свързан към нея. Ако обаждането е локално, централата свързва логическите канали на двете страни, с което завършва процеса по неговото осъществяване. В противен случай, централата изпраща запитване до базата данни в искане на инструкции за свързване на обаждането. Трябва да бъде отбелязано, че на запитването може да не бъде отговорено изцяло само от една база данни, а това да става на части от базите данни в различни възли за управление на услугите, както и че в този процес може да бъдат намесени и външни доставчици на телефонни услуги. Резултат от запитването е свързване на логическите канали между участващите централи и образуването на верига, водеща до търсения абонат. Централата, имаща директна връзка с търсеният абонат, изпраща съобщение до телефонния апарат, активиращо неговото звънене. Той бива уведомен за наличие на входящо обаждане и с вдигане на слушалката връзката бива осъществена.

При започване на разговора, телефонните централи трябва да имат готовност за преобразуване на аналоговия гласов сигнал в цифров вид, удобен за пренасяне през телефонната мрежа. При приключване на разговора, директно свързаните към говорещите страни централи изпращат съобщения, уведомявайки

останалите участващи от веригата за прекратяването на връзката. Те от своя страна прекъсват техните логическите канали, свързващи обаждането, освобождавайки своите ресурси.

Фигура 2.1. Свързване на телефонно обаждане при традиционна телефонна мрежа



2.3. Основни компоненти на VoIP мрежите

Основните компоненти, съставящи VoIP мрежите са много сходни в своята функционалност с тези, изграждащи традиционните телефонни мрежи. VoIP мрежите изпълняват всички задачи, характерни за традиционните телефонни мрежи, но в допълнение те трябва да предоставят и начин за връзка с тях. Макар и наричани по различен начин от различните производители, сходната им функционалност позволява разделянето на основните VoIP елементи на три групи:

- Медиа шлюзове
- Медиа шлюзове/сигнализиращи контролери

- IP мрежа

2.3.1. Медиа шлюзове

Медиа шлюзовете са отговорни за осъществяването на обаждания, обработката на заявки за входящи обаждания, конвертиране на гласовия поток от аналогов в цифров вид (кодиращи-декодиращи или кодек функции) и създаване на пакети, пренасящи гласовите данни. В допълнение те могат да изпълняват и други функции, като компресиране на гласовия трафик, премахване на ехото в сигнала, непредаване на паузите в речта и събиране на статистически данни.

Медиа шлюзовете са интерфейса, осигуряващ взаимодействието между пакетно-базираните IP мрежи и PSTN. За всяко обаждане се използва отделна RTP сесия, като задачата на медиа шлюза е създаването на пакетите, пренасящи частите на речта. Интерфейсът към PSTN, освен връзка с традиционните телефонни мрежи, е и алтернативен път за гласовия трафик, в случаите на претоварване на VoIP мрежата, както и в случаите на прекъсване на някоя VoIP връзка или отпадане на мрежови елемент.

Медиа шлюзовете могат да съществуват под различни форми. Възможно е те да бъдат както отделни телекомуникационни хардуерни елементи, така и ролята им да бъде изпълнявана от персонален компютър с работещ на него VoIP софтуер. Медиа шлюзовете могат да изпълняват функциите на един или няколко от изброените по-долу видове:

- Магистрален шлюз, служещ за интерфейс между традиционна телефонна и VoIP мрежа, управляващ голям брой цифрови връзки. Той предоставя различни видове интерфейси към PSTN, включващи DS-1, DS-3, E3,OC-3, STM-1 и други.
- Жилищен шлюз, осигуряващ стандартен аналогов интерфейс на VoIP мрежата. Примери за това са кабелните модеми, xDSL и широколентовите безжични устройства. Този вид шлюз дава достъп на крайни потребители до VoIP мрежата.

- Шлюз за достъп, предоставящ стандартен аналогов или цифров интерфейс между УТЦ и VoIP мрежа.
- Бизнес медиа шлюз, осигуряващ стандартен интерфейс между цифрова УТЦ и VoIP мрежата.

2.3.2. Медиа шлюз контролери

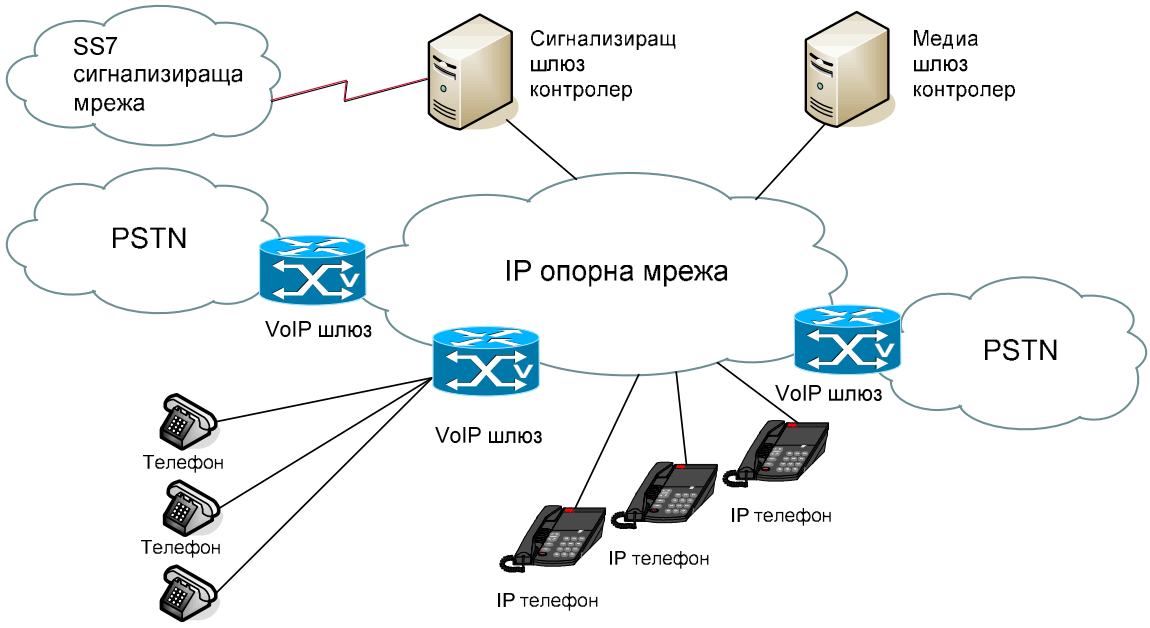
Медиа шлюз контролерите осигуряват сигнализацията и контрола върху обажданията и всички предлагани услуги във VoIP мрежата [2]. Те служат за координиране на функциите на медиа шлюзовете. Други техни функции са съпоставянето на телефонни номера и мнемонични имена в IP адреси, намиране на адреси/потребители, управление на ресурсите, авторизация и автентикация на потребителите. При наличие на връзки към PSTN, медиа шлюз контролерите преобразуват сигнализацията SS7, използвана в традиционната телефония, в конкретния за VoIP мрежата протокол за сигнализация.. Сигнализацията във VoIP мрежата служи за управление на връзката между двете крайни точки и уговаряне на нейните параметри. След изпълнението на тази задача, шлюз контролера не изпълнява други функции по време на разговора, до момента, в който някоя от двете крайни точки изпрати съобщение за смяна на статуса на връзката или шлюз контролера уведоми някоя от тях за наличие на изчакващо обаждане или смяна на конфигурацията на връзката. Пакетите, съдържащи гласовите данни, не минават през медиа шлюз контролерите, а се обменят директно между участниците в разговора или преминават през медиа шлюз в случаите, в които има нужда от преобразуване на сигнала.

Възможно е ролята на шлюз контролера да бъде разделена на сигнализиращ шлюз контролер и медиа шлюз контролер. За всички обаждания, с начална и крайна точка в пределите на VoIP мрежата, е достатъчна функционалността на медиа шлюз контролера. В случаите, когато е необходима връзка между PSTN и VoIP мрежите, се налага и използването на сигнализиращи шлюз контролери. Техните функции са съсредоточени върху преобразуване на служебните съобщения и сигнализацията, което е необходимо за свързване на двата вида мрежи.

2.3.3. IP мрежа

Възможно е цялата VoIP мрежа да бъде разгледана като един логически комутатор, осигуряващ връзките между разпределените системи (Фиг. 2.2).

Фигура 2.2. IP мрежа



IP инфраструктурата трябва да гарантира безпроблемното доставяне на гласовите данни и сигнализиращия трафик. За това е необходимо да се установят изискванията за допълнителна честотна лента, с оглед бъдещото добавяне на гласовия трафик, и при нужда да се увеличи капацитетът на връзките. Дори след осигуряване на необходимия капацитет е препоръчително използването на механизми, осигуряващи качество на услугите, за да се гарантира приоритет на гласовия трафик и сигнализиращите протоколи. Изискване към IP инфраструктурата е поддържането на тези механизми. Поради високата чувствителност на гласовите данни към закъснение и загуба на пакети, времето за възстановяване на функционалността на IP мрежата при отпадане на връзка или устройство трябва да бъде сведено до минимум.

2.4. Безжични IP телефонни мрежи

С нарастващата употреба на безжични IP мрежи, използващи високоскоростните Wi-Fi стандарти IEEE 802.11b/g/a, и с все по-широкото навлизане на VoIP технологиите се наблюдава развитието на нов аспект на VoIP комуникациите – безжична IP телефония. При нея са налице същите предимства, налични при изграждане на VoIP мрежа, обслужваща стационарни апарати, като същевременно безжичните IP телефони предлагат и същата функционалност, като настолните модели. Вече съществуват производители на GSM телефони, предлагащи модели, способни да обслужват както разговори през обществените клетъчни мрежи, така и през безжични VoIP мрежи. По този начин се осигурява прозрачно за потребителите превключване между корпоративната и обществената телефонна мрежа, водещо до редица улеснения и спестяване на разходи.

Основни проблеми при използването на Wi-Fi мрежите за предаване на гласови данни са обхвата на действие на точките за достъп и сигурността. Въпреки, че безжичните мрежи са уязвими към много от проблемите със сигурността, засягащи стационарните мрежи за данни, те също така могат да се възползват от предлаганите за тях решения. За разлика от до голяма степен унифицираните потребителски системи за работа с данни, базирани предимно на Windows, липсата на утвърдени стандарти при операционните системи на мобилните IP телефони не позволява голям брой устройства да бъдат едновременно засегнати от една и съща атака или вирус. Производителите на защитен софтуер вече предлагат продукти, сканиращи устройствата при тяхното свързване към IPT мрежата, както и съществуват разработки на антивирусен софтуер за мобилни устройства.

От гледна точка на проектирането и изграждането на мрежовата инфраструктура, съществуват някой особености при интегрирането на безжична IP телефония. При конфигурирането на виртуалните локални мрежи, обслужващи крайни VoIP устройства, се поставя за цел ограничаването им до комутаторите за достъп. По този начин се намалява покриващото им дърво и се постига по-бързо синхронизиране на устройствата. Съществуват някой изключения на това правило, като едно от тях се отнася до употребата на безжични IP телефони [1]. За да бъде

възможно използването на безжичните телефони в роуминг, връзката между тях трябва да се осигури на второ ниво от OSI модела. Това се постига чрез създаването на една VLAN мрежа, обслужваща всички безжични IP телефони и обхващаща цялото ниво на достъп. По този начин се осигурява връзка между всички мобилни устройства, независимо от тяхното местоположение, тоест към кой комутатор за достъп е свързана точката за достъп, чийто услуги ползват. Тъй като всяка VLAN мрежа се характеризира със собствено покриващо дърво, то VLAN мрежата, обслужваща безжични устройства ще бъде единствената засегната от по-дълго време за възстановяване на свързаността след евентуално отпадане на устройство или възникване на друг проблем.

2.5. Електрическо захранване на IP телефони

Съществуват две възможности за осигуряване на електрическо захранване на IP телефонните апарати. Едната от тях е телефоните да бъдат захранвани с адаптери от електрическата мрежа, втората е чрез подаване на необходимото захранване през Етернет мрежата - Power over Ethernet (PoE) [13]. При PoE за захранване на крайните устройства се подава 48 V DC през стандартното структурно окабеляване на разстояние до 100 метра. Освен стандартът IEEE 802.3af описващ PoE, се използват и някой фирмени решения.

IP телефоните могат да бъдат захранвани или по усукана двойка от структурното окабеляване, използвана за пренос на данни или по неизползвана такава. Причината за съществуването на тези две възможности е употребата в някой мрежи на комутатори, неподдържащи PoE. В този случай могат да бъдат използвани пач панели за осигуряване на захранване, като LAN кабелът, идващ от комутатора за достъп минава през пач панела, който от своя страна подава захранване през неизползван за данни чифт. Когато комутаторите за достъп поддържат PoE, за захранване и данни се използват едни и същи чифтове.

Различните модели IP телефони може да изискват различно захранващо напрежение. При включване към мрежата на устройство, изискващо електрическо захранване, комутаторът първоначално подава напрежение със зададена по

подразбиране стойност. По време на инициализацията си устройството изпраща съобщение, оказващо напрежението, необходимо за функционирането му. В отговор на това комутаторът може да промени подаваното напрежение. Така се избягва подаването на по-ниско или по-високо от необходимото напрежение, както и необходимостта от ръчно конфигуриране на отделните портове.

При инсталиране на голям брой устройства (IP телефони, безжични точки за достъп и други), захранвани през Етернет мрежата, е важно да се вземат предвид, както изискването за по-голяма захранващата мощност на хардуера, предлагащ PoE, така и допълнителното количество отделяна топлината. PoE комутаторите консумират три до четири пъти повече електроенергия и отделят съответно по-голямо количество топлина. Това налага по-стриктно следене на всички изисквания по отношение на работната температура на хардуера и осигуряване на климатизация в помещенията с мрежово оборудване.

Основно предимство при използването на PoE е осигуряването на необходимата за VoIP оборудването надеждност. Електрическите компании, захранващи жилищните и офис сградите обикновено гарантират 99.9% наличност на предлаганите услуги. Това съответства на приблизително 48 часа годишно липса на захранване. Противно на това, с използването на UPS устройства за захранване на комутаторите за достъп, се осигурява над 99.999% надеждност за свързаните към тях телефони. Тъй като IP телефоните, до които достига само работеща мрежова връзка, но не и електрическо захранване, не могат да изпълняват своите функции, компаниите, които не са имплементирали PoE, не могат да осигурят надеждност от 99.999% на мрежовата инфраструктура, при положение, че захранването на IP телефоните е с 99.9% наличност. Това ще означава надеждност от 99.9% за цялата VoIP система, тъй като тя се определя от надеждността на най-слабото звено, в случая електрическото захранване.

Телефонните компании гарантират осем часа работа след спиране на захранването. Тъй като не съществуват стандарти и регулационни изисквания относно PoE, общоприета практика е осигуряването на до два часа функциониране на IP телефоните при липса на захранване. Счита се, че това време е достатъчно при аварийни ситуации за осъществяване на връзка със спешните служби.

3. Основни предимства на VoIP

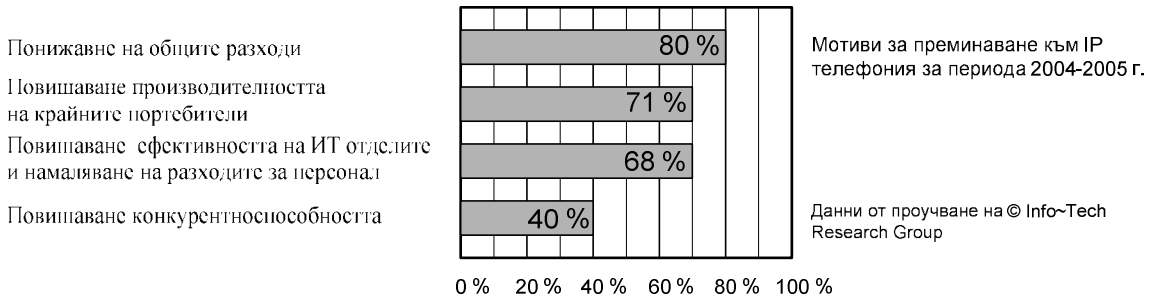
3.1. Бизнес стимули за имплементиране на VoIP

Въпреки, че мотивите на всяка компания за преминаване към IP телефония са толкова уникални, колкото и самата компания, проучвания показват, че основните очаквания от миграцията са почти винаги едни и същи и включват [14]:

- Понижаване на общите разходи
- Повишаване производителността на крайните потребители
- Повишаване ефективността на ИТ отделите и намаляване на разходите за персонал
- Повишаване конкурентноспособността

Разликата в цената да се прави бизнес днес и цената, на която ще се прави същият бизнес след внедряването на тази технология е основният критерий за успехът от преминаването към IP телефония (Фиг. 3.1).

Фигура 3.1. Основни бизнес стимули



3.1.1. Понижаване на общите разходи

При първото представяне на VoIP технологията през 1995 година, анализите предричат понижаване на общите разходи за бизнес комуникации на компаниите,

избрали да заменят традиционните си телефонни системи. Въпреки това, ранните форми на VoIP не са в състояние да задоволят очакванията на част от тези компании. Основната причина е използването на Интернет като транспортна среда, който макар и доказал своята ефективност при преноса на данни за множество приложения, не е предоставял надеждна преносна среда за телефонни комуникации. С въвеждането на протоколи, осигуряващи качество на услугите и в публичните IP мрежи, съвременните VoIP технологии предлагат възможности за значително намаляване на разходите, свързани с обслужването на самостоятелна телефонна мрежа, без необходимост от компромиси с качеството на гласа. За това допринасят редица фактори, които могат да бъдат разделени в следните основни категории:

3.1.1.1. Намаляване на фиксираните телефонни такси

Традиционните телефонни линии биват наемани от локални оператори, налагащи фиксирани месечни такси за обслужване на линия, както и такса за откриване на нова телефонна линия. Проучвания показват, че с въвеждането на IP телефония, обслужваща междуофисните комуникации, броят на необходимите телефонни линии, наемани от традиционен оператор, може да спадне с до 95% [8].

3.1.1.2. Отпадане на таксите за допълнителни услуги

Преминаването към VoIP не само предоставя възможност за използване на множество допълнителни услуги, но и всяка от тях е напълно безплатна. При линиите, наети от традиционните телефонни компании, всички допълнителни услуги биват таксувани отделно от провежданите разговори. Такива услуги са използване на гласова поща, прехвърляне на обаждане, пренасочване на входящите обаждания и други, като тяхното използване винаги води до повишаване на разходите за наетата линия. Макар и това повишение само по себе си да не е съществено, при компании използващи стотици или дори хиляди телефонни линии, този натрупващ се разход е значителен.

3.1.1.3. Съкращаване на таксите за междуселищни разговори

Извършването на телефонни обаждания през частните корпоративни мрежи за данни значително намалява месечните телефонни сметки на компаниите. Размерът на тези спестявания зависи, както от количеството на разговорите вътре в компанията, така и от отдалечеността на отделните й офиси. Компаниите с интернационални офиси реализират значително намаляване на разходите, елиминирайки таксите за множество международни разговори.

Едно от основните преимущества при имплементиране на VoIP е отпадането на разходите за междуселищни и международни разговори до отдалечените корпоративни офиси [8]. При традиционната телефония тези разговори минават през мрежата на обществена телефонна компания, като таксите за тях са по-високи от тези за селищни разговори. При наличие на частна глобалната мрежа за данни или VPN тунели, минаващи през Интернет и достигащи до всички офиси, въвеждането на IP телефония напълно премахва този разход. Целият гласов трафик и необходимата сигнализацията преминават единствено през мрежата на компанията, като телефонните компании не участват на нито един етап.

Освен разговорите, при които и двете крайни точки се намират в мрежата на една и съща компания, съществува необходимост и от провеждане на разговори с дестинация, извън пределите на частната мрежа. Макар и разходите за тези разговори да не могат да бъдат напълно избегнати, IP телефонията позволява тяхното значително намаляване. Начинът за това е, трафикът генериран от всеки разговор с начална точка в дадена компания и дестинация извън нея, да бъде пренасян чрез частната й корпоративна мрежа до офиса, намиращ се най-близо до дестинацията на обаждането. На това място данните биват конвертирани и пренасочени към местния телефонен оператор. При този сценарий цената на разговора намалява с увеличаването на участъка, в който за пренос се използва частната WAN мрежа. Ако крайната точка се намира в същото населено място, където е отдалечения офис на компанията, целият разговор бива таксуван като селищен.

3.1.1.4. Понижаване цената на мрежовата инфраструктура

Необходимостта от поддържане и разширяване на две непрекъснато еволюиращи, но отделни мрежи за глас и данни налага на компаниите значителни разходи. С обединяването на всички комуникации върху единна IP мрежа, голяма част от тях могат да бъдат многократно намалени или дори напълно избегнати. При наличие на единна мрежа отпада необходимостта от инвестиции в специализирано телефонно оборудване за всеки отделен офис, примери за което са частните учрежденски телефонни централи и поддържането на отделна ISDN мрежа, предназначена единствено за конферентни връзки. Друг положителен ефект е опростяването на мрежовата инфраструктура, а от там и улесняване на администрирането и разрастването, както и повишаване на гъвкавостта.

В случаите на изграждане на мрежова инфраструктура в нови сгради и помещения, необходимостта от окабеляване за една, а не за две отделни мрежи може да намали разходите с до 50%. Аналогичен е и случая при необходимост от подмяна на окабеляването. При IP телефони с вграден комутатор отпада необходимостта от два отделни кабела, за LAN и телефон, между комуникационния шкаф и розетката в работното помещение. Спестяванията са не само от намаленото количество използвани кабели, пач панели, розетки и други материали, но и от цената на труда и времето за окабеляване.

3.1.2. Повишаване производителността на крайните потребители

Освен чисто финансовите печалби от въвеждането на VoIP, съществуват и редица други преимущества, които са не по-малко значими. Последните анализи на международни компании сочат, че през 2006 г. представата за VoIP като за технология за спестяване на разходи във все по-голяма степен бива изместена от възприемането й като източник на нова функционалност и разширяване на възможностите на фирмените комуникации.

Съществуват тенденции в световен мащаб за насърчаване на служителите, работещи от своите домове. Изграждането на единна мрежа за глас и данни

значително улеснява както тяхната дейност, така и на служителите пътуващи често в командировки и нямащи достъп до телефонните и мрежовите услуги, налични на работното им място. Единната мрежа за глас и данни позволява отдалечените потребители да получат достъп не само до всички мрежови услуги, но и до всички предлагани телефонни услуги. Така става възможно използването на един и същи служебен стационарен телефонен номер независимо от местоположението на служителя, както и достъп до централизиран телефонен указател и централизирана гласова поща. Освен възможността служителите да пренасят своите IP телефони, което е удачно при дълготрайни премествания, съществуват и редица компютърни приложения, симулиращи IP телефони и предлагащи същия набор от функции с възможност за инсталиране върху преносими компютри и PDA устройства.

Възможността всеки VoIP потребител да използва един и същи телефонен номер във всеки даден момент, независимо от офиса или кабинета, в който се намира, е от голямо значение за съвременния бизнес. От една страна това значително облекчава самите служители и комуникациите между тях, позволявайки им да се фокусират върху служебните си задължения, вместо върху търсенето на телефонни номера. От друга, клиентите и бизнес партньорите получават директна връзка с желания служител без да се налага да изчакват прехвърляне на разговора или от тях да се очаква да знаят на кой номер отговаря търсения служител в конкретния момент. За случаите, в които служителите нямат достъп до VoIP мрежата, съществуват приложения, динамично пренасочващи входящите обаждания на базата на предварително зададени правила. Те могат да бъдат задавани индивидуално от всеки потребител чрез интерфейса на IP телефона или чрез приложение, работещо на персоналния му компютър. Пренасочването може да става по различен начин в зависимост от часа на обаждането, типът му, типът на обаждащия се или други критерии. Всяко входящо обаждане може да бъде прехвърлено към IP телефона на служителя, неговият мобилен телефон или пейджър. По този начин се осигурява постоянна връзка с всеки служител, като прехвърлянето на обажданията става мигновено и прозрачно за обаждащите се.

В модела базиран на УТЦ, предоставянето на набора от услуги, налични в централните офиси на компаниите, във всеки един от отдалечените офиси,

означава многократно инвестиране в един и същи хардуер и софтуер. Поради това, често служителите, работещи извън централния офиси, не разполагат с част от тези функции. Това затруднява работния процес при преместване на кадри от един в друг офис, както и от или в централата. В първия случай се налага обучение за работа с новите за потребителя услуги, докато във втория потребителите на системата трябва да се откажат от част от ползваните до този момент от тях услуги. Използването на централизирани VoIP приложения и централизирано обработване на обажданията дава възможност за равнопоставеност на всички потребители относно достъпа им до услуги, без необходимост от допълнителни инвестиции.

С въвеждането на IPT бизнес приложения, всеки IP телефон има възможност да изведе на дисплея си голяма част от типовете информация, съхранявана в базите данни, намиращи се на произволно място в корпоративната мрежа или Интернет. Примери за това са възможността служителите да получат достъп до своя бизнес календар през интерфейса на телефоните в конферентните зали, както и извеждането на телефонния указател на компанията на телефонния дисплей, спестяващо обажданията за справка.

Софтуерните телефони имат същата функционалност, като хардуерните IP телефони, но освен това предлагат и по-голяма гъвкавост в сферите на тяхното приложение. Те представляват софтуерно приложение, работещо на персонален компютър, което в комплект със слушалки и микрофон напълно замества стационарните телефонни апарати. Такъв телефон може да бъде конфигуриран да звъни едновременно или вместо IP телефона на същия потребител. Това намалява нуждата от инвестиции в хардуер и улеснява работата на служителите, давайки им възможност да работят от своя дом, клиентски офис или хотелска стая, запазвайки функционалността и персоналните настройки на служебният им IP телефон.

Традиционните системи за гласова поща са ограничени във възможностите си за свързване към различни телефонни централи, поради използваните от тях частни протоколи и физически връзки. IP системите за предаване на съобщения, както чисто гласови, така и електронна поща и други, позволяват лесна интеграция към IP телефонната мрежа. Въвеждането на IP приложение, заменящо традиционните системи за гласова поща, предоставя възможност за достъп на

всички служители, имащи връзка към IP мрежата, като това става през унифициран интерфейс. В допълнение, тези приложения позволяват конвертиране на съобщенията от гласова в електронна поща и обратно. Така достъпът до всяко съобщение може да бъде осъществен, както през телефонен апарат, така и чрез персонален компютър.

3.1.3. Повишаване ефективността на ИТ отделите и намаляване на разходите за персонал

Въвеждането на единна мрежа за глас и данни улеснява администрирането и води до намаляване на частта от бюджета, предназначена за персонала, обслужващ информационните системи. Използването на УТЦ изисква наемането на специалисти, обучени за работа със специфичните за всеки производител продукти и използваните от тях частни протоколи. Противно на това, единната IP мрежа, пренасяща глас и данни, може да бъде обслужвана от екип с по-общи мрежови познания, което прави компаниите също така по-малко зависими от напускането на ключови специалисти. Това е удобство и в случаите на разрастване и необходимост от наемане на нови кадри.

В случаите на използване на отделни УТЦ в различните офиси на дадена компания, съществува необходимост от наемане на специалисти за поддръжката и обслужването на всяка от тези централи, или сключване на договори с външни фирми за изпълнение на тези задачи. Единната IP мрежа позволява централизирането на тези дейности и по този начин управлението на по-голяма потребителска мрежа с по-малко ИТ персонал. Премахването на необходимостта от наемане на външни фирми дава по-голям контрол върху собствената мрежа, както намалява и времето за реакция в случаите на проблеми или рутинно обслужване.

Според проучване на BERBEE [7] разходите по преместванията на съществуващи потребители, добавянето на нови и промените в настройките на потребителските акаунти могат да достигнат до 14% от годишния бюджет на ИТ отделите. Средностатистически, компаниите преместват своите служители веднъж годишно. При използване на VoIP всеки потребител може сам да инсталира и

премества своя телефон, както и да променя неговите настройки. Това облекчава поддържащия персонал и прави потенциалните спестявания от тези дейности значителни, независимо от размера на компанията. Освен това, повечето VoIP системи позволяват администрирането им да се извършва през уеб браузър от произволен отдалечен компютър. Така отпада необходимостта от използване на услугите на външни фирми за поддръжка в отдалечените офиси.

3.1.4. Повишаване конкурентноспособността

Основната цел на компаниите не е спестяването на разходи. Компаниите съществуват, за да осигуряват печалба, обслужвайки клиенти. IP телефонията повишава конкурентноспособността, като предлага възможност за разработване на специфични за различните отрасли приложения, облекчаващи клиентите при връзките им с компанията.

Добре структурирана VoIP система позволява клиентите да използват един единствен номер при нужда от връзка с даден служител, един и същ интерфейс на гласова поща и една и съща платформа, обслужваща набор от приложения в центъра за обслужване на повикванията. По този начин клиентите получават едно и също обслужване и услуги, независимо с кой офис, отдел или служител искат да се свържат. IP базиран център за обслужване на повикванията позволява гъвкавост и ефективност при прехвърлянето на обаждания, насочвайки клиентите към подходящите служители. Това значително улеснява клиентите и прави компаниите по-конкурентноспособни.

3.2. Приложенията - истинският потенциал на VoIP

За много от компаниите, имплементиращи VoIP, основно предимство са не директните спестявания от месечни такси и поддръжка, а възможността за лесно разработване и внедряване на нови приложения. IP телефонната среда се базира на съществуващи стандарти, протоколи и програмни езици, използвани от широк кръг разработчици на приложения. Това позволява бързото създаване, тестване и

предлагане на пазара на множество приложения, без тяхното обвързване с конкретен производител на хардуер. Тези приложения могат да бъдат както с широка употреба, като системи за гласова поща, така и строго индивидуални, свързани и разработени специално за нуждите на конкретен бизнес. За да може напълно да бъдат разбран потенциалът на VoIP е необходимо телефонните апарати да бъдат разглеждани като мрежови клиенти, подобно на персоналните компютри [5]. Като такива, те имат достъп до мрежови услугите и приложения, използвани ежедневно от потребителите на IP мрежата.

На фигура 3.2 е показано примерно приложение, работещо в IPT мрежа. Този вид приложение служи за информиране на всички служители за предстоящо събитие, в случая за въвеждане на нова система за гласова поща.

Фигура 3.2. Приложение за IP телефони

Използването на IP телефони за разпространение на съобщения значително намалява времето и разходите в сравнение с разпечатването на брошури или използването на електронна поща, предполагащо достъпа на всеки служител до персонален компютър. То също дава възможност за получаване на допълнителна информация само чрез натискането на бутон, имащ съответното означение, което премахва необходимостта от провеждане на обучение на служителите. Целта на подобни приложения е да подобряват ефективността на потребителите на системата при ежедневното изпълнение на служебните им ангажименти. Други примери са предизвестяването за вируси и изпращането на служебни съобщения или повикване на служители. Предимството при предаването на предупреждения за

вируси през телефонната мрежа е бързото им достигане до техните получатели, като известяването става както визуално, така и със звуков сигнал. По този начин съобщението достига веднага до потребителите и не попада в списъка с електронна поща, при което рискът от отваряне на писмо, съдържащо вирус, преди достигане до предупреждението за него, е голям. При групови съобщения предимствата са освен в бързината на разпространяването им и във възможността за обратна връзка. Тя може да се осъществи, като чрез натискане на указан бутон на телефонния апарат повикващият получава потвърждение, че съобщението е прието.

За всяка компания съществуват три до пет ключови дейности, на които тя разчита за своя бизнес успех [5]. За тях са налице точни и не субективни критерии за оценка. Промени, отразяващи се положително на тези критични области водят до покачване на приходите, реализирани от компанията.

Тази концепция е изключително важна при взимане на решения за преминаване към единна IPT мрежа, тъй като положителното влияние върху критичните за бизнес успеха сфери трябва да се тълкува като основен стимул за промяна. Решаваща стъпка в процеса на планиране на бъдеща имплементация е оценяването на нейното влияние именно върху тези ключови дейности. След края на имплементацията въпросът, който ще бъде поставен е не дали решението е работещо, а дали инвестицията в него е оправдана. Отговорът до голяма степен зависи от откриването и разработването на IPT приложения, насочени към повишаване ефективността на дейностите, оценявани като ключови. Целта при изграждането на IP телефонна мрежа не се свежда единствено до провеждане на телефонни разговори, тя е и подобряване на работния процес като цяло, възвръщане на инвестициите и увеличаване на приходите. До колко тази цел ще бъде постигната зависи от влиянието, което бъдещата IPT имплементация оказва върху отговорите на следните въпроси:

- Как да бъдат реализирани по-големи приходи?
- Как може да се ускори разработването на нови продукти?
- Как могат да бъдат намалени и по-добре контролирани разходите?
- Как да се постигне по-голямо удовлетворение на клиентите?

- Как да се постигне по-голямо удовлетворение на служителите?
- Как може да се увеличи продуктивността на служителите?
- Как може компанията да изпъкне пред конкурентите си?

Стремежът на много от компаниите, сменящи или подновяващи телефонната си система, е запазване на текущо наличните функции. За разлика от този остарял начин на мислене, правилният въпрос при преминаване към IP телефонна система е не какви са предлаганите до сега функции, а какви са потенциалните възможности, неизползвани до този момент. По конкретно въпросът е какви са приложенията, които могат да бъдат създадени и които ще допринесат за развитие в най-важните за бизнеса сфери. С изместването на фокуса по този начин и с увеличаването на изискванията към новите технологии, те придобиват все по-голямо въздействие върху съвременния бизнес.

За да могат да бъдат създадени ефективни приложения е необходимо пълно разбиране на работния процес от страна на партньора, отговарящ за тяхното разработване и внедряване. Това налага изграждане на доверие между двете страни, тъй като макар и част от ключовите за компанията инициативи да са видими и публично известни, то някои от тях или конкретни работни процеси свързани с тях са поверителна корпоративна информация. Успехът на приложенията, а до голяма степен и на IPT системата като цяло, зависи от степента, до която разработчиците им разбират важните за клиента им инициативи, ключовите бизнес процеси, помагащи за осъществяването на тези инициативи, както и хората, които участват в тези процеси.

3.3. Възвръщане на инвестициите

Планирането на всяка инвестиция винаги е свързано с изчисляването на периода за нейната възвръщаемост. При инвестиране в традиционни телефонни системи се предполага този период да е от порядъка на пет до седем години. Един от основните мотиви за преминаване към VoIP е намаляването на времето за възвръщане на инвестициите до под две, а в много случаи и до под една година [3].

Това се постига чрез облекчаване на администрирането, намаляване на необходимите за поддръжка ресурси и персонал и спестяване от дублирано окабеляване и хардуер. Не по-малко важен фактор, допринасящ за по-бързата възвращаемост, е възможността за разработване на приложения, насочени към ключови за дадения отрасъл дейности, повишаващи ефективността на работния процес и намаляващи разходите. Фокусът при минимизирането на този период е не толкова върху намаляването на инвестициите, колкото върху откриването на важни бизнес задачи, за които могат да бъдат намерени бързи, евтини и ефективни IPT решения. Целта е постигане на бърза финансова възвръщаемост на инвестициите, направени с цел усъвършенстване на бизнес процеси, допринасящи за общата печалба или за улесняване на крайните потребители. Важен е фактът, че IPT технологията позволява елиминиране на редица разходи, считани за необходими преди нейното въвеждането.

Изчисляването на периода за възвръщане на инвестициите, направени при изграждането на VoIP комуникации се осъществява в три стъпки. Първата от тях е изчисляването на текущите разходи, свързани с телефонната система. Втората е детайлно пресмятане на разходите по изграждането на IPT мрежата, като в тях се включват и тези за необходимото хардуерно оборудване. Третата стъпка се състои в комбинирането на изчисленията от предишните две и получаване на времева рамка за възвръщане на нужните за преминаването към единна мрежа инвестиции. Таблица 3.1 представя примерна схема за изчисления.

Таблица 3.1 Изчисляване на ROI

Месечни такси преди въвеждане на VoIP	4367
Месечни такси след имплементиране на VoIP	1863
Общи месечни спестявания	**2504**

Цена на необходимия нов хардуер	22390
Цена на труд за инсталиране на хардуера	1200
Цена на труд за изграждане на VoIP мрежата	1000
Обща цена на имплементацията	**24590**

При горния пример периодът на възвръщаемост е 9.82 месеца. Възвръщаемостта на инвестициите, изчислена на базата на този период, е процента от направените разходи, възстановени през първата година, който в разгледания пример е 122 %. Тези цифри ще бъдат различни за всяка отделна компания, но като цяло описват бизнес предимствата при изграждането на VoIP комуникации.

В заключение, факторите влияещи на възвращаемостта на инвестициите при имплементиране на IPT са:

- Занижени разходи за мрежова инфраструктура
- Занижени административни разходи
- Занижени разходи по поддръжката
- Занижени месечни такси
- Внедряване на приложения, оптимизиращи ключови за конкретния отрасъл дейности

4. Използвани технологии

4.1. Протоколи

VoIP протоколите се разделят на два вида:

- Протоколи за управление и сигнализация
- Протоколи пренасящи гласовите данни

Голяма част от тези протоколи са стандартизирани от водещи организации в сферата на комуникациите, като Международния телекомуникационен съюз (ITU) и Съюза на Интернет инженерите (IETF). Съществуват и патентовани фирмени разработки, запълващи празнини в стандартните протоколи или добавящи продуктово зависима функционалност.

4.1.1. Протоколи за управление и сигнализация

Задачата на сигнализиращите протоколи е осъществяването и прекратяването на връзки между две или повече крайни устройства. Най-често използваните протоколи за сигнализация в IP телефонните мрежи са:

- H.323 (peer-to-peer модел)
- Session Initiation Protocol (SIP) (peer-to-peer модел)
- Media Gateway Control Protocol (MGCP) (модел клиент/сървър)
- Megaco/H.248 (модел клиент/сървър)
- Skinny Client Control Protocol (SCCP) (модел клиент/сървър)

4.1.1.1. H.323

Първоначално H.323 е разработен като протокол за осъществяване на механизъм за предаване на мултимедиен трафик в локалните мрежи [22]. Въпреки,

че той все още се използва от редица производители за предаване на видеоконферентни връзки, нуждите на VoIP са довели до неговата еволюция. H.323 има пълния набор от функции, необходими за създаване и поддържане на сесия между крайни устройства. На транспортното ниво протоколът, използван при пренос на аудио и видео данни е UDP, докато за управление и сигнализация се използва TCP. H.323 се състои от система от подпротоколи, всеки от които е отговорен за различен аспект от създаването на връзка.

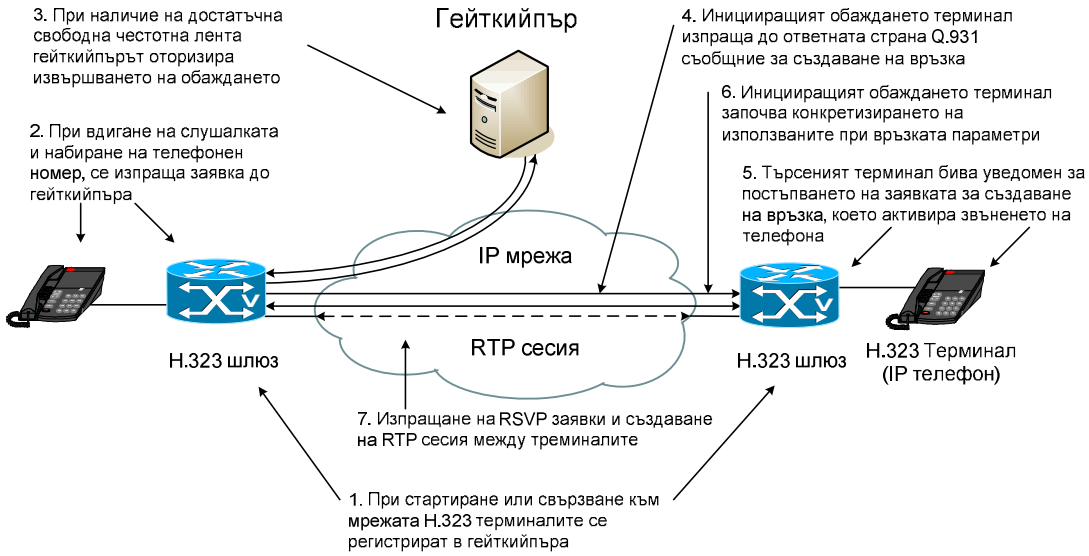
- H.225 е опростена версия на Q.931 и отговаря за изграждането на IP връзка между две крайни H.323 устройства.
- H.245 предоставя възможност крайните устройства да договарят параметрите на връзката, например кодеците, които всяко от тях може да използва, тип на предаваната информация (глас, видео), както и определя коя крайна точка е водеща и коя - подчинена
- RAS H.323 се използва от крайните устройства за комуникацията им с гейткипърите с цел управление на тяхната регистрация, достъп и състояние

Основни компоненти при работата на H.323 са шлюзовете и гейткипърите. Шлюзовете служат за преход между различни протоколи, като едновременно изпълняват ролята на крайна точка на H.323 мрежата и интерфейс към други мрежи. Функцията на гейткипърите е централизирано управление на разрешението за връзки, сигнализацията във VoIP мрежата и разпределение на честотната лента. Гейткипър и управляваните от него медиа шлюзове формират H.323 зона (Фиг.4.1). Архитектурата на H.323 не налага изрично наличието на гейткипър, но той помага за обхващането на по-големи мрежи, отделяйки функциите по контрол и управление на обаждането от медиа шлюзовете.

Спецификацията на H.323 е по-тежка в сравнение с другите сигнализиращи протоколи, като съществуват някой недостатъци, свързани с мащабируемостта на IP мрежата. Един от проблемите, свързани с това, е използването на TCP базирани връзки и необходимостта от множество едновременни сесии, значително

натоварващи мрежата. Това е основен проблем при текущо наложилата се версия 2 на H.323, като той до голяма степен е решен от следващите я версии 3, 4 и 5.

Фигура 4.1 Свързване на телефонно обаждане с използване на H.323 сигнализация



4.1.1.2. Session Initiation Protocol

SIP е лек, текстово базиран сигнализиращ протокол, работещ на приложното ниво от OSI моделът. Той е разработен от IETF като система за сигнализация между потребители на телефонни приложения и обмен на съобщения в IP мрежи. За транспортни протоколи се използват TCP или UDP. Архитектурата на SIP наследява някой от принципите на HTTP и SMTP с цел опростяване, ефективност и лекота при разширяване на VoIP мрежата. Основната функция на SIP е създаването на мултимедийни сесии. Те могат да бъдат разделени в три категории: мултимедийни конференции, телефонни обаждания и разпространение на мултимедийни данни. Процеса на създаване на сесия включва изпращането на “покани” под формата на Session Description Protocol (SDP) съобщения. Чрез тях участниците в сесията уточняват параметрите на бъдещата връзката. Възможно е изграждането на сесии както между двама, така и между повече потребители, като

поканите за тях могат да бъдат изпратени и от потребител, който не е участник в сесията.

Типовете хардуерни компоненти, съставящи SIP мрежа, се различават от използваните при H.323. Крайните устройства, наречени потребителски агенти, се разделят на два вида – клиентски и сървърни. Клиентските устройства са тези, иницииращи заявки, докато функцията на сървърните агенти е следене за заявки и при наличие на такива вземане на решения за тяхната обработка. Обикновено крайните устройства могат да изпълняват и двете функции, но по време на транзакция изпълняват само една от двете. Конкретната им роля зависи от устройството, иницииращо връзката.

Междинните елементите на SIP мрежата, маршрутизиращи трафика, са наречени SIP сървъри и могат да бъдат категоризирани в три групи – прокси сървъри, пренасочващи сървъри и сървъри за регистрация.

SIP улеснява мобилността, като пренасочва повикванията към текущото местоположение на потребителите, използвайки данни от сървърите за регистрация. Заявките за регистрация на местоположението на SIP клиентите се обработват на базата на техния IP адрес, e-mail или URL. Често тези сървъри са физически обединени с прокси или пренасочващите сървъри.

Съществуват два модела за работа на SIP мрежата – клиентите могат да сигнализират, използвайки прокси сървър или пренасочващ сървър [6].

- При първия модел, клиентите изпращат своите заявки за връзка до прокси сървъра, който от своя страна ги обработва или пренасочва към друг SIP сървър (Фиг. 4.2). Прокси сървърите могат да скрият самоличността на изпращащия заявката, като я препращат от свое име. За ответната страна поканата за сесия има за подател прокси сървъра. Други функции, изпълнявани от прокси сървърите, са автентикация, авторизация, контрол върху достъпа до мрежата, маршрутизиране и сигурност. Ролята им е сходна на изпълняваната от гейткипърите в H.323 мрежите.

Фигура 4.2. Свързване на телефонно обаждане с използване на SIP сигнализация и прокси сървър

- При пренасочване на обажданията SIP сървърът, получил заявка за връзка, не я осъществява от името на клиента, а след проверка в базата данни, връща адреса на търсения потребител (Фиг. 4.3). Имайки желания адрес, иницииращият връзката сам извършва сигнализирането без използване на посредник.

Фигура 4.3. Свързване на телефонно обаждане с използване на SIP сигнализация и пренасочващ сървър

4.1.1.3. Media Gateway Control Protocol

За разлика от H.323 и SIP, които са peer-to-peer протоколи, MGCP е базиран на модела клиент/сървър. Описан в RFC 2705, MGCP е вътрешен за разпределена система протокол, която изглежда за външния свят като единичен шлюз. Функциите на традиционната телефонна централа се разпределят между основните компоненти на MGCP – медиа шлюз и медиа шлюз контролер. По този начин се улеснява независимото управление на всеки VoIP комутатор като самостоятелно устройство. За договаряне на параметрите на дадена връзка се използва протокола SDP. Медиа шлюзовете осигуряват прехода между различни типове мрежи, като мрежи с комутация на канали, аналогови или IP мрежи. Те също така информират медиа шлюз контролерите за възникващи събития. От друга страна медиа шлюз контролерите управляват сигнализирането, необходимо за извършване, поддържане и прекратяване на обаждане (Фиг. 4.5). Те дават инструкции на медиа шлюзовете за създаване или преустановяване на връзки при генериране на обаждания. Най-често тези инструкции са за създаване или прекратяване на RTP сесии между крайните устройства.

Фигура 4.5 Свързване на телефонно обаждане с използване на MGCP сигнализация

Сигнализирането между медиа шлюзове и медиа шлюз контролери е под формата на структурирани съобщения, пренасяни от UDP пакети. MGCP е независим от преносната среда и може да бъде използван за управление на ATM мрежи или мрежи с комутация на канали.

4.1.1.4. Skinny Client Control Protocol

Най-разпространения частен протокол за VoIP сигнализация е въведеният от Cisco SCCP. Той е лек протокол, базиран на модела клиент/сървър. Вземането на всички управляващи решения се извършва от мрежови сървър, наречен CallManager. Клиентът, чиято роля се изпълнява от Cisco IP телефон, разполага с минимално количество интелект. Това позволява използването на IP телефони с по-малка процесорна мощ и по-малко памет. CallManager сървърът е отговорен за разпознаването на типа клиент, контрола върху осъществяването и прекратяването на обаждания, изпращането на сигнали за получени гласови съобщения и други. Комуникацията между CallManager сървъра и IP телефоните се извършва чрез SCCP, а в случаите, в които обаждането трябва да бъде пренасочено към не IP мрежа през граничен шлюз, за сигнализиране се използват H.323 или MGCP.

4.1.1.5. Megaco/H.248

Megaco/H.248 е стандарт, породен от общите усилия на IETF и ITU. Той силно наподобява концепциите на MGCP и използва същите наименования на VoIP елементите [18]. Поради това се полагат усилия, насочени към обединяването на двата протокола. Архитектурата на Megaco/H.248 дефинира медийните шлюзове като осигуряващи преход между различни медии, докато медиа шлюз контролерите служат за управление на обажданията. В процеса на изграждане на връзка, Megaco използва серии транзакции, координирани от медиа шлюз контролерите. Основна цел при създаването на Megaco е стандартизирането на хардуера, използван за IP телефония.

4.1.2. Протоколи за пренос на гласови данни

След края на процеса за свързване, комуникиращите крайни устройства могат да започнат обмена на гласови данни. За пренос на тези данни се използва протоколния стек RTP/RTCP/IP/UDP

4.1.2.1. Real-time Transport Protocol

RTP е протокол от приложното ниво на OSI модела, използващ UDP за транспорт и негарантиращ получаването на данните. Той е описан в RFC 1889 и RFC 1890 и осигурява преноса на данни за приложения, работещи в реално време, като интерактивни глас и видео. Допълнителни функции са идентифициране на вида на пренасяните данни, маркиране на пакетите с поредни номера, отбелязване на времето на изпращане и следене за успешното получаване. По този начин RTP предлага възможности за възстановяване на реда на пакетите при получаване, установяване загуба на пакети, сигурност и разпознаване на използваните кодиращи схеми. Разликите в използваните кодеци и в честотата на създаване на пакети водят до разлики в честотната лента, необходима за една RTP сесия. Независимо от това, RTP е протокола с най-големи изисквания към честотната

лента в IP телефонна среда. За две крайни станции, двойката от техните IP адреси дефинира връзката между тях, като гласовият трафик се предава чрез самостоятелна RTP сесия за всяко отделно обаждане.

4.1.2.2. Real Time Control Protocol

Протоколът Real Time Control Protocol е съпътстващ, но не задължителен за работата на RTP. Основна негова функция е осигуряването на информация относно качеството на преноса на данни, извършван от RTP. RTCP не дава информация за мястото, на което възникват проблеми, а единствено, че те съществуват. Въпреки това, RTCP може да се използва за локализиране на проблемните области чрез съпоставяне на информацията, предоставена от всеки отделен медиа шлюз.

RTCP предоставя възможност за следене на качеството на обажданията, отчитайки загубата на пакети, закъснението, джитера и други основни параметри, влияещи на връзката. При проектиране на VoIP архитектура, честотната лента, използвана от контролния трафик трябва да бъде фиксирана като част от необходимата за една гласова сесия. В RFC спецификацията се препоръчва тази част да бъде пет процента от RTP трафика.

4.1.2.3. Compressed RTP

Протоколът Compressed RTP (cRTP) е разновидност на RTP, при която се прилага компресиране на хедърите на IP пакетите. При използване на протоколния стек IP/UDP/RTP, размерът на хедъра на всеки пакет е 40 байта. cRTP намалява този размер до 2 или 4 байта, което значително намалява и необходимата за провеждане на едно обаждане честотна лента. В зависимост от използвания кодек, cRTP дава възможност да бъдат обслужени до два пъти по-голям брой едновременни телефонни обаждания в сравнение с мрежа, използваща RTP.

Ограничение на cRTP е възможността за неговото прилагане единствено върху директни връзки. Причина за това е, че компресирането на IP хедъра до 4 байта не позволява поставянето в него на IP адрес. Това прави невъзможно

маршрутизирането на пакетите и налага тяхното предаване единствено през връзки, за които не е необходима адресация. Друг фактор, който трябва да се вземе предвид при употреба на cRTP, е необходимостта от обработка на пакетите от страна на маршрутизаторите, свързана с компресиране и разкомпресиране на хедърите. Тези операции значително натоварват процесорите на мрежовите устройства, което може да окаже негативно влияние върху качеството на обажданията.

4.2. Кодеци

По своята природа гласовите комуникации са аналогови, докато мрежите за пренос на данни са цифрови. Процеса на преобразуване на аналоговите сигнали в цифрова информация и обратно се извършва с помощта на алгоритъм за кодиране-декодиране, наречен кодек. Съществуват много стандарти, описващи такива алгоритми, повечето от които използват кодиране на сигнали с импулсно-кодова модулация (PCM). В допълнение на конвертиращата си функция, кодеците компресират потока от данни и осигуряват премахване на ехото в сигнала. Компресията на потока намалява изискванията към честотната лента за предаване на VoIP комуникациите. Различните кодеци компресират информацията в различна степен, а някой я предават некомпресирана. Компресията спестява честотна лента, но има и своите негативни страни. Една от тях е обратнопропорционалното съотношение между степента на компресия и толерантността на трафика към загуба на пакети. Пример за това е кодекът G.729, при който загуба на два последователни пакета води до лошо качество с прекъсвания.

В LAN мрежи, където се предполага наличието на достатъчна честотна лента, се препоръчва използването на некомпресиращи кодеци като G.711. Това е така, тъй като компресирането е свързано с допълнително натоварване на процесорите на мрежовите устройства, както и с време за извършване на операцията, допринасящо за по-голямо закъснение на пакетите. За разлика от високоскоростните LAN мрежи, WAN връзките обикновено са със значително по-малка честотна лента, което прави компресирането задължително. Целта е

достигане на желания брой едновременни разговори, без това да налага значително увеличаване на честотната лента. Най-често използваните кодеци са:

4.2.1. Кодек G.711

G.711 се използва по подразбиране от всички производители, както на VoIP оборудване, така и на аналогови телефонни централи. Този стандарт не прилага компресия на гласовия поток, като честотната лента, необходима за една връзка, е 64 Kbps.

4.2.2. Кодек G.729

G.729 е втория най-разпространен кодек и дефакто стандарт при предаване на глас във WAN среда. След прилагане на компресиращия алгоритъм един разговор, кодиран с G.729, заема поток от 8 Kbps, като качеството на говора е незначително по-ниско от това на G.711.

4.2.3. Кодек G.723

G.723 е стандарт, някога препоръчван при необходимост от голяма компресия на данните. Потокът заеман от обаждане, кодирано с G.723, е 6.3 или 5.3 Kbps. Тъй като качеството на говора е значително по-ниско спрямо това на G.729, въпреки необходимата по-малка честотна лента, този кодек не се използва често.

4.2.4. Кодек G.722

G.722 подобно на G.711 използва 64 Kbps за предаване на едно телефонно обаждане, но предлага висока прецизност при преобразуването на речта. Докато при предишните три описани стандарта се кодира аналогов звук в диапазона на 3.4 KHz, G.722 предлага звук с честотна лента 7 KHz. Очаква се този стандарт да стане популярен в бъдеще [17].

Подробните характеристики на кодеците, разгледани по-горе, са описани в таблица 4.1 [19].

Таблица 4.1. Характеристики на най-често използваните кодеци

Кодек	Честотна лента за пренасяне на гласовите данни (Kbps)	Оценка по MOS	Закъснение породено от използвания кодек	Размер на пакета (байтове)	IP/UDP/RTP хедъри (байтове)	Компресиран с cRTP хедър (байтове)	Хедър за втори слой (байтове)	Обща необходима честотна лента	Обща необходима честотна лента при непредаване на паузите в речта
Ethernet									
G.711	64	4.1	1.5	160	40		14	85.6	42.8
G.711	64	4.1	1.5	160		2	14	70.4	35.2
G.729	8	3.9	15	20	40		14	29.6	14.8
G.729	8	3.9	15	20		2	14	14.4	7.2
PPP									
G.711	64	4.1	1.5	160	40		6	82.4	41.2
G.711	64	4.1	1.5	160		2	6	67.2	33.6
G.729	8	3.9	15	20	40		6	26.4	13.2
G.729	8	3.9	15	20		2	6	11.2	5.6
G.723	6.3	3.9	37.5	30	40		6	16	8
G.723	6.3	3.9	37.5	30		2	6	8	4
Frame Relay									
G.711	64	4.1	1.5	160	40		4	81.6	40.8
G.711	64	4.1	1.5	160		2	4	66.4	33.2
G.729	8	3.9	15	20	40		4	19.7	9.9
G.729	8	3.9	15	20		2	4	9.6	4.8
G.723	6.3	3.9	37.5	30	40		4	15.5	7.8
G.723	6.3	3.9	37.5	30		2	4	7.6	3.8
ATM									
G.711	64	4.1	1.5	160	40		5 клетки	106	53
G.711	64	4.1	1.5	160		2	4 клетки	4	42.1
G.729	8	3.9	15	20	40		2 клетки	2.3	14.1
G.729	8	3.9	15	20		2	1 клетки	14.1	7.1
G.723	6.3	3.9	37.5	30	40		4 клетки	22.3	11.1
G.723	6.3	3.9	37.5	30		2	4 клетки	11.1	5.6

4.3. Методи за оценяване качеството на гласовия сигнал

Оценката на качеството на предавания гласов сигнал може да стане чрез използването на обективен или субективен подход [13]. Оценяването, извършвано с

помощта на компютър, се счита за обективен метод, докато определянето на качеството на базата на човешка преценка за субективно. При разработване и настройване на параметрите на кодеците се използват субективни критерии. Стандартните обективни методи, като тоталното хармонично изкривяване и процентното измерване на шума спрямо гласовия сигнал, не винаги отразяват точно човешката преценка, което обикновено е целта на повечето техники за оценяване на качеството.

4.3.1. MOS

Общоприет метод за субективно измерване на качеството на речта е MOS (Mean Opinion Score) – оценка на разбираемостта на говора. Тестването чрез MOS се извършва, като едни и същи тестови фрази биват изговаряни последователно от мъж и жена на група слушатели през една и съща комуникационна среда. Поради факта, че качеството на говора и звука са субективни за всеки индивид, препоръчително е подбирането на разнородна група слушатели и тестови фрази. След изслушването им, слушателите определят тяхната оценка със стойности между едно и пет, където едно отговаря на лошо, а пет отлично качество. Тестването чрез MOS се използва както за сравняване на различни кодеци, така и за сравнение на качеството на даден кодек при различни обстоятелства, като промяна в нивото на външния шум, няколкократно кодиране и декодиране на сигнала и други. Изискването за повече от един слушател при определяне на качеството на говора прави невъзможно прилагането на MOS в реално време и извън лабораторна среда.

Невъзможността за използване на MOS в реална работна среда налага създаването на обективен метод за анализиране качеството на речта – PESQ (Perceptual Evaluation of Speech Quality). PESQ е стандарт на ITU, описан в публикация P.862, измерващ изкривяванията на гласовия сигнал при преминаването му през VoIP мрежа. Въпреки сравнително добрите резултати съществуват случаи, в които PESQ дава висока оценка на разговори с лошо качество и обратно.

4.3.2. E Model

Друг стандарт на ITU, известен като E моделът е G.107. Този модел отчита характеристиките при възприемане на речта и дава оценка на качеството й, вариращa между 0 и 100. Например, практически възможните стойности при оценяване на кодека G.711 са между 50 и 94. Формулата за тяхното изчисляване е R=Ro-Is-Id-Ie+A, където:

- Ro е критерий, формиран от силата на звука
- Is е фактор, отнасящ се до понижаване на качеството по време на речта
- Id е фактор, отнасящ се до деградация на качеството, появяваща се със закъснение относно речта
- Ie отразява негативно влияние на мрежовите устройства върху качеството
- A е фактор, определящ преимуществото

E моделът е лек протокол, независещ от размера на тестваната мрежа, даващ възможност за извършване на периодични проверки на качеството на речта по време на разговор.

4.3.3. RTCP XR

Друг протокол, измерващ качеството на VoIP връзките е стандартът, разработен от IETF – RTCP XR (RTP Control Protocol Extended Reports). RTCP XR може лесно да бъде софтуерно имплементиран както в IP телефони, така и в шлюзове. Метриките, използвани за измерване на качеството, са брой загубените или отхвърлени пакети, закъснение, шум и ниво на ехото в сигнала, като тежестта на всяка от тях може да бъде конфигурирана. Съобщенията, съдържащи конкретни стойности на тези параметри, могат да бъдат прихванати и декодирани от протоколен анализатор или да бъдат извлечени с помощта на SNMP и подадени за обработка в система за оценка на мрежовата производителност.

5. Възможни проблеми и фактори, влияещи на качеството на предаване на гласови данни през IP мрежа

5.1. Качество на услугите

Качеството на услугите е основно изискване при VoIP мрежите. Въпреки възможните ценови предимства и голямото разнообразие от функции и услуги, ако VoIP телефонията не е в състояние да предложи качество, поне еквивалентно на това на класическите телефони, то прилагането й би изгубило смисъл [20]. За по-голямата част от трафика, преминаващ през IP мрежа за данни, закъсненията и загубата на пакети не са критични. Пакетите, пристигнали в неправилен ред, биват буферирани и след пристигане на закъснелите пакети, редът им бива възстановен, а липсващите се изпращат отново. Противно на това, гласовите данни са свръхчувствителни към забавяне и загуба на пакети, което води до влошаване качеството на връзката. Съществуват редица фактори, влияещи негативно на качеството на услугите. Това са:

- Надеждност
- Ширина на честотната лентата
- Закъснение
- Джитер
- Загуба на пакети
- Сигурност

5.1.1. Надеждност

Надеждността може да се дефинира като вероятността даден продукт или услуга да работят, когато са необходими. При покупката на продукт или услуга, от тях се очаква да бъдат надеждни. Мрежа, която не е надеждна е не само неудобна, тя е и скъпа. При все по-голямата зависимост от компютърните мрежи за

изпълнението на бизнес приложения и пренос на глас, неработещата мрежа коства както ценно време, така и средства.

Често повод за размисъл при преминаване от традиционна към IP телефония е надеждността на бъдещата система. Това е така, защото потребителите са свикали с почти постоянната наличност на използваните от тях телефонни услуги. Стандартна цел е постигането на 99.999% надеждност, което означава не повече от 5.3 минути годишно, в които системата да не работи. При IP телефонните мрежи това може да бъде постигнато с подходящо планиране, проектиране, внедряване и експлоатация на системата [10].

Счита се, че традиционните телефонни системи имат 99.999% надеждност. Истината е, че те постигат това чрез дефиниране на надеждността по начин, който намалява тежестта на компонентите, за които няма резервиране. Оценяването на IP телефонното решение на Cisco, използвайки индустриални стандарти за теоретична оценка на надеждността, показва, че то също постига търсените 99.999% време на работоспособност. Приложен е методът за анализ на средното време между отказите (CBMO), разработен от Telcordia (бивша Bellcore), при който се оценяват поотделно софтуера, хардуера, електрическото захранване и надеждността на проектирането на мрежата.

Производителите на класическите централи постигат търсената надеждност, считайки системата за неработоспособна само в случаите на проблеми в самата централа. Тази дефиниция не обхваща от край до край процеса на едно обаждане, тя изключва проблемите, свързани с повредени телефони, липса на захранване или прекъснати жици. По сходен начин Cisco дефинират надеждността на своята IP телефонна система, като възможност за осъществяване и провеждане на обаждания в границите на двата най-горни резервирани слоя на мрежовата архитектура, с използване на резервиран Cisco CallManager. При този сценарий, проблем в който и да е отделен хардуерен компонент или софтуерен продукт ще предизвика превключване към неговия резервен дубликат. Така, чрез резервираност на основните мрежови елементи и четири часа средно време за ремонт (CBP), IP телефонната мрежа постига 99.999% работоспособност. Как е достигнато до този извод е обяснено по-долу.

Важно е да се отбележи, че в своята дефиниция за надеждност Cisco изключва компонентите, намиращи се на най-долния слой от мрежовата архитектура – слоя за достъп до мрежата. Обикновено един комутатор в този слой поддържа около 120 потребителя, което е съизмеримо с броя линии, поддържани от една карта на класическа телефонна централа. Производителите на тези телефонни централи също изключват слоя за достъп от своето определение за надеждност. В противен случай желаните 99.999% работоспособност не биха били достижими. Cisco също не биха постигнали тази надеждност без резервиране. Обикновено СВМО на един комутатор за достъп до мрежата е между 60000 и 150000 часа. При средна стойност от 100000 часа и четири часа СВР, теоретичната надеждност е 99.996% или 21 минути неработоспособност годишно. Очевидно е, че не е възможно лесно да се постигне 99.999% надеждност между две крайни точки, нещо повече – целта на доставчиците на традиционните гласови услуги е постигане на 99.95% време на работоспособност за крайните потребители.

За пълен анализ на IP телефонна система е необходимо да се разгледат и оценят поотделно следните елементи, влияещи на надеждността й:

- Хардуер
- Софтуер
- Среда за пренос
- Електрическо захранване
- Мрежовото проектиране

Разгледана е система с внедрена N+1 резервираност на опорния слой, разпределителния слой и CallManager сървърите. Устройствата в слоя за достъп, както и средата за пренос, не са включени в анализа.

5.1.1.1. Надеждност на хардуерните компоненти

Надеждността на хардуера се определя с помощта на метода на Telcordia – "Преброяване на частите", който анализира СВМО за всички компоненти по пътя

на разговора между точка А и точка Б. При IP телефонните мрежи е необходимо да се разгледат два отделни пътя, използвани при осъществяването на едно обаждане. Първият от тях е между IP телефона и Cisco CallManager сървъра, а вторият е между двата телефона или между IP телефона и шлюза за връзка с публичната комутируема телефонна мрежа. Изчисленията за всеки от пътищата се правят поотделно, като устройствата (двойките устройства), влизащи и в двата пътя, се взимат под внимание само веднъж. Зададено е четири часа СВР, което се смята за стандарт при сключване на договори за поддръжка.

Надеждността на дадено устройство се получава като произведение на СВМО на неговите компоненти. Като пример е разгледан комутатор от разпределителния слой (Таб. 5.1 и 5.2).

Таблица 5.1. Надеждност на модулите на комутатор от разпределителния слой

Модул	СВМО	СВР	Надеждност
WS-6509	369,897	4ч.	99.99892%
WS-CAC-1300W	316,456	4ч.	99.99999%
WS-X6K-SUP1A-MSFC2	46,235	4ч.	99.99135%
WS-X6408A-GBIC	93,457	4ч.	99.99572%

Таблица 5.2. Надеждност на комутатор от разпределителния слой (без резервиране)

Надеждност	99.985988%
Неработоспособност за една година	73.7 минути
СВМО	28,545 ч.

След пресмятането на надеждността на отделните устройства, следва да бъде изчислена и надеждността на резервираната паралелната система. Разглежда се само възможността за поява на повреда в резервното устройство през времето,

необходимо за отстраняване на повреда, възникнала в основното резервирано устройство. Тъй като ремонта отнема не повече от четири часа, надеждността на паралелната група е много висока. Дори при успешно превключване между устройствата, всички текущи обаждания биват прекъснати, а осъществяването на нови обаждания е възможно чак след края на превключването. Това е проблем относно надеждността на системата, но той засяга нейното проектиране и за това е разгледан в частта, отделена на надеждността на проектирането. За изчисляване на хардуерната надеждност на резервиращите устройства се използва формулата

$$\text{Паралелна надеждност} = 1 - \left[\prod_{i=1}^{n} (1 - \text{надеждност на устройството}_{(i)}) \right]$$

където "n" е броя на паралелните устройства, а "i" е номера на устройството.
Тогава за надеждността на резервиран комутатор от разпределителния слой се получават следните резултати (Таб. 5.3):

Таблица 5.3. Надеждност на резервиран комутатор от разпределителния слой

Надеждност	99.99999804%
Неработоспособност за една година	< 6 s
CBMO	101,880,673 h

Надеждността на останалите паралелни двойки устройства се получава с аналогични пресмятания, след което може да се определи и надеждността на целия път, необходим за провеждане на телефонно обаждане. В разглеждания пример е използвано резервиране на комутаторите в разпределителния и опорния слой, Cisco CallManager сървъра и шлюза. За определяне на общата надеждност се взима предвид надеждността на всяка двойка устройства, получена, използвайки данните на Telcordia за надеждността на техните компоненти. Единствено хардуера на Cisco CallManager сървърите бива доставян от външни производители и поради това не

са налични изчисления на Telcordia за неговите компоненти. Надеждността може да бъде определена на базата на броя изделия, върнати за ремонт. Моделът MCS 7835 има повече от седем милиона работни часа със CBMO над 1000000 часа за период от три месеца. Така се получават следните резултати за резервираните двойки устройства (Таб. 5.4):

Таблица 5.4. Надеждност на резервираните двойки устройства

	Опорен комутатор	Разпределителен комутатор	Шлюз	Хардуерна платформа на Cisco CallManager
Надеждност	99.99999665%	99.99999972%	99.99999880%	99.99999%
Неработоспособност за една година	< 6 s	< 6 s	< 6 s	< 6 s
CBMO	59,787,111 h	710,343,430 h	166,668,151 h	200,040,000 h

Крайния резултат за надеждността на цялата хардуерна система е 99.99993%, получен чрез умножение на процентите на надеждност на отделните резервирани устройства.

5.1.1.2. Надеждност на софтуера

За точното определяне на надеждността на дадено мрежово устройство е необходимо да се вземе предвид и времето, в което то не работи поради софтуерни проблеми. Към този момент не съществува индустриален стандарт, измерващ надеждността на софтуерни продукти. Най-добрият известен метод е анализиране на данните от практическото използване на даден продукт. От гледна точка на IP телефонните мрежи, трябва да бъде разгледан броят на софтуерните проблеми, довеждащи до неработоспособност на системата при различни версии на мрежовата операционна система (IOS). За CBP се приема 6 минути – време, за което мрежовото устройство може да презареди операционната си система и да възстанови трафика и връзките си при средно голяма мрежова инфраструктура. На

тази база е установено, че IOS 12.1 има 99.99986% надеждност или 71740 часа СВМО. За разлика от IP мрежите, служещи единствено за пренос на данни и използващи стандартни IOS системи, IP телефонните мрежи ползват IOS софтуер класифициран като "нововъведен". Тази разлика трябва да бъде отразена и в изчисленията на надеждността. При тестване на нов софтуер е установен консервативно СВМО от 10000 часа при 6 минути СВР. Също така консервативно се подхожда и към надеждността на стандартния софтуер, като за него се приема 30000 часа СВМО.

Резултатът, получен за софтуерната надеждност, може да бъде прибавен като показател за отделен компонент при пресмятането на хардуерната надеждност. Това е така, защото софтуерните проблеми, довеждащи до неработоспособност на хардуерно устройство или софтуерното му рестартиране са изолирани и влияят единствено на конкретното устройство и то по начина, по който влияят неговите хардуерни модули. Практически наблюдения също показват, че софтуерните проблеми при едното от две резервирани устройства не довеждат до аналогични проблеми и във второто. Според изчисленията, хардуерната надеждност на самостоятелен комутатор от разпределителния слой е 99.98598%. Софтуерната надеждност при 10000 часа СВМО и 6 минути СВР е 99.999%. Това променя надеждността на комутатора на 99.98498%. Надеждността на резервирания разпределителен комутатор се променя съвсем незначително и спада с не-повече от една секунда годишно – от 99.9999804% на 99.99999774%. Тъй като всички изчисления до тук са закръглявани до третия знак след десетичната запетая, то софтуерната надеждност не оказва влияние върху получените резултати.

5.1.1.3. Надеждност на електрическото захранване

Електрическото захранване оказва влияние върху надеждността на цялата IP телефонна мрежа. Отпадането на електрическото захранване, за разлика от проблемите, свързани с хардуера и софтуера, не се отразява само върху дадено устройство, а засяга цяла сграда или множество сгради наведнъж. Това влияе сериозно на теоретичната надеждност на всички устройства, включени в

дефиницията за наличност. При изчисленията са използвани данни, предоставени от APC Corporation. Данните са валидни за повечето части на Европа, Северна Америка и Япония, с изключение на някой по-рискови региони, например щата Флорида, САЩ.

- Средният годишен брой спирания на захранването, достатъчно продължителни за да окажат влияние върху работата на IP телефонната система, е 15.
- 90% от спиранията на захранването са с продължителност по-малка от 5 минути
- 99% от спиранията на захранването са с продължителност по-малка от един час
- Липсата на захранване е около 100 минути годишно.

За постигане на 99.999% наличност на захранването, са необходими дизел генератор и UPS устройства, с батерия, гарантираща минимум един час възможност за работа след отпадане на захранването. Те трябва да осигуряват електричество на всички устройства от разпределителния и опорния слой, както и на шлюзовете и CallManager сървърите. Необходимо е също и наличието на договор за поддръжка, осигуряващ отстраняване на повредите в UPS устройствата и генератора в рамките на четири часа. При тези условия, липсата на електрическо захранване ще бъде не повече от 2 минути годишно, което съответства на 99.99962% надеждност. Това ще повлияе на дотук пресметнатите 99.99993% по начин, по който би повлияло добавянето на нов модул към хардуерно устройство. Така новата цялостна надеждност на системата става равна на 0.9999962 * 0.9999993 или 99.99955%.

5.1.1.4. Надеждност на мрежовото проектиране

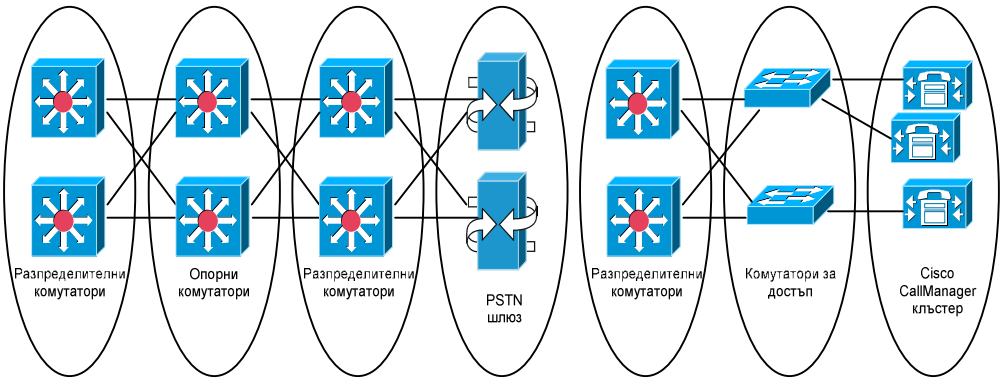
За надеждността на мрежата значение имат проектирането на топологията на мрежата и използваните мрежови протоколи. При неправилно проектирана

мрежа с неподходящи протоколи и конфигурации, времето за възстановяване или прехвърляне на работата към резервиращото устройство лесно може да надхвърли 5 минути, елиминирайки всяка възможност за постигане на търсената надеждност, въпреки усилията за надежден хардуер и софтуер. За постигане на висока надеждност протоколите трябва да могат да установят кога е настъпила повреда и веднага да превключат към резервиращия компонент или устройство. Системата трябва също да следи готовността на резервните компоненти, за да осигури успешно превключване при необходимост. 99.999% надеждност може да бъде постигната при спазване на следните правила за проектиране:

- Проектиране на архитектурата с опорен, разпределителен и слой за достъп
- Използване на EIGRP или OSPF маршрутизиращи протоколи със стандартни стойности на таймерите
- Конфигуриране на HSRP за всички IP подмрежи за достъп, включително тези за IP телефони и CallManager сървъри.
- Използване на RSTP вместо STP
- Свързване на всеки комутатор за достъп към два разпределителни комутатори
- Свързване на всеки разпределителен комутатор към два опорни комутатора
- Избягване трънкинг на устройства от един и същи слой
- Конфигуриране на QoS

Когато тези правила са спазени може да се пресметне надеждността на всеки слой на архитектурата, като се разглежда времето за прехвърляне на работата към резервиращото устройство и възстановяване на всеки от тези слоеве. Важно предположение при този анализ е, че системата разполага с достатъчни ресурси, за поемане на цялото натоварване по време на отстраняване на повредата в някое устройство. На фигура 5.1 са показани различните елементи, които трябва да бъдат анализирани.

Фигура 5.1. Елементи на мрежовото проектиране влияещи върху неговата надеждност



- Разпределителен слой: При повреда на устройство или връзка на този слой могат да бъдат задействани три различни механизми за прехвърляне на работата към резервиращото устройство – HSRP, IP маршрутизиране или STP. Чрез тестове е установено, че това може да отнеме до 30 секунди.
- Опорен слой: Устройствата от разпределителния слой трябва да имат пътища с еднакво тегло за преминаване през опорния слой, което да не налага преизчисляване на маршрутите в IP мрежата за успешното маршрутизиране на трафика при отпадане на някое опорно устройство. Консервативна стойност за нужното време е 10 секунди
- PSTN шлюз: При повреда в PSTN шлюза, CallManager сървъра осъществява обаждането, използвайки списък с алтернативни устройства. Процеса на избор на алтернативно устройство отнема до 10 секунди
- Cisco CallManager сървър и комутатори за достъп: Повреда в комутатора за достъп, със свързан към него Cisco CallManager сървър, предизвиква превключване към резервиращия сървър. Това става, когато не се получат три последователни съобщения, потвърждаващи съществуването на връзката. Стандартно при TCP тези съобщенията се изпращат на всеки 30 секунди т.е. три съобщения за 61 секунди, което прави средно време на неработоспособност 75 секунди.

След определяне на средната продължителност на неработоспособност на отделните елементи, влияещи върху надеждността на мрежовото проектиране, може да бъде направен извод за цялостната му надеждност (Таб. 5.5).

Таблица 5.5. Надеждност на мрежовото проектиране

	Разпределителен комутатор	Опорен комутатор	Комутатор за достъп	Шлюз	Cisco CallManager
СВМО при софтуера	10,000 h	30,0000 h	30,000 h	10,000 h	0,000 h
СВМО при хардуера	28,545 h	21,866 h	75,380 h	36,511 h	40,000 h
Честота на годишните софтуерни откази (%)	.876 (365*24/ 10,000 = .876)	.292	.292	.876	.876
Честота на годишните хардуерни откази (%)	.306	.401	.116	.240	.219
Обща честота на отказите (%)	1.182	.693	.408	1.116	1.095
Продължителност на отказите	30 s	10 s	75 s	10 s	75 s
Усреднено време на неработоспособност за година	35 s	7 s	31 s	11 s	82 s

От представените данни следва, че общото време на неработоспособност на мрежовите устройства, свързано с мрежовото проектиране е 166 секунди годишно, което съответства на 99,99947% надеждност.

След като са налични резултатите за надеждността на хардуера, софтуера, електрическото захранване и мрежовото проектиране, е възможно да бъде пресметната цялостната надеждност на IP телефонната система. При същия принцип на изчисления се получава 0.9999962*0.9999947*0.9999993 или 99.999% наличност, което е приблизително 5.3 минути неработоспособност годишно.

Направеният анализ доказва високата надеждност на VoIP телефонните мрежи, изградени при зададените правила. Поради това, опасения относно надеждността на системата са неоснователни при взимането на решения за бъдеща миграция към единна мрежа за глас и данни.

5.1.2. Ширина на честотната лента

Определянето на необходимата за качествени гласови комуникации ширина на честотната лента е важна задача при изграждането на VoIP мрежи. Както и при мрежите за данни, недостатъчната честотна лента може да доведе до загуба на пакети и други проблеми, свързани с качеството на услугите. Едно от големите предимства на VoIP – обединяването на глас и данни в единна мрежа, налага взимането на сложни решения при разпределянето на честотната лента между тях. Като цяло, гласовите услуги са по-чувствителни към липса на честотна лента отколкото другите мрежови услуги и затова трябва да има приоритет при предаването на техния трафик. Мрежовите задръствания, породени от липса на честотна лента, водят до увеличаване на размера на опашките в устройствата и съответно до закъснения на VoIP пакетите. Недостатъчна честотна лента може да доведе до джитер, тъй като VoIP пакетите биват изпращани спорадично, изчаквайки останалия трафик. Според направени тестове, загубата на пакети ще бъде пренебрежимо малка в мрежи, в които закъснението е по-малко от 100 ms и джитера не надвишава 40 ms.

Ако една VoIP мрежа използва същото кодиране, прилагано при класическите телефони, необходимата й честотна лента ще бъде по-голяма, поради нуждата от служебни протоколи, обслужващи обажданията. За разлика от традиционната телефония, при която за всяко обаждане има отделен канал с фиксирана честотна лента, VoIP обажданията могат да използват методи, като компресия на гласовия поток, компресия на RTP хедърите и следене на активността на говорещите (VAD), с цел намаляване на трафика. Следенето на активността на говорещите се използва, за да се избегне предаването на празни пакети по времето, в което и двете страни не говорят.

Изчисляването на необходимата честотна лента се базира на очаквания най-голям брой едновременни обаждания. Всяко претоварване на мрежата с обаждания над предвидения брой би довело до влошаване на качеството на всички обаждания. Формулата за изчисляване на честотната лента, необходима за гласовия трафик, тоест само за RTP е:

Битове за сек = сампли в сек*размер на пакета*брой обаждания*8 бита за сек
Сампли в сек = 1000 ms / интервал на създаване на пакет в ms

Пример: За 2000 пълен дуплекс обаждания кодирани с G.711, имащи интервал на създаване на пакети от 20 ms и размер на пакета 200 байта (40 байта IP хедър и 160 байта данни), необходимата честотна лента е 160 Mbps :

50 сампли в сек = 1000 ms / 20 ms

160 Mbps = 50 * 200 * 2000 * 8

За получаване на общата необходима честотна лента, трябва да се вземе предвид и трафика, породен от протоколите за сигнализация и протоколите на каналния слой. Честотната лента, необходима за сигнализация, зависи от интервалите, през които се генерират обаждания и от конкретния използван протокол. Ако голям брой обаждания бъдат направени в кратък интервал от време, то честотната лента, нужна за сигнализация може да бъде значителна. Общо правило е за протоколите за сигнализация да се отделя около 3% от честотната лента, използвана за пренасяне на гласови данни. При разгледания пример, ако всичките 2000 обаждания бъдат извършени в интервал от една секунда, честотната лента нужна за сигнализация ще бъде 4.8 Mbps. Тогава необходимата честотна лента при направените предположения за размер на пакета, използван кодек, интервал на извършване на обажданията и брой на обажданията ще бъде 164.8 Mbps. Промяна дори в едно от тези предположения ще доведе и до промяна в необходимата честотната лента.

Освен използвания кодек, броят на семплите в пакета е също фактор, влияещ при определянето на честотната лента, необходима за едно обаждане. Размерът на сампъла зависи от използвания кодек, но броят на семплите, включени в пакета, определя колко пакета биват изпращани за една секунда (Таб. 5.6). Поради тази причина той оказва влияние върху честотната лента, необходима за едно обаждане.

Пример за това е разговор, кодиран с G.711, който използва 80 байта за кодиране на сампъл и сампъл честота 10 ms. Необходимата честотна лента за разговор при един сампъл за пакет ще бъде:

80 B + 20 B за IP +12 B за UDP + 8 B за RTP = 120 байта за пакет
120 B за пакет * 100 пакета в секунда = 12000 * 8 бита / 1000 = 96 Kbps за обаждане

При същите характеристики на обаждането, но при два сампъла в пакет изчисленията са:

(80 B * 2 сампъла) + 20 B за IP +12 B за UDP + 8 B за RTP = 200 байта за пакет
200 B за пакет * 50 пакета в секунда = 10000 * 8 бита / 1000 = 80 Kbps за обаждане

Таблица 5.6. Необходима честотна лента в зависимост сампъл честотата

Сампъл честота	Етернет - 14 байтов хедър	PPP - 6 байтов хедър	Frame Relay - 4 байтов хедър	ATM - 53 байтова клетка с 48 байта полезен товар
G.711 at 50.0 pps сампъл честотата 20 ms	85.6 Kbps	82.4 Kbps	81.6 Kbps	106 Kbps
G.711 at 33.3 pps сампъл честотата 30 ms	78.4 Kbps	76.3 Kbps	75.7 Kbps	84.8 Kbps
G.729a at 50.0 pps сампъл честотата 20 ms	29.6 Kbps	26.4 Kbps	25.6 Kbps	42.4 Kbps
G.729a at 33.3 pps сампъл честотата 30 ms	22.4 Kbps	20.3 Kbps	19.7 Kbps	28.3 Kbps

Проблемите, породени от по-големия брой сампли за пакет, са увеличаване на закъснението на пакетите поради нуждата от по-дълго изчакване при формиране на пакета, както и нарастване на закъснението при сериализиране на по-големи пакети. Поради това, преди прилагане на този метод за намаляване на честотната лента, необходима за едно обаждане, трябва да се направят изчисления за съответствие с изискването за максимално закъснение от 150 ms.

Всички VoIP пакети са изградени от две части – гласови сампли и IP/UDP/RTP хедъри с дължина съответно 8,12 и 20 байта. Размерът на гласовия сампъл зависи от използвания кодек, докато сборът от хедърите е винаги 40 байта. В зависимост от кодека този размер може да бъде два пъти по-голям от полезния товар на пакета. За да бъде избегнато излишното изразходване на честотната лента е възможно използването на вариант на транспортния протокол RTP – cRTP, компресиращ хедърите до 2 или 4 байта.

5.1.3. Закъснение

Закъснението е интервала от време, за което един пакет достига до своя получател. Стремежът е да се постигне минимално закъснение, въпреки че то не може да се избегне изцяло поради технологични причини. Голямото закъснение не винаги довежда до по-ниско качество на телефонната връзка, но може да причини липса на синхронизация на говорещите страни. За разговори на територията на една държава, за допустимо закъснение се приема времето от 150 ms, а при международни разговори 400 ms [15]. Времето, необходимо за получаване на един пакет, се изчислява като сбор от закъсненията, причинени от различните обработки и компоненти, през които той преминава.

- Една от причините за закъснение е времето, необходимо на крайните станции за създаване на пакети. То е равно на времето, за което станцията "пълни" един пакет. На практика, колкото по-голям е размерът на пакета, толкова е по-дълъг периодът за неговото запълване. Друг важен фактор, определящ закъснението при пакетиране, е кодекът, използван за преобразуване на аналоговия гласов сигнал в цифров. Размерът на пакета и кодекът влияят също и на времето, необходимо на получателя за обработване на пакета. Ако размерът на пакетите е малък, закъснението ще бъде по-малко, но зависещо от хардуерните и софтуерните компоненти на медийния шлюз. Независимо от избраната комбинация от размер на пакета, кодек и шлюз, закъснението при пакетиране не трябва да надвишава 30 ms.

- Сериализирането на данните е друг източник на закъснение. То е обратно пропорционално на скоростта на връзката, т.е. колкото е по-бърза една връзка, толкова по-малко е закъснението. Например времето, необходимо за предаване на един байт чрез 64 Kb връзка е 125 μs, докато при OC-3/STM-1 връзка то е 0.05 μs. Въпреки, че този тип закъснение е неизбежно, то може да бъде намалено чрез използването на високоскоростни интерфейси.
- Закъснението при разпространение е времето, необходимо на електрическия или светлинния сигнал за преминаване по дължината на дадена връзка. Скоростта на тези сигнали е винаги по-малка от скоростта на светлината. Този тип закъснение винаги съществува, но оказва влияние само когато пакетите преминават големи разстояния. Формулата за неговото пресмятане е следната:

  Закъснение при разпространение = Дължина на линията в км / (299.300 км * 0.6)

  Пример: Изчисляване на закъснението при разпространение за оптична линия с дължина 6000 км.

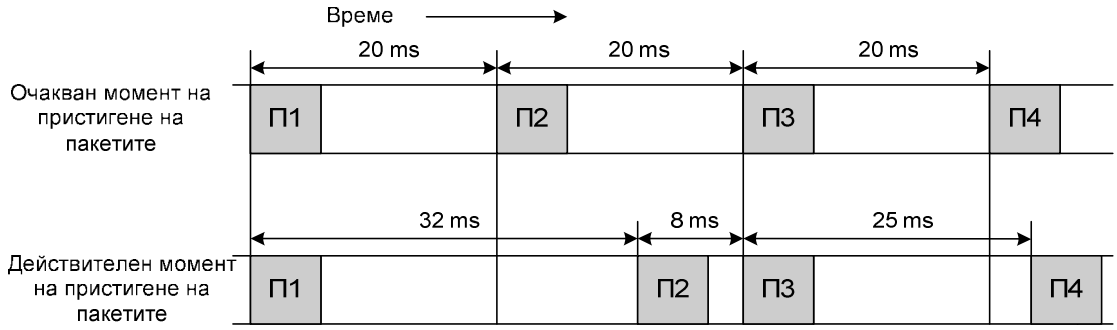
  0.0334 s = 6000 км / (299.300 км * 0.6)
- Причина за голяма част от закъснението е престоят на пакетите в буферите на мрежовите устройства, преди да бъдат изпратени. Времето, прекарано в буферите, зависи от натовареността на мрежата. Големината на буферите за интерфейсите на всяко устройство може да бъде конфигурирана, като колкото по-малки са, те, толкова по-малко е закъснението. За съжаление размерът на буфера основно зависи от количеството трафик, предавано от устройството през даден интерфейс. Така с увеличаване на трафика трябва да бъде увеличен и размерът на буфера, а от там и закъснението. Поради това, при предаване на гласови данни, трябва да се осигурят линии с необходимата скорост, предвид тяхната натовареност, за да се избегне нарастването на опашките в буферите.

- Последната причина за закъснение е продиктувана от времето, за което дадено мрежово устройство буферира пакетите при определяне на интерфейса, на който те трябва да бъдат препратени. Това закъснение обикновено е малко и зависи единствено от архитектурата на мрежовите устройства.

5.1.4. Джитер

Джитер е разликата между времето, за което се очаква даден пакет да бъде получен и времето, за което той бива получен [6]. Ако пакетите се изпращат през 20 ms, то се очаква, че интервалът на пристигането им ще е също точно 20 ms. Това не винаги е така. На фигура 5.2, илюстрираща джитер, пакети едно (П1) и три (П3) пристигат точно когато са очаквани, докато пакет две (П2) пристига със закъснение от 12 ms, а пакет четири (П4) с 5 ms по-късно.

Фигура 5.2. Джитер при предаване на пакети



Главната причина за джитера е промяната в големината на опашките в буферите на мрежовите устройства, породена от динамично изменящото се количество трафик, преминаващ през тях. Друга причина е възможността отделните пакети да преминават по различни пътища в мрежата, които въпреки еднаквото си тегло са с различна физическа дължина.

За да бъде избегнат негативния ефект на джитера, медийните шлюзове използват компенсиращи буфери, помагащи за реконструкцията на гласовите

данни. В тях пакети пристигнали по-рано изчакват определен интервал от време пристигането на изпратените преди тях пакети. Ако това стане в оказаният интервал, гласовия сигнал бива възстановен без загуба на фрагменти. Тези буфери могат да елиминират ефекта от джитера, но не и при големи отклонения от очакваното време за пристигане на пакетите. В тези случаи медийният шлюз може да отхвърли пакети, пристигащи в грешна последователност, което да доведе до прекъсвания в гласовия сигнал.

5.1.5. Загуба на пакети

Съществуват много причини за загубата на пакети и тя не винаги може да бъде избегната. Много често количеството трафик, минаващо през мрежата, бива подценявано. По време на мрежови задръствания е възможно препълване на буферите на мрежовите устройства, което довежда до отхвърляне на новополучени пакети. Загубата на пакети на приложения, неработещи в реално време, е нежелателна, но не и критична. Тези приложения обикновено използват TCP за транспортен протокол и толерират известно количество загубени пакети, поради възможността за повторното им предаване. От друга страна, приложенията работещи в реално време, използват UDP за транспорт и са значително по-чувствителни към загуба на пакети. UDP няма механизми за повторно предаване на загубена информация, но дори и при наличие на такива, ограниченията, налагани с цел качество на услугите, не биха позволили тяхното използване. Времето за установяване липсата на пакет, повторното му предаване и получаването му значително надхвърлят ограниченията от 150 ms за преминаване на пакет през мрежата.

Допустимият процент загубени пакети зависи от използвания кодек. При използване на G.711, загуби под 5% не биха причинили спад в качеството, под това на класическите телефони. Този процент е чувствително по-нисък при високо компресиращите кодеци, като G.723.1 и G.729A, където допустимите стойности са съответно 1% и 2%. С цел влизане в тези граници се използват множество различни методи за Клас на Услугите (CoS), даващи приоритет при предаването на VoIP

трафика. Като цяло се приема правилото, че въпреки негативния ефект от загубата на пакети, тя е за предпочитане пред изчакването им чрез увеличаване размера на буферите, тъй като това води до закъснение на всички пакети.

5.1.6. Сигурност и решения свързани с нея

Бързото разпространение на VoIP дава предпоставки за повишаване на риска от заплахи за сигурността и налага спешното разработване на средства за защита. Само до преди няколко години сигурността не е била считана за съществен проблем, тъй като VoIP технологията се е прилагала предимно в малки по размери и затворени към външния свят корпоративни мрежи. Използването днес на VoIP за комуникации извън пределите на локалната мрежа, излага потребителите им на същите многобройни рискове, като тези, застрашаващи мрежите за пренос на данни. Най-общо заплахите за сигурността могат да бъдат разделени на два основни класа – заплахи, свързани с отказ на услуги и заплахи от компрометиране на лични ресурси [11]. Първият тип заплахи прави системните ресурси неизползваеми, докато при втория ресурсите и данните стават достояние или биват използвани от атакуващите системата.

5.1.6.1. Заплахи за сигурността

Една от най-често срещаните атаки е “отказ на услуга” (DoS). Тя причинява загуба на услуга или невъзможност мрежата да функционира и може да е с продължителност от няколко минути до няколко дни. Атаката се осъществява чрез изчерпване на ресурсите на система или чрез консумиране на цялата честотна лента. Изчерпването на ресурси е насочено към определени компютърни системи, предоставящи услуги. Целта е да бъдат използвани до край ресурси като памет, дисково пространство или капацитет на процесора, като по този начин се нарушава или преустановява нормалното изпълнение на услуги. Консумирането на честотната лента е атака срещу мрежовите ресурси. “Отказ на услуга” се получава, когато целият капацитет на мрежовата връзка е зает и предаването на данни стане

невъзможно или прекалено бавно. Осъществяването на нови връзки за телефонни разговори, файлови услуги, Web сървъри, Mail сървъри и всякакви други услуги, изискващи мрежова комуникация става невъзможно. Вече създадените връзки стават бавни, блокират се или се прекъсват. Макар и атаките "отказ на услуга" да не нанасят поражения на базите данни или друг тип информация, те могат да доведат до прекъсване на работния процес. Компаниите разчитат на надеждността на телефонната им система. Тя осигурява както връзка с клиентите им, така и връзка между техните служители. Имайки предвид необходимостта от предаване на гласовите данни в реално време, както и чувствителността им към закъснение, атаките "отказ на услуга" могат да причинят сериозна загуба на приходи.

Друга заплаха е подслушването на разговори. Това може да стане чрез неправомерно прихващане на пакетите на Real-time Transport Protocol (RTP), пренасящи гласовите данни. Статистически проучвания показват, че опасността от подслушване вътре в корпоративната мрежа е особено голяма [12]. Причината е неефективността на защитните стени и шлюзовете при атаки, инициирани от вътрешността на мрежата. Подслушването може да бъде извършено с помощта на софтуер, следящ мрежовия трафик и прихващащ всички или конкретен тип пакети. Друг начин е придобиването на контрол върху сървъра, обслужващ повикванията. При нормални условия RTP пакетите не преминават през сървъра, обслужващ повикванията. Но ако бъде компрометиран, той може да „заблуди" IP телефоните в двата края, че всеки от тях ползва кодек, който другият не поддържа. Така сървърът поема ролята на преобразуващ двата кодека и през него започват да преминават всички пакети от дадения разговор.

Подобно на подслушването на разговор е възможно да бъде прихванат и служебния трафик, подготвящ обажданията. Чрез модифициране на отделни полета в пакетите му може да бъде осъществявано неоторизирано обаждане дори без наличие на IP телефон, а също така и фалшифициране на самоличността на обаждащия се. По този начин атакуващите извършват скъпи обаждания, заблуждавайки сървъра, обслужващ повикванията, че това е станало от телефоните на неподозиращи потребители на IP телефонната мрежа.

Друг възможен риск е неоторизираното пренасочване на входящите обаждания. По този начин лицата, извършващи обаждане към даден потребител и нямащи представа за извършеното пренасочване, биха предоставили лична или поверителна информация, предназначена за потребителя на атакувания телефон, директно на атакуващите системата.

Не на последно по важност място е проблемът със спама, разпространяван по IP телефоните. Макар и смятан по-скоро за неудобство, отколкото за заплаха за сигурността, по-голямо количество нежелан трафик може да навреди на нормалното функциониране на бизнеса по начин, подобен на атаките от типа "отказ на услуга". Пример е всекидневното отделяне на време от страна на потребителите на VoIP телефони за прослушване на гласовата си поща и изтриване на преобладаващите и нежелани рекламни съобщения.

Въпреки че, както и мрежите за данни, VoIP технологията също използва IP пакети, стандартните мерки за сигурност, предпазващи мрежите за данни, не винаги са приложими. Причина за това са времевите ограничения при предаване на глас в реално време. Международните стандарти задават горна граница от 150 ms закъснение при предаване на VoIP пакетите. Това ограничение налага сериозни изисквания към пропускателната способност на защитните устройства и техния софтуер, далеч надвишаващи тези при пренос на данни. За намаляване на риска от изброените по-горе заплахи за сигурността, помага придържането към описаните по-долу практики при проектирането и изграждането на VoIP мрежи.

5.1.6.2. Виртуални LAN мрежи

Използването на виртуални LAN мрежи (Virtual Local Area Network-VLAN) за разделяне на гласовите от останалите типове данни помага за повишаване не само на производителността на мрежата, но и на сигурността. Виртуалната LAN мрежа, използвана за гласови данни, трябва да бъде отделена от останалите чрез механизми за филтриране на пакети и/или чрез защитна стена. Препоръчително е да се използват различни подмрежи с отделни адресни пространства за глас и данни, както и отделни DHCP сървъри за всяка.

5.1.6.3. Криптиране

Винаги когато е възможно и обосновано, трафикът, пренасящ гласови данни, трябва да бъде криптиран [11]. Възможно, защото не всички крайни устройства имат необходимите ресурси за криптиране на данните. При ефективно работещи VoIP мрежи негативният ефект от криптирането на трафика е пренебрежимо малък, но при мрежи, разполагащи с ограничени ресурси, то би довело до забавяне на пакетите, което е недопустимо при работа в реално време. Причини за това са необходимото процесорно време и увеличаването на размера на пакетите. Този ефект се засилва при няколкократно криптиране на един и същи трафик. Поради това се препоръчва криптирането да се извършва от маршрутизатор или граничен шлюз, а не от всяко крайно потребителско устройство Криптирането също така трябва да бъде и обосновано. Проучване, направено сред доставчици на традиционна телефония показва, че въпреки предлагането на услугата криптиране, потребителите рядко се интересуват от нея, а още по-рядко прибягват до използването й. Противно на това съществува схващане, че успешното реализиране на VoIP мрежа включва пълно криптиране на трафика. Една от причините за това е голямото разнообразие и лесното имплементиране на софтуерни продукти, много от които безплатни. Тези продукти използват техники като VPN, IPSec и SSL и по подразбиране криптират всички линии в IP телефонните мрежи. Въпреки лесното му прилагане, криптирането на целия трафик рядко е необходимо. В повечето корпорации, необходимото ниво на сигурност се постига при криптиране на телефонните линии единствено на изпълнителните директори и на лицата, боравещи с класифицирана информация. В допълнение може да бъдат използвани VPN тунели между ключови отдели, като човешки ресурси и финанси.

5.1.6.4. Защитни стени

Защитните стени се използват за създаване на бариера между локалната вътрешна мрежа и връзката й към външния свят. При правилно проектиране, целия

трафик за и от локалната мрежа минава през защитната стена и бива допуснат или отхвърлен на базата на зададена политика за сигурност. При имплементиране на VoIP, към задачите на защитните стени се добавя и филтрирането на трафика между сегментите за глас и данни. Това не е тривиална задача, особено когато в мрежата се използват компютърно базирани IP телефони. От една страна, тъй като са компютърно базирани, те се намират на сегмента за данни, от друга, като телефонни приложения те работят с гласови данни. При липса на защитна стена, целия гласов трафик от или към тези устройства трябва да бъде изрично разрешен, тъй като RTP използва динамични UDP портове. Оставянето на тези UDP портове отворени, е голяма заплаха за сигурността. Поради това всички компютърно базирани IP телефони трябва да бъдат отделени със statefull защитна стена, която да проверява VoIP трафика. В противен случай е възможно осъществяване на атаки "отказ на услуга", използващи наличието на отворени UDP портове. Други сценарии, при които е необходимо преминаването на трафик от сегмента за данни в този за гласови данни или обратно и съответно използването на защитна стена за контролирането на този трафик са:

- IP телефон или CallManager сървър (гласови данни) извършващи достъп до гласова поща (данни)
- Потребител (данни), извършващ достъп до прокси сървър (гласови данни)
- Прокси сървър (гласови данни), извършващ достъп до мрежови ресурси (данни)
- Трафика между IP телефон (гласови данни) и сървъра обслужващ повикванията (гласови данни) или прокси сървъра (гласови данни) трябва да премине през защитната стена, защото при тази връзка се използва посредничеството на сегмента за данни

В случаите на използване на защитна стена, тя трябва да бъде подбрана с директна поддръжка на SIP и/или H.232. В противен случай е необходимо отварянето на портове за преминаването на тези протоколи, което влияе негативно на сигурността и означава, че защитната стена не поддържа адекватно VoIP.

Добра практика при изграждането, както на VoIP мрежи, така и на мрежи за данни, е използването на Етернет комутатори. Свързването на VoIP устройствата посредством комутатори вместо хъбове намалява риска от прихващане на пакети. Докато един хъб изпраща пакетите до всички свои портове, комутаторът е способен да определи към кой порт е свързан получателя на пакета и да го изпрати само на него. С цел повишаване на сигурността е възможно „заключването" на физически порт на комутатора към конкретен MAC адрес. Това прави невъзможно свързването на неоторизирани устройства към този порт на VoIP мрежата.

5.1.6.5. Ограничаване на трафика

С цел избягване на атаки "отказ на услуга", критичните мрежови елементи, като маршрутизатори и комутатори, трябва да бъдат конфигурирани по начин, забраняващ един вид трафик да изчерпи до край ресурси, като честотна лента, памет или процесорно време.

5.2. Методи за осигуряване качество на услугите

Възможността различните видове трафик да получават различен приоритет при преминаване през мрежата се дефинира като качество на услугите. Във VoIP среда това позволява да се даде предимство на гласовия трафик или да се моделира трафика на данни така, че да не се допуска спиране или продължително прекъсване на гласовия поток. Въпреки че методите, осигуряващи качество на услугите дават приоритет на определени видове трафик по време на мрежови задръствания, в случаите на хронични задръствания този подход е неефективен. В тези случаи единственото решение на проблема е разширяване на честотната лента.

Осигуряването на качество на услугите във VoIP мрежите е задължително. В противен случай липсата на контрол върху проблеми, като джитер, закъснение и загуба на пакети може да причини насичане на разговора, прекъсвания или дори разпадане на връзката.

При конфигуриране на механизми за качество на услугите, гласовия трафик получава най-висок приоритет, следван от видео приложенията и на последно място приложенията, работещи с данни. Възможно е те от своя страна да бъдат разделени в няколко класа, за да се осигури предимство на някой приложения пред други.

Съществуват множество различни методи за конфигуриране на качество на услугите, като конкретният им избор зависи от индивидуалните характеристики на всяка мрежа. Определящи фактори са типът на мрежата, наличната честотна лента, броя на потребителите и изискванията им към качеството. Важно е също така да бъдат анализирани основните мрежови приложения, споделящи една и съща честотна лента с гласовия трафик, за да не се допусне влошаване на тяхното качество в следствие приоритета, даден на VoIP пакетите. Таблица 5.7 отразява изискванията към честотната лента на някой мрежови приложения и тяхната чувствителност към закъснение, джитер и загуба на пакети.

Таблица 5.7. Изисквания към честотна лента на мрежовите приложения

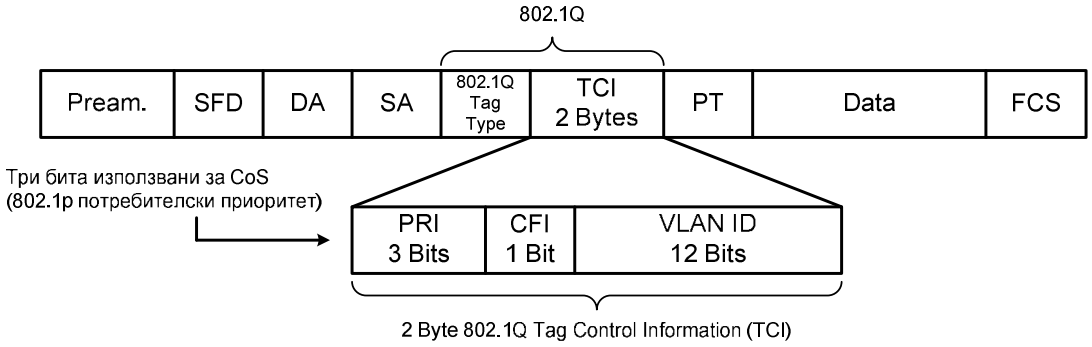
Приложение	Необходимост от честотна лента	Чувствителност към		
		Закъснение	Джитер	Загуба на пакети
IP телефония	Ниска	Висока	Висока	Средна
Видео конференции	Висока	Висока	Висока	Средна
Поточно видео	Висока	Средна	Средна	Средна
Поточно аудио	Ниска	Средна	Средна	Средна
Интернет сърфиране	Средна	Средна	Ниска	Висока
Електронна поща	Ниска	Ниска	Ниска	Висока
Файлов трансфер	Средна	Ниска	Ниска	Висока

Най-често използваните методи за осигуряване качество на услугите са 802.1p/Q, Differentiated Services (DiffServ), Call Admission Control (CAC) и приоритизиране по IP адрес [9].

5.2.1. Качество на услугите чрез 802.1p/Q

Стандартът IEEE 802.1Q осигурява качество на услугите, като добавя четири допълнителни байта към стандартния 802.3 Етернет фрейм, включващи три битово 802.1p поле и поле, служещо за идентификатор на виртуална локална, мрежа - VLAN ID. Този стандарт се поддържа от повечето Етернет комутатори. Полето за потребителски приоритети 802.1p позволява създаването на осем класа, категоризиращи мрежовия трафик [1]. За гласови данни и протоколи за сигнализация се използва стойност 110, даваща най-висок приоритет. Възможно е също използването на полето VLAN ID за определяне на предимство при предаване на трафика на отделените виртуални мрежи, но този метод не се препоръчва, тъй като не позволява диференциране на отделни протоколи. Използването единствено на 802.1p/Q не гарантира качество на услугите от край до край в VoIP мрежата, тъй като неговите механизми работят на каналното ниво в OSI модела и са валидни само в отделния сегмент. Старшите трите бита на полето TCI (Фиг. 5.3), наричани и определящи Клас на Услуга (CoS), могат да бъдат дублирани на мрежовото ниво от старшите три бита на полето Тип на Услуга (ToS) в хедъра на IP пакетите. Тези три бита се наричат IP Precedence и служат за задаване приоритет при IP трафика

Фигура 5.3. Етернет фрейм

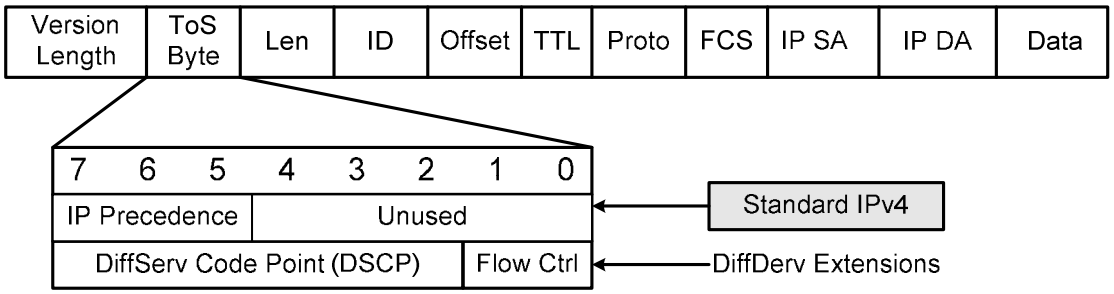


.По този начин устройствата работещи, както на слой 2, така и на слой 3, получават информация за неговия приоритет. Паралелното използването на двете технологии осигурява качество на услугите в цялата мрежа – както в локалните сегменти, така и при рутирането на между тях.

5.2.2. Качество на услугите чрез диференцирани услуги DiffServ

DiffServ е стандарт на IETF, описан в RFC 2474 и 2475. Това е сравнително по-нов модел, при който мрежовите устройства третират трафика на базата на относителен приоритет, зададен в полето за Тип на Услугата (ToS). За разлика от по-старите модели, кодирането на приоритета се извършва с помощта на шест, а не на три бита (Фиг. 5.4). Използват се шестте най-старши бита от еднобайтовото ToS поле, наречени DSCP и тяхната стойност служи за определяне на поведението при предаването към следващото устройство (PHB).

Фигура 5.4. IPv4 пакет



Възможни са три категории услуги: EF (Expedited Forwarding) за приложения в реално време, чувствителни към закъснение и загуба на пакети, AF (Assured Forwarding) за останалите приоритетни потоци (възможни са 4 класа услуги) и DE (Default forwarding). DE е предназначен за потоците без приоритет, предавани според наличните в момента ресурси, които представляват 80% от общият трафик (Таб. 5.7). Класа EF гарантира предаване на данните с най-малко закъснение и загуби. Неговото двоично представяне в хедъра на пакетите е числото 101110. Тъй като описаното от този клас поведение отговаря на изискванията на VoIP трафика, то това е препоръчителната стойност, поставяна в пакетите пренасящи гласови данни. Препоръчителните стойности за останалите типове трафик са:

Таблица 5.7. Стойности за задаване приоритета на различните видове трафик

Слой 2	Слой 3			Приложения
CoS	IP Precedence	PHB	DSCP	
7	7	-	56-63	Резервирано
6	6	-	48-55	Резервирано
5	5	EF	46	Гласови данни
4	4	AF41	34	Видео конференции
3	3	AF31	25	Сигнализация
2	2	AF2y	18,20,22	Високо приоритетни данни
1	1	AF1y	10,14,16	Средно приоритетни данни
0	0	DE	0	Данни без приоритет

5.2.3. Управление на разрешението за връзка (CAC)

CAC е общ термин, описващ метод, чрез който дадено устройство може да предотврати надхвърляне на определен лимит при използване на мрежови ресурс, като по този начин се запазва качеството на съществуващите връзки. Употребата на CAC във VoIP мрежи е свързана с отказа за иницииране на нови обаждания, ако свободната честотна лента е по-малка от необходимата за желаната връзка при използвания кодек. Пример за това е интерфейс с конфигурирана честотна лента от 128 Kbps, през който преминават пет VoIP обаждания, за всяко от които са необходими 24 Kbps. Опит за осъществяване на шесто обаждане ще бъде отхвърлен от CAC механизмите, въпреки наличието на неизползвана честотна лента. В противен случай честотната лента на интерфейса ще бъде разпределена между шестте връзки предоставяйки 21.33 Kbps на всяка от тях, вместо необходимите им 24 Kbps, което би се отразило негативно на качеството на всички връзки. Когато връзката бъде отказана, в зависимост от конфигурацията си, иницииращото устройство или ще потърси алтернативен маршрут за осъществяване на обаждането или ще сигнализира за отказа чрез сигнал за заета линия. Съществуват различни методи за имплементиране на CAC, като за целите на VoIP най-често използвани са RSVP (Resource Reservation Protocol) и H.323 гейткипъри. RSVP е протокол, служещ за резервиране на необходимата честотна лента по продължение на цялата връзка от край до край в IP мрежата.

Резервирането се извършва в посока от приемащото устройство към предаващото, като типът на връзката е симплекс (еднопосочна). Дуплексните връзки изискват две индивидуални RSVP сесии. H.323 гейткипърите взимат решения за допускане или отхвърляне на нови връзки на базата на конфигурираната честотна лента на интерфейсите и тяхната моментна заетост. Сборът от честотната лента, използвана от текущите връзки и необходимата за ново обаждане се изваждат от честотната лента на интерфейса и при разликата по-малка от нула, обаждането бива отхвърлено.

5.2.4. Приоритет на IP адреси

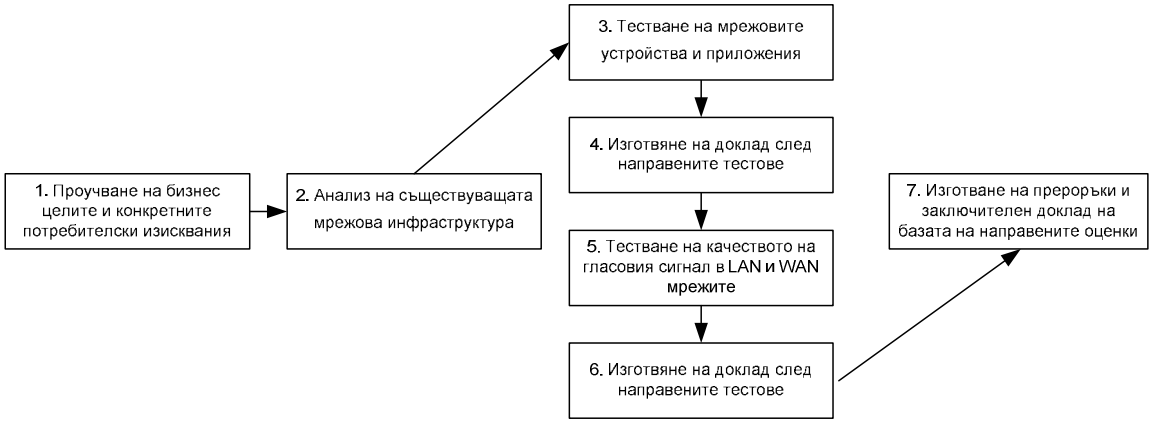
Приоритетът на VoIP трафика може да бъде задаван и на базата на IP адреси. Методът е особено подходящ за устройства със статично зададени IP адреси, които много рядко се променят. Такива са VoIP шлюзовете, комуникационните и CallManger сървъри. Качество на услугите се осигурява, като маршрутизаторите и комутаторите в мрежата биват конфигурирани да дават приоритет при предаването на пакетите, изпращани от горните устройства.

6. Имплементиране на VoIP решение

6.1. Оценка на съществуваща IP мрежа за данни

Необходимо условие за успешно имплементиране на IPT е наличието на надеждна мрежа за данни, служеща за основа на обединените комуникации. Макар и в повечето компютърни мрежи да съществува неизползвана честотна лента, и въпреки че те изпълняват безпроблемно своите функциите по пренос на данни, в много малко случаи добавянето на VoIP без извършване на промени е успешно начинание. За да се осигури плавен преход към единна мрежа за глас и данни е необходимо преди имплементирането на новата система да бъде извършен цялостен анализ и оценка на съществуващата мрежова инфраструктура (Фиг.6.1). Целта на този анализ е да се установи дали мрежата за данни има възможност за пренасяне и на гласовия трафик и какви са промените, необходими за това. Той включва оценка на капацитета на мрежата, на съществуващия трафик, на използваните WAN/LAN технологии и хардуерни устройства, окабеляването на помещенията, възможностите за захранване на IP телефоните, достъпа до безжичната мрежа и други. Необходимо е да бъдат локализирани всички съществуващи пропуски и да бъдат определени начините за тяхното отстраняване, преди да се премине към внедряването на IP телефония.

Фигура 6.1 Анализ на съществуващата мрежова инфраструктура



6.1.1. Оценка на капацитета на мрежата

Когато става въпрос за мрежи, пренасящи данни, понятието капацитет се определя като количеството трафик, което мрежата е проектирана да пренася. Но когато се говори за капацитет на VoIP мрежа, той се тълкува по-скоро като брой едновременни разговори, които мрежата може да предава. Понятието максимално натоварване е основен елемент при оценяване на съществуващи мрежи преди имплементиране на VoIP. За неговото определяне е необходимо да бъдат разгледани съществуващите локални и WAN сегменти, съществуващият трафик на данни, както и наличният хардуер.

Анализът на съществуващата мрежова инфраструктура трябва да започне с идентифициране на всички мрежови връзки, които в бъдеще ще пренасят гласов трафик и документиране на тяхната честотна лента. Това ще помогне за ранното откриването на местата, които биха могли да причинят задръствания. Възможно е тези места да остават незабелязани при преноса на данни, но при добавяне на глас, чувствителен към закъснение и загуба на пакети, предварителното им отстраняването ще предотврати проблеми, като лошо качество и разпадане на връзки, след обединяването на мрежите за глас и данни.

Сам по себе си капацитетът на една връзка не е достатъчен, за да се направи заключение относно способността й да поеме допълнителното натоварване от гласовия трафик. За да се направи това е необходимо анализиране на текущата натовареност на линиите с данни, преди въвеждането на глас. Възможно е физическият капацитет на дадена линия да позволява желания брой обаждания, но когато се отчете и трафика, генериран от мрежовите приложения, да се достигне до извод, че е необходимо разширяване на честотната й лента. Ако тези сметки не бъдат направени предварително, е възможно забавяне на преноса на данни поради механизмите за качество на услугите, осигуряващи предимство на гласовите данни. Така например, времето за осъществяване на файлов обмен може да бъде няколкократно увеличено в моментите на интензивно използване на гласовата мрежа. Въпреки че оценката на капацитета трябва да се направи за всички мрежови линии, вероятността тя да разкрие потенциални проблемни области във

високоскоростните локални мрежи е малка. За сметка на това особено внимание трябва да бъде отделено на WAN връзките, разполагащи със значително по-малка честотна лента.

За да се определи броят на едновременните обаждания, които дадена линия трябва да може да поддържа, се използва статистиката за нейното максимално натоварване преди въвеждането на VoIP. Необходимата информация може да бъде получена от локалната телефона компания или да се извади от статистиката на УТЦ. Тази статистика също показва процента на разговори вътре в компанията, които ще бъдат поети от VoIP системата, и тези извън нея, минаващи през традиционните телефонни компании. Това определя и броят на наетите телефонните линии, които трябва да останат след имплементирането на VoIP.

След установяване на очакваното максимално натоварване на мрежовите връзки е необходимо да се извърши тестване, проверяващо неговото въздействие върху съществуващата мрежа. Стандартните средства за наблюдение на мрежата и мрежовите анализатори могат да предоставят основна информация за използваната честотна лента и местата, на които е възможна появата на проблеми. За по-задълбочено анализиране, се използват специфични за VoIP приложения, които генерират очаквания обем гласови данни и следят за възникващи грешки и проблеми. Това позволява проверка в реални условия на джитера, закъснението и загубата на VoIP пакети. Възможно е да се симулира различна натовареност на мрежата и използването на различни кодеци. Също така е възможно да се тества как компресирането на данни се отразява върху натовареността на мрежовото оборудване и съответно на кои връзки може да бъде приложено.

По време на оценяването на капацитета на съществуващата мрежа трябва да бъдат взети решения, дали отдалечените офиси ще продължат да имат връзки към традиционните телефонни оператори или всички разговори извън корпоративната мрежа ще минават през шлюза, разположен в централния офис. Във вторият случай, всички разговори с дестинация извън компанията ще бъдат транспортирани през WAN връзките до централния офис, от където ще бъдат пренасочвани към подходящ шлюз, служещ за връзка с публичните телефонни мрежи. Това улеснява администрирането на мрежата, намалява разходите за хардуер и повишава

надеждността, но също така увеличава изискванията към капацитета на мрежата. Кой от двата начина ще бъде избран зависи от размера на отдалечените офиси и най-вече от изискванията им за честотна лента, необходима за провеждане на разговори извън границите на корпоративната мрежа. Тази информация може да бъде получена от статистиката, изготвяна от УТЦ или телефонните компании.

6.1.2. Оценка на съществуващият хардуер

Хардуерът в съществуващата мрежа директно влияе върху капацитета й и успешното имплементиране на VoIP. По време на анализа на мрежовата инфраструктура, параметрите на всеки хардуерен елемент трябва да бъдат оценявани за съответствие с бъдещите изисквания. Добавянето на гласови данни може да удвои мрежовия трафик, което налага проверка, дали всички устройства могат да поддържат този обем. Необходимо е да се осигури 100 Mbps, пълен дуплекс, до всеки IP телефон и поддържането на VLAN мрежи, което е във възможностите на повечето съвременни комутатори за достъп. Ако съществуващият хардуер позволява добавянето на нови модули и може да бъде увеличен броят на портовете, то е възможно запазването на текущото оборудване. Допълнителни портове няма да са необходими, ако IP телефоните са с вграден комутатор. Освен комуникациите на слоя за достъп, трябва да бъде проверено и дали връзките към разпределителния и опорния слой са способни да поемат новите натоварвания. Друго важно съображение при оценката на хардуера е възможността му да осигурява необходимите за VoIP механизми за качество на услугите, даващи приоритет на гласовите данни.

6.1.3. Оценка на безжичната инфраструктура

Когато планираната VoIP система включва поддръжката на безжично предаване на гласови данни, наличната безжична инфраструктура трябва да бъде внимателно оценена, поради някой особености при добавянето на глас към предаваните от нея данни. Изхождайки от ограниченото количество обаждания,

които се поддържат от точките за достъп, трябва точно да бъдат предвидени местата, на които има вероятност от изчерпване на наличните ресурси и да се добавят необходимият брой устройства. Важно е да се осигури цялостно покритие в сградите, тъй като достъпът до мрежата за данни по-рядко бива използван от хора в движение, което за сметка на това е основно предимство при използването на безжичен телефон. Трябва да се вземе предвид, че добавянето на точки за достъп изисква свободни портове в комутаторите за достъп, както и съответното окабеляване.

6.1.4. Оценка на възможностите за захранване на IP телефоните

Решението дали IP телефоните да бъдат захранвани през Етернет мрежата или не трябва да бъде взето след оценка на възможностите на съществуващите комутатори за достъп. При наличие на комутатори, поддържащи PoE или позволяващи подмяна или добавяне на PoE модули, те могат да бъдат използвани за захранване на IP телефоните. В противен случай комутаторите трябва да бъдат подменени или IP телефоните трябва да бъдат захранвани локално с мрежови адаптери.

6.2. Стратегии при имплементирането

Съществуват редица фактори, влияещи върху процеса на миграция към единна мрежа за глас и данни. Сред тях са сложността на имплементирането, бизнес нуждите и размера на всяка отделна компания или офис. Едно от основните предимства на IPT технологията е това, че тя позволява да бъде имплементирана на части. По този начин могат да бъдат запазени инвестициите, направени в отделни УТЦ, като те продължат да работят успоредно с IPT системата до изтичане на техните договори за поддръжка или докато преходът бъде завършен напълно.

Преди обединяването на двете мрежи е необходимо да бъде създаден подробен план, описващ както конфигурациите на IP телефоните, така и методи и схеми за тестване на бъдещата система, като за целта се взимат предвид и

изискванията на потребителите. Процесът на миграция може да протече по две различни схеми. При първата се извършва цялостна подмяна на телефонните системи в рамките на една нощ или почивен ден. По този начин се избягва нуждата от осигуряване на взаимодействие между традиционната телефонна мрежа и VoIP. Общоприето правило е, че миграция на мрежи с по-малко от 1000 потребители може да бъде извършена по този начин, докато при по-голям брой потребители имплементирането на VoIP се извършва на отделни етапи [7]. Процесът на постепенна миграция налага изграждането на връзка, най-често една или няколко T1/ E1 линии, между съществуващата УТЦ и IPT системата. Чрез нея се осигурява комуникация между потребителите на двете системи по време на прехода. Числото 1000 не е твърдо фиксирано като определящ фактор при избор на стратегия. Възможно е и по-голям брой потребители да бъдат едновременно прехвърлени към IPT, както е възможно и броят да бъде значително по-малък от 1000 при отежняващи обстоятелства - например при миграция на център за обслужване на повикванията. При възможност е препоръчително миграцията да не се извършва поетапно, за да се избегнат проблемите при осигуряването на взаимодействие между двете системи. Друга причина за това може да бъде необходимостта от добавяне на допълнителни T1/E1 PRI модули към съществуващите УТЦ, които няма да бъдат използвани след приключване на миграцията.

При организации с множество офиси трябва да бъде обмислена последователността на миграционния процес. Типична стратегия е изграждането на централизирана VoIP архитектура за обслужване на обаждания, имплементиране на VoIP в отделните офиси и като последна стъпка мигриране на централния офис. Началният етап се състои в изграждането на ядрото на телефонната система. Част от него са група от сървъри за обслужване на обажданията, намиращи се обикновено в главния офис, където е разположена и информационната система, осигуряваща бизнеса на компанията. Тези сървъри управляват създаването и прекратяването на връзките както за централния, така и за всички отдалечени офиси. След като основата на VoIP архитектурата бъде изградена е възможно лесно добавяне на допълнителни сегменти, обслужващи отделните офиси, след извършване на нужното конфигуриране на тяхната IP мрежата. Създаването на

ядрото на VoIP системата включва и инсталиране, конфигуриране и тестване на шлюз, осигуряващ връзката със съществуващата УТЦ. Важно е да се отбележи, че на този етап не е необходимо и не се извършва миграция на централния офис, въпреки разполагането в него на основите й. Началната цел е единствено изграждането на гъвкава система, позволяваща лесна интеграция на нови сегменти. В зависимост от избора на производител и предлаганите от него решения е възможно разпределянето и резервирането на ядрото на VoIP архитектурата в два или повече отделни географски района. По този начин се осигурява по-голяма устойчивост на системата в случай на аварии и природни бедствия.

6.2.1. Миграция на отдалечен офис

Използването на различни телефонни платформи в отделните офиси на една компания възпрепятства централизираното им управление, както и възможността за използване на пълния набор функции на УТЦ при междуофисна комуникация. С преминаването към единна мрежа, първо в отдалечените офиси се преминава и към единна телефонна платформа, като по този начин се улесняват връзките между потребителите и се допринася за по-голямата им ефективност.

Факторите, определящи реда на миграция на отделните офиси са често същите, влияещи върху решението дали и кога е най-подходящо да се премине към IP телефония въобще. Добро планиране на тази последователност може значително да намали евентуалното неудобство и проблеми при имплементацията, както и да ускори възвращаемостта на инвестициите (ROI). Освен в случаите когато има специфични изисквания от страна на компанията, въвеждаща VoIP, първи в схемата на миграция биват избирани офисите, отговарящи на някой от следните условия:

- Текущо се използват IP Centrex линии, позволяващи преноса на данни и глас върху една и съща мрежа. Поради високата цена за поддръжка на такива линии, въвеждането на VoIP би довело до значително намаляване на разходите.

- Преместването в нова сграда е момент, особено подходящ за взимане на решение за преминаване към единна мрежа за глас и данни. В този случай при изготвяне на планове за окабеляването на сградата може да бъде избегнато прокарването на две паралелни мрежи, както и закупуването на аналогово телефонно оборудване.
- Изтичането или наближаването на края на договора за поддръжка на УТЦ, или необходимост от нейната смяна поради повреда или морално остаряване са също моменти, много подходящи за преминаване към VoIP комуникации.
- Не на последно място имплементирането на VoIP е удачно при офиси, намиращи си в географски отдалечени райони, както и при наличието на много извънградски разговори, провеждани от дадения офис. В тези случаи изграждането на VoIP мрежа би намалило или напълно елиминирало разходите за тези обаждания.

6.2.2. Миграция на централен офис

В зависимост от броя на потребителите и сложността на имплементацията е възможно миграцията на централния офис да бъде извършена на отделни етапи. При този сценарий се препоръчва разделянето на служителите да стане на базата на съществуващите работни отдели или друга логическа схема. Това е така, тъй като независимо от доброто планиране, винаги се наблюдава известно нарушение в работата на потребителите при смяна на телефонната система. Основен проблем е запазването на пълната функционалност при комуникациите между служители, използващи старата и новата телефонна система. Мигрирането наведнъж на цели отдели води до минимизиране на нежеланите ефекти.

Размерът на отделните групи потребители може да варира между 50 и 500 в зависимост от индивидуалните изисквания. Най-често потребителите биват разделяни на административни служители и служители, работещи в центровете за обслужване на повикванията. Причина за това е невъзможността за разделяне на един работещ център за обслужване на повикванията на две, технологично напълно различни платформи и същевременно запазване на неговата функционалност. От

техническа, а и от бизнес гледна точка, мигрирането на такъв център е желателно да бъде извършено или в началото или в края на цялостния процес.

Най-общо препоръките при планиране на миграция към единна комуникационна среда се свеждат до следното:

- Не е необходимо увеличаване капацитетът на цялата мрежа за данни в един и същ момент. Това е необходимо само за отделните й части, преминаващи към IPT.
- Съществуващият хардуер, отговарящ на новите изисквания, може и трябва да бъде използван.
- Всички мрежови инвестиции трябва да се правят с оглед на бъдещо интегриране на гласовите комуникации, дори и ако то е отложено във времето.

6.3. Избор на хардуерна платформа

Едно от най-важните решения, което трябва да се направи преди сливането на мрежите за глас и данни, е изборът на фирмата-производител на мрежовото оборудване, служещо за платформа на новата VoIP система. От производителя се очаква да предлага решения, които да осигуряват максимална гъвкавост и възможност за лесно разширяване. Друго очакване е възможността за продължителна употреба на избраните компоненти, без да се налага тяхната цялостна смяна при навлизането на новости в областта. Съществуват няколко фактора, които трябва да бъдат взети предвид при правенето на този избор [14]. Влиянието, което оказва всеки от тях е различно за отделните компании. Затова е възможно правилният избор на производител за две компании, работещи в една и съща сфера, да не е еднакъв, поради разлики в техните индивидуални изисквания.

6.3.1. Финансова мощ

Един от основните фактори е финансовата мощ на производителя. Тя е важна по няколко причини. По-очевидната е очакването фирмата-производител да бъде на пазара през следващите пет, десет и дори двадесет години, осигурявайки поддръжка и резервни части за произведените устройства. Друга причина е очакването производителят да има финансовата възможност за провеждане на нови проучвания и разработки, както и за поддръжка на съществуващата гама продукти. Изискването за финансова мощ не се отнася единствено до общия капитал на дружеството, а до финансовите аспекти, имащи отношение към разглежданата VoIP система. Някой от въпросите, които трябва да бъдат зададени на проучваните производители на мрежово оборудване са:

- Печеливша ли е компанията? Била ли е някога печеливша? Ако не, кога се очаква да бъде?
- Какъв е техният финансов баланс?
- Каква част от годишния бюджет бива отделяна за проучване и разработки и каква част за проучване и разработки в сферата на VoIP комуникациите?
- Какви са тенденциите им за наемане на персонал, отговорен за поддръжката на разглежданата система?

6.3.2. Услуги и функционалност

Голяма част от компаниите, имплементиращи VoIP, отдават прекалено голямо значение на този фактор, почти елиминирайки значимостта на останалите. Макар и важно, наличието или отсъствието на отделни функции не трябва да е ръководещо при избора на VoIP система. Основните търсени функции са налични при всички производители, а разликите между предлаганите решения обикновено се състоят в по-незначителни услуги. Оценка на базата на предлаганите функции трябва да бъде направена, като на всяка от тях се съпостави коефициент, отговарящ на важността й за компанията. Услуги, които не се използват към настоящия

момент и не се планира скорошното им внедряване, не бива да имат същата тежест, като основните и най-често използвани функции.

6.3.3. Надеждност на локалните партньори на компанията-производител

Не на последно по важност място е необходимостта от оценка на надеждността на локалните партньори на компанията-производител, изпълняващи имплементирането и поддръжката на избраната система. Това се налага, тъй като фирмите-производители рядко предлагат тези услуги. Поради това, че качеството на работа, нейното свършване в срок и последващата поддръжка зависят изцяло от партньорската фирма, работните отношения с тях обикновено са по-важни от тези с производителя.

6.3.4. Критерии за избор на локален партньор на компанията-производител

6.3.4.1. Финансова мощ

Както и при избора на производител, така и при избора на неговия партньор, извършващ имплементацията на системата и нейната поддръжка, финансовата мощ е фактор от голямо значение. От нея зависят както качеството на лабораториите, в които се извършва обучението на специалисти, така и нивото на самите специалисти, работещи за дадената компания. Отново важен въпрос е печеливша ли е компанията ?

6.3.4.2. Доверие

Голяма част от покупките са продиктувани от отношението към клиентите, цената на продукта или и от двете. При провеждане на преговори важен въпрос е дали търговският агент е единствения представител на компанията, който е ангажиран с изграждането на проекта и решаването на проблемите свързани с него или успоредно с него работи и технически екип. Ако по време на сделката

фирмата-доставчик не е достатъчно ангажирана с нея, каква е вероятността за коректни отношения след нейното осъществяване?

6.3.4.3. Опит

Важен фактор, влияещ върху избора на фирма за изграждане VoIP телефонната система е нейният опит с избрана платформа. Освен това, значение има и броят на техния персонал, отговарящ за нейното изграждане, както и броят на хората, отговарящи за нейната поддръжка. Дали фирмата разполага с два отделни екипа и ако не, обоснован ли е рискът от забавяне на внедряването на системата, поради пренасочване на изграждащия екип към извършване на поддръжка на друга система по време на течащата имплементацията? Относно опита на компанията много може да се научи от фирмата-производител, на която тя е партньор. Дори при отговор на производителя, че всеки техен партньор може да извърши имплементирането успешно, важно е да се поиска мнението, кой от тях ще го извърши най-добре, тъй като до голяма част успеха на проекта зависи именно от неговото изпълнение.

7. Конфигуриране на мрежовите устройства за VoIP

Като пример за конфигурация на IPT мрежа е разгледана компания с един централен и два отдалечени офиса. Избрана е стратегия за постепенна миграция към единна IP мрежа за гласи и данни. Първи етап при нея е инсталирането на CallManager сървър в централния офис и осигуряване на неговата свързаност със съществуващата УТЦ. Следващ етап е цялостното преминаване към IPT на отдалечените офиси и конфигуриране на тяхното взаимодействие с CallManager сървъра. Последна стъпка при обединяването на мрежите за глас и данни е миграцията на централния офис.

С цел обхващане на по-голям брой примерни ситуации, конфигурирането на обединената мрежа е разгледано в междинен стадий. На разглеждания етап е извършена инсталацията на CallManager и е завършено пълното преминаване към IPT в Офис1. От съображения за избягване на инвестиция в IP телефони на този етап, в Офис2 са използвани наличните аналогови телефонни апарати, свързани към маршрутизатора Router2 с помощта на FXS модули. Целта при това решение е постигане на спестявания от таксите за междуградски разговори при междуофисните комуникации преди преминаването към IPT и в Офис2.

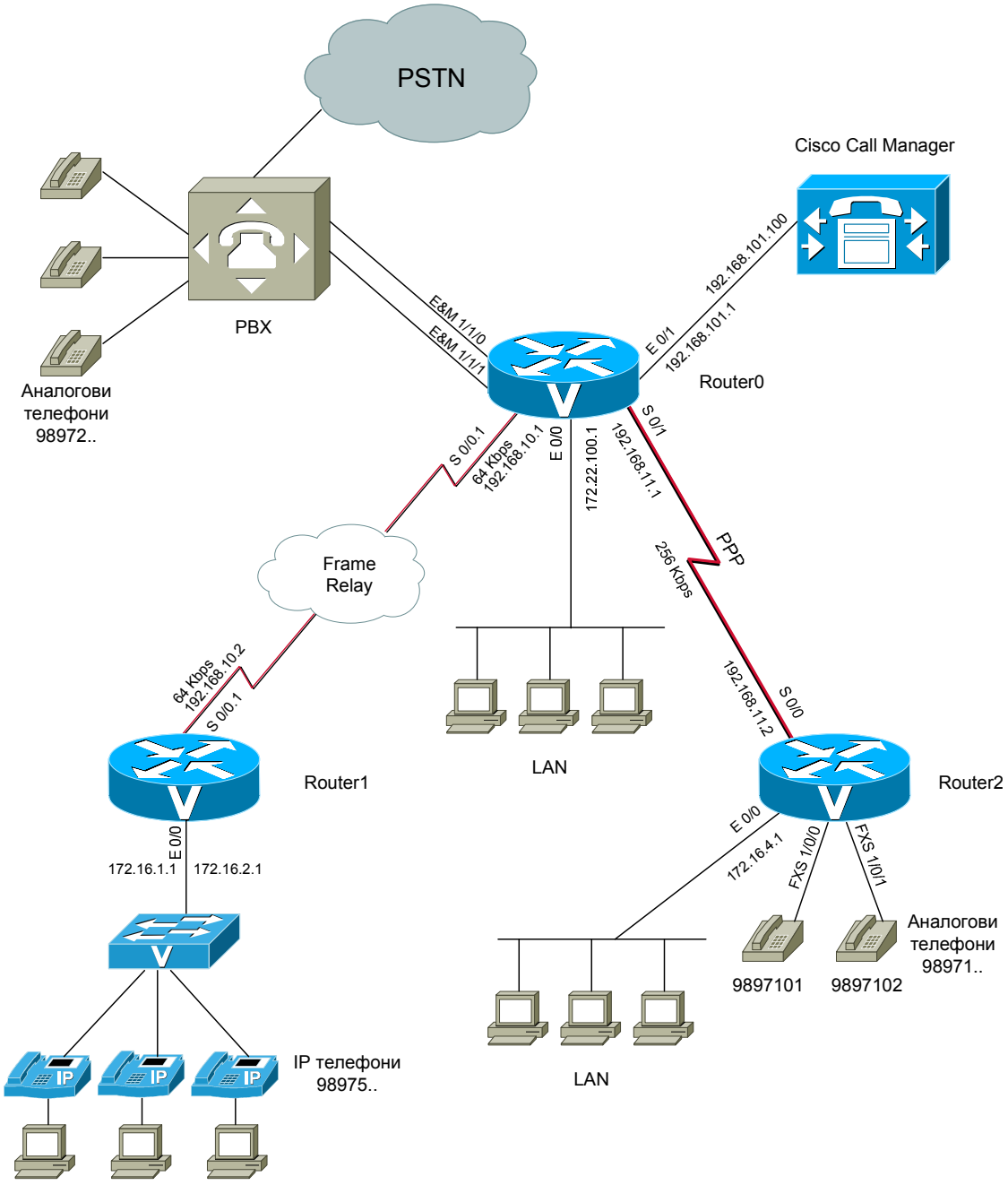
Инфраструктурата на съществуващата мрежа за данни е базирана на Cisco устройства. След събиране на статистика за натовареността на аналоговата телефонна мрежа на компанията е извършен и цялостен анализ на мрежата за данни. За успешно пренасяне на гласовите данни е установена необходимост от увеличаване на честотната лента на една от WAN връзките. С цел запазване на направените в мрежово оборудване инвестиции, при изграждането на IP телефонната мрежа е използвано оборудване на Cisco. Това предоставя възможност при сливането на мрежите за глас и данни да бъдат добавяни гласови модули към съществуващите устройства, което не налага цялостна подмяна на мрежовия хардуер. WAN връзката между Офис1 и централния офис е осъществена през Frame Relay мрежа. За връзка между Офис2 и централния офис е използвана наета линия. Връзките на всички офиси с обществената телефонна мрежа се осъществяват през централният офис.

При изграждане на телефонна мрежа трябва да бъде определен номерационен план, на който се подчиняват комуникациите в нея. Цел при неговото създаване е постигане на логическо съответствие между част от телефонния номер и физическото местоположение на търсения потребител. Друга важна характеристика на номерационния план е възможността за разширяването му, без това да налага промени в номерата на съществуващите потребители. Преди изграждане на номерационния план, трябва да бъде взето решение за начина, по който телефонни абонати извън мрежата на компанията ще имат достъп до нея. Съществуват два възможни начина, както и тяхното паралелно прилагане. Първият начин е разговори, постъпващи от външни телефонни мрежи да бъдат пренасочвани към търсения абонат от оператор, отговарящ на един или няколко фиксирани телефонни номера. Вторият начин е чрез автоматичен вход (DID), при който повикванията от обществената комутируема телефонна мрежа се маршрутизират директно, като за целта се използва набраният номер. Сигнализацията се предава в лентата на самият телефонен канал, без да бъде необходима намесата на оператор. При него е необходимо наемане на определен набор номера от обществения телефонен оператор. В разглеждания пример компанията е наела номерата в интервала от 9897100 до 9897599. Тяхното разпределение е както следва:

- 9897100 до 9897199 са предназначени за Офис2
- 9897200 до 9897299 са предназначени за централния офис
- 9897500 до 9897599 са предназначени за Офис1
- 9897300 до 9897499 са резервирани за бъдещи разширявания

Представените по-долу конфигурации са базирани на мрежовата инфраструктура, изобразена на фигура 7.1

Фигура 7.1. Съществуваща IP мрежа на компанията



7.1. Конфигуриране на предаване на гласови данни през Frame Relay мрежа

В разглеждания пример връзката между маршрутизаторите Router0 и Router1, позволяващи предаване на гласови данни, се осъществява през Frame Relay

мрежа. Маршрутизаторите, предаващи гласови данни, не винаги са директно свързани към WAN мрежата и достъпът им до устройствата с WAN интерфейси се осъществява през локалната мрежа. В тези случаи командите, конфигуриращи Frame Relay, се отнасят до устройствата имащи връзка с WAN, а не до вътрешните VoIP маршрутизатори. За осигуряване на качеството на гласовите услуги е необходимо конфигурирането на QoS механизми при изграждането на Frame Relay връзка. Те включват задаване на строг приоритет на гласовите данни чрез LLQ или IP RTP Priority, конфигуриране на Frame Relay Traffic Shaping, фрагментиране на данните и минимизиране на използваната честотна лента.

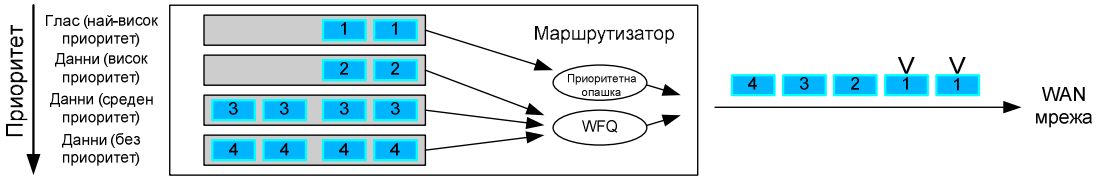
7.1.1. Задаване на строг приоритет на гласовия трафик

Съществуват два основни метода за задаване на приоритет на гласовия трафик [23]:

- IP RTP Priority работещ чрез Priority Queue/Weighted Fair Queuing (PQ/WFQ)
- LLQ работещ чрез PQ/Class Based Weighted Fair Queuing (PQ/CBWFQ)

При използване на IP RTP Priority, за всеки Frame Relay постоянен виртуален канал (PVC) бива създавана опашка със строг приоритет, обслужваща всички RTP пакети, изпращани до определен диапазон от UDP портове. Въпреки че конкретно използваните портове биват уточнявани в процеса на създаване на връзки, то диапазонът от портове е винаги един и същ за всички устройства, предаващи гласови данни. Веднъж разпознат, гласовият трафик бива поставян в опашка, имаща строг приоритет спрямо другите типове данни. Налагането на този приоритет става единствено в случаите на задръстване на дадения порт. Тогава само трафикът от приоритетната опашка бива предаван, а след нейното изпразване останалият трафик се изпраща по принципите, определени от WFQ (Фиг. 7.2).

Фигура 7.2. Предаване на пакети с IP RTP Priority



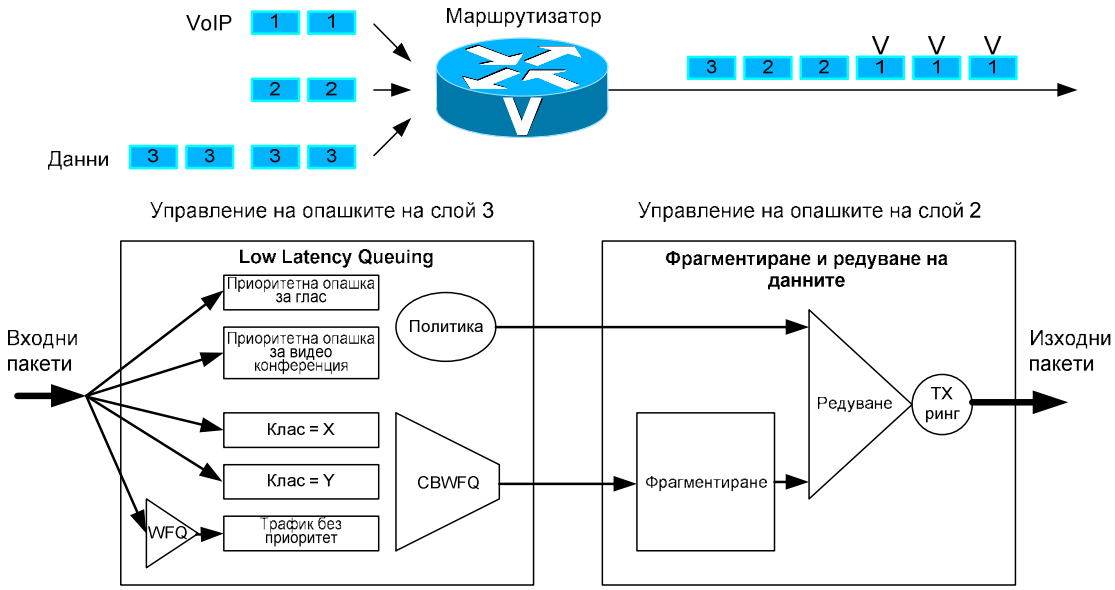
Конфигурирането на IP RTP Priority се извършва чрез командата:

```
Router(config-map-class)#frame-relay ip rtp priority starting-rtp-port
port-range bandwidth
```

където трябва да бъдат зададени номера на началния и броя портове, включени в диапазона от UDP портове, ползвани от RTP, който стандартно е 16384-32767. С тази команда се задава и максималната честотна лента, която може да бъде отделена за приоритетната опашка. Тя се определя на базата на максималния брой едновременни обаждания, които връзката трябва да може да предава.

Low Latency Queue (LLQ) е механизъм, предоставящ по голяма гъвкавост при приоритизиране на различни видове трафик (Фиг. 7.3).

Фигура 7.3. Предаване на пакети с LLQ



При имплементиране на VoIP гласовият трафик отново бива поставян в опашка със строг приоритет, но е възможно конфигуриране на параметри за недопускане на блокиране на останалия трафик. Това става чрез оказване на максималната честотна лента за приоритетната опашка. При настъпване на задръстване, тя бива обслужвана до достигане на този праг, след което пристигащите за нея пакети биват отхвърляни. LLQ позволява конфигуриране на няколко класа данни с различен приоритет и задаване на гарантирана честотна лента за всеки от тях.

Друго предимство на LLQ е възможността за определяне на пакетите, попадащи в приоритетните опашки, не само на базата на UDP портове, но и чрез списъци за достъп (Access List), хост адреси, ToS, IP Precedence и DSCP стойности. LLQ е по-сложен за конфигуриране и изборът между него и IP RTP Priority трябва да бъде основан на съществуващите видове трафик и техните времеви изисквания. Конфигурирането на LLQ се извършва на четири етапа:

1. Създаване на **`class map`** за гласовия трафик и определяне на критериите за принадлежност към него. За създаването му се използва командата:

```
Router(config)#class-map ?
      WORD class-map name
      match-all Logical-AND all matching statements under this classmap
      match-any Logical-OR all matching statements under this classmap
Router(config)#class-map match-all voice-traffic
```

Ключовата дума `match-all` изисква трафика, поставян в приоритетната опашка да изпълнява всички условия, зададени с командата **`match`**, докато при `match-any` е достатъчно само едно то тях да бъде изпълнено.

Критериите за съвпадение се задават с командата **`match`**. Нейният синтаксис за задаване на списък за достъп е:

```
Router(config-cmap)#match access-group ?
      <1-2699>     Access list index
      name         Named Access List
```

Възможно е чрез нея да се дефинира диапазон от UDP портове, ползвани от RTP:

```
Router(config-cmap)# match ip rtp 16384 16383
```

или съвпадение по DSCP класифицирането на пакетите от изпращащия ги хост:

```
Router(config-cmap)# match ip dscp ef
```

2. Създаване на клас (class map) за сигнализиращия трафик и определяне на критериите за принадлежност към него. Изпълнението на тази стъпка не е задължително.

```
Router(config)#class-map match-all voice-signaling
Router(config-cmap)#match access-group 103
Router(config)#access-list 103 permit tcp any eq 1720 any
Router(config)#access-list 103 permit tcp any any eq 1720
```

3. Определяне политиката за разпределяне на ресурсите на мрежовата връзка между различните създадени класове. Изпълнението на тази стъпка става чрез следните команди.

```
Router(config)#policy-map VOICE-POLICY
```

Командата **policy-map** създава политика на разпределение с името **VOICE-POLICY**. Следва конфигуриране на приоритета за отделните класове и максималната допустима честотна лента за всеки от тях. :

```
Router(config-pmap)#class voice-traffic
Router(config-pmap-c)#priority ?
      <8-2000000> Kilo Bits per second
```

Чрез тези команди данните от класа **voice-traffic** биват изпращани в опашката със строг приоритет. Стойността след командата **priority** определя нейната максимална честотна лента.

```
Router(config-pmap)#class voice-signaling
Router(config-pmap-c)#bandwidth 8
```

След създаване на клас **voice-signaling**, чрез команда **bandwidth** се резервират 8 Kbps за сигнализиращия трафик.

```
Router(config-pmap)#class voice-default
Router(config-pmap-c)#fair-queue
```

Командата **fair-queue** налага данните, неотговарящи на критериите за принадлежност към горните класове да бъдат предавани спрямо принципите, определени от WFQ. Важно условие при конфигуриране на политика на разпределение е сборът от стойностите след командите **priority** и **bandwidth** да бъде по-малък или равен на стойността на minCIR за конкретния PVC. В противен случай, създадената политика не може да бъде приложена към физическата връзка.

4. Активиране на LLQ чрез прилагане на дефинираната политиката за разпределение към изходящ WAN интерфейс:

```
Router(config)#map-class frame-relay VoIPovFR
Router(config-if)#service-policy output VOICE-POLICY
```

7.1.2. Конфигуриране на моделирането на Frame Relay трафика

Параметрите, моделиращи Frame Relay трафика, са удобен и ефективен начин за управление на мрежовите задръствания. При избор на подходящи стойности е възможно да бъдат избегнати точките на задръстване, свързващи високоскоростните връзки на централните офиси с по-бавните връзки към отдалечените клонове. Чрез тях може също да бъдат зададени стойности, ограничаващи потока от данни, изпращани през виртуалните вериги.

Един от параметрите, описващи Frame Relay връзките, е максималната им гарантирана пропускателна способност (CIR). Въпреки че е възможно обемът на моментно предаваните данни да надхвърля тази стойност, при конфигуриране на

връзки, предаващи гласови данни, това трябва да бъде забранено. Причината е липсата на гаранция за доставяне на по-големият обем, което в дадени случаи може да доведе до отхвърляне на гласови пакети и съответно понижаване на качеството на сигнала. Командата за определяне стойността на CIR има следният синтаксис:

```
Router(config-map-class)#frame-relay cir bits-per-second
```

Друг параметър, влияещ върху качеството на услугите при Frame Relay връзка, е максималния гарантиран брой битове, предавани за определен интервал от време (Bc). Препоръчителна стойност за този интервал (Tc) е 10 ms, като той не трябва да превишава 125 ms. Формулата за изчисляване на Tc е Tc = Bc / CIR. Тъй като не съществува команда за директно задаване на Tc, това може да бъде извършено чрез подходящо подбиране на стойността на Bc и задаването й със следната команда:

```
Router(config-map-class)#frame-relay Bc bits-per-second
```

Be е параметър, определящ броя битове за интервал от време, за които се прави опит да бъдат предадени в допълнение на гарантирания за този интервал трафик. По подразбиране стойността на Be е равна на нула, но след промяна тя може да бъде възстановена чрез командата:

```
Router(config-map-class)#frame-relay Be 0
```

7.1.3. Фрагментиране на данните

Активиране на механизъма за фрагментиране на данните се препоръчва за всички интерфейси, имащи скорост по-малка от 768 Kbps. Размерът на фрагментите трябва да бъде зададен така, че той да не налага фрагментиране на гласовите данни и същевременно забавянето при сериализирането на данните да не е повече от 20 ms. Определянето на големината на фрагментите между два маршрутизатора се извършва на базата на порта с най-ниска скорост на предаване

на данни. Пример за това е връзка между два маршрутизатора със скорости на интерфейсите им съответно 512 Kbps и 128 Kbps. В този случай размерът на фрагментиране и на двата маршрутизатора се задава на базата на връзката със скорост от 128 Kbps (Таб. 7.1). Всички постоянни виртуални вериги, конфигурирани върху един физически интерфейс, трябва да имат размер на фрагментите равен на този, използван от веригата пренасяща гласови данни.

Таблица 7.1. Фрагментиране на данните

Най-ниска скорост на предаване на данни	Препоръчителен размер на фрагментите
56 Kbps	70 bytes
64 Kbps	80 bytes
128Kbps	160 bytes
256 Kbps	320 bytes
512 Kbps	640 bytes
768 Kbps	1000 bytes
1536 Kbps	1600 bytes

Командата, задаваща размера на фрагментите има следния синтаксис:

```
Router(config-map-class)#frame-relay fragment bytes
```

7.1.4. Минимизиране на използваната честотна лента

Минимизиране на използваната честотна лента се постига чрез компресиране на хедърите на RTP пакетите. Този механизъм не трябва да бъде използван, ако след неговото активиране натовареността на процесора на маршрутизатора надхвърли 75 процента [23]. Компресирането на RTP хедърите не води до подобряване качеството на гласовия сигнал. То се препоръчва само при интерфейси със скорост по-малка от 768 Kbps. За конфигуриране се използва следната команда:

```
Router(config-if)#frame-relay ip rtp header-compression
```

При конфигурирането на маршрутизатор Router1 не е необходимо задаване на номерационен план и логически постове, тъй като IP телефоните в Офис1 получават тази и друга мрежова информация от CallManager сървъра при тяхното стартиране [4]. Конфигурацията на маршрутизатор Router1 се получава след прилагане на изброените по-горе команди:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router1
!
logging buffered 10000 debugging
enable secret 5 $1$MYS3$TZ6bwrhWB25b2cVpEVgBo1
!
ip subnet-zero
!
class-map match-all voice-signaling
  match access-group 103
class-map match-all voice-traffic
  match access s-group 102
!-- Дефиниране на класовете за гласов и сигнализиращ трафик и задаване на
!-- критерии за принадлежност на данните към тях, съответно списъците за достъп
!-- 102 и 103
!
policy-map VOICE-POLICY
  class voice-traffic
  priority 45
  class voice-signaling
  bandwidth 8
!-- Създаване на политика за разпределяне на ресурсите между отделните класове
!-- и поставяне на гласовия трафик в опашка със строг приоритет и максимална
!-- честотна лента 45 Kbps. Резервиране на 8 Kbps за сигнализация
!
  class class-default
  fair-queue
!-- Класът class-default се асоциира с трафика, неотговарящ на критериите за
!-- принадлежност към останалите класове. Командата fair-queue определя
!-- предаването на тези данни по принципите на WFQ
```

```
!
interface Ethernet 0/0
no ip address
!
interface Ethernet0/0.10
  encapsulation dot1q 10
  ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/0.20
  encapsulation dotq1 20
  ip address 172.16.2.1 255.255.255.0
  ip helper-address 192.168.101.100
!-- Задаване на трънк интерфейс с два подинтерфейса, ползващи енкапсулация IEEE
!-- 802.1q и принадлежащи съответно към VLAN 10 за данни и VLAN 20 за глас.
!-- Този интерфейс служи за връзка с комутатора за достъп, към който са
!-- свързани IP телефоните. Адресът зададен с командата ip helper-address служи
!-- за предаване на DHCP и BootP заявки, направени от IP телефоните към
!-- CallManager сървъра [4]
!
interface Serial0/0
  bandwidth 64
  no ip address
  encapsulation frame-relay
  no fair-queue
  frame-relay traffic-shaping
  frame-relay ip rtp header-compression
!-- Активиране на механизмите за моделиране на трафика. Ако това не бъде
!-- направено, трафикът не може да бъде разделен на създадените класове и
!-- командите за фрагментиране и LLQ не се изпълняват
!
interface Serial0/0.1 point-to-point
  bandwidth 64
  ip address 192.168.10.2 255.255.255.252
  frame-relay interface-dlci 400
  class VOIPovFR
!-- Свързване на подинтерфейса с главният клас VoIPovFR. Името VoIPovFR
!-- се определя от потребителя. Този интерфейс осигурява връзка с
!-- маршрутизатор Router0 в централния офис
!
ip classless
!
map-class frame-relay VOIPovFR
```

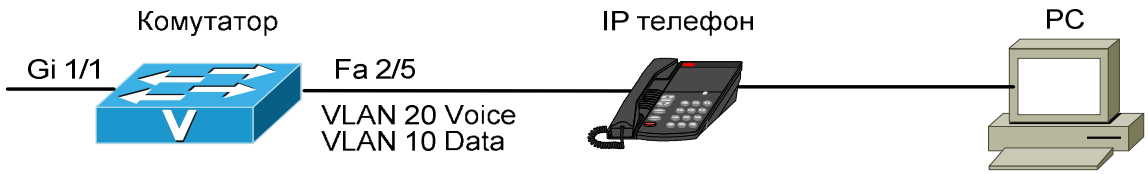
```
  no frame-relay adaptive-shaping
!--- Деактивиране на адаптивното моделиране на Frame Relay трафика
!
  frame-relay cir 64000
  frame-relay bc 640
!-- Изхождайки от формулата Tc = BC/CIR, конфигуриране на минималната допустима
!-- за Tc стойност от 10 ms чрез определяне на параметъра bc
!
  frame-relay be 0
  frame-relay mincir 64000
!-- Конфигуриране на минималния гарантиран трафик да съвпада с максималния.
!-- По подразбиране той е равен на половината от параметъра CIR
!
  service-policy output VOICE-POLICY
!-- Активиране на LLQ за постоянната виртуална верига
!
  frame-relay fragment 80
!-- Задаване стойност на размера за фрагментиране от 80 байта. Тази стойност се
!-- избира на базата на интерфейса с най-ниската скорост от участващите във
!-- връзката
!
access-list 102 permit udp any any range 16384 32767
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
!-- Списъкът за достъп 102 определя условията за поставяне на пакети в опашката
!-- със строг приоритет на базата на UDP портове, използвани за предаване на
!-- гласови данни. Условията на списъка за достъп 103 описват сигнализиращия
!-- трафик, като в конкретния случай параметрите отговарят на използваните от
!-- протокола H.323 V2
!
router rip
  network 192.168.10.0
  network 172.16.1.0
  network 172.16.2.0
```

7.2. Конфигуриране на комутатор за достъп със свързани към него IP телефони

При внедряване на IP телефони, както е в случая с Офис1 в разглеждания пример, е необходимо конфигуриране на връзките им със Cisco Catalyst комутатора

за достъп (Фиг. 7.4). Това включва конфигуриране на неговите интерфейси, електрическото захранване и качество на услугите.

Фигура 7.4. Схема на свързване на IP телефон и персонален компютър към комутатор за достъп



7.2.1. Конфигуриране на портовете на комутатора за достъп

Cisco IP телефоните разполагат с вграден в тях трипортов 10/100 комутатор. Всеки от неговите портове е с фиксирано предназначение. Порт 1 служи за връзка с комутатора за достъп или друго мрежово устройство, поддържащо VoIP. Порт 2 е вътрешен 10/100 интерфейс, пренасящ гласовия трафик. Порт 3 служи за връзка към персонален компютър или друго крайно устройство. Това позволява към един порт на комутатора за достъп да бъдат свързани едновременно IP телефон и през него персонален компютър. В този случай е необходимо гласовият трафик да бъде отделен от останалите данни с помощта на VLAN.

Съществува отделен гласов VLAN, който трябва да бъде активиран за всеки порт пренасящ гласов трафик, генериран от IP телефон. По подразбиране този VLAN е деактивиран. При неговото активиране автоматично бива активирана и Port Fast опцията за дадения порт. Синтаксисът на командата, активираща гласовия VLAN е:

```
Switch(config-if)#switchport voice vlan ?
      <1-4094>      Vlan for voice traffic
      dot1p         Priority tagged on PVID
      none          Do not tell telephone about voice vlan
      untagged      Untagged on PVID
```

- Първата опция изисква въвеждане на VLAN ID (идентификационен номер). В този случай комутаторът за достъп изпраща контролни CDP пакети, конфигуриращи IP телефона да предава гласовият трафик в 802.1Q фреймове, съдържащи VLAN ID и CoS стойност, указваща приоритет. По подразбиране стойността на CoS полето е 5 за гласовия трафик и 3 за контролните съобщения. Гласовия 802.1Q трафик се предава в гласовия VLAN
- Ключовата дума `dot1p` указва изпращането на CDP пакети, конфигуриращи IP телефона да предава гласовия трафик в 802.1p фреймове съдържащи VLAN ID 0 и CoS стойност по подразбиране. 802.1p трафикът се предава във VLAN за достъп
- Ключовата дума `none` позволява на IP телефона да използва собствената си конфигурация. Гласовият трафик се предава във VLAN за достъп
- Ключовата дума `untagged` указва изпращането на CDP пакети, конфигуриращи IP телефона да предава гласовия трафик без информация за VLAN ID и CoS стойност. Гласовият трафик се предава във VLAN за достъп

Следващият пример показва създаването на VLAN 10 за мрежови трафик и VLAN 20 за гласови данни на порт 0/5 на комутатора за достъп:

```
Switch #configure terminal
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 20
```

7.2.2. Конфигуриране на електрическото захранване за крайните устройства

Стандартът 802.3af, отнасящ се до електрическото захранване, предавано през Етернет мрежа, дефинира 15,4 W, осигурявани по подразбиране на всеки порт. Това може значително да натовари както устройствата, осигуряващи захранване,

така и електрическата мрежа. Решение е използване на функцията за интелигентно управление на захранването с помощта на CDP съобщения. Тя дава възможност крайните устройства да указват необходимото им захранване и то да се регулира за всеки порт на комутатора поотделно. Командата **power inline** служи за конфигуриране на PoE за даден порт. Нейният синтаксис е:

```
Switch(config-if)#power inline ?
      auto         Automatically detect and power inline devices
      consumption  Configure the inline device consumption
      never        Never apply inline power
      static       High priority inline power interface
```

- По подразбиране всички портове, поддържащи PoE са конфигурирани с опцията `auto`. Устройствата, които биват захранвани, се обслужват по реда на тяхното включване към мрежата. В случаите, когато не е налично достатъчно захранване за всички устройства, не може да бъде гарантирано кои от тях, намиращи се в `auto` режим, ще бъдат захранени
- Опцията `consumption` позволява ръчно конфигуриране на конкретна стойност
- Прилагането на ключовата дума `never` в конфигурацията на даден порт забранява подаването на захранване към него
- Портовете, конфигурирани с ключовата дума `static`, имат предимство при получаването на захранване пред портовете, зададени като `auto`. Необходимото захранване за `static` портовете бива резервирано дори и в случаите, в които към тях няма свързано устройство. Отделеното за тях захранване може да бъде или максималната стойност по подразбиране (15,4 W) или може да бъде зададено като конкретна стойност при конфигурацията на порта. При `static` портове за определяне на захранването не може да се използват CDP съобщения

За устройствата, свързани към `static` портовете се гарантира наличие на захранване. Към такива портове обикновено се свързват устройства с по-голяма

важност като безжични точки за достъп и телефонни апарати на ключови потребители. При необходимост на повече захранване от потреблението на `static` портовете, последните конфигурирани биват автоматично поставяни в състояние `error-disable`. Както `static`, така и `auto` портовете не подават захранване към устройства, изискващи по-голямо захранване от максималното предлагано от PoE модула. Следващия пример показва конфигуриране на PoE на порт 0/5:

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/5
Switch(config-if)#power inline auto
```

7.2.3. Конфигуриране на методите за осигуряване качество на услугите

По подразбиране, механизмите осигуряващи качество на услугите са деактивирани за всички портове. Командата **auto qos voip** улеснява тяхното конфигуриране, като прави предположения за мрежовата инфраструктура на базата на използваната ключова дума. Изпълнението на тази команда води до приоритизиране на определен трафик в изходящата опашка. В противен случай всички данни биват предавани според реда на тяхното пристигане. Синтаксиса и е:

```
Switch(config-if)#auto qos voip ?
       cisco-phone         Trust the QoS marking of Cisco IP Phone
       cisco-softphone     Trust the QoS marking of Cisco IP SoftPhone
       trust               Trust the DSCP/CoS marking
```

При първо задаване на **auto qos voip**, механизмите за качество на услугите биват активирани за целия комутатор, а заедно с това биват конфигурирани отделните опашки и прагове в глобалната конфигурация. Следваща стъпка е конфигурирането на порта, на който е зададена командата, да приема входящите CoS стойности. Конфигурирането на връзка с IP телефон става по следния начин:

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/5
Switch(config-if)#auto qos voip cisco-phone
```

В случаите, в които гласовият трафик преминава през трънк порт на комутатора за достъп, е необходимо конфигуриране на качество на услугите чрез задаване на ключовата дума **trust**:

```
Switch#configure terminal
Switch(config)#interface gigabitethernet 1/1
Switch(config-if)#auto qos voip trust
```

Когато гласовият трафик преминава по връзка от трети слой на OSI модела, трябва да бъде указано предаването на информация за приоритета на различните видове трафик, съдържаща се в хедърите на IP пакетите. За целта се използва допълнителна команда, налагаща предаването на **dscp** стойностите:

```
Switch#configure terminal
Switch(config)#interface gigabitethernet 1/1
Switch(config-if)#auto qos voip trust
Switch(config-if)#mls qos trust dscp    !--- Catalyst 3560/3750/6500
ИЛИ
Switch(config-if)#qos trust dscp        !--- Catalyst 4500
```

7.2.4. Конфигуриране чрез макроси

Някой комутатори предлагат възможност за конфигуриране на техните портове чрез предварително дефинирани макроси. Съществуват различни макроси, описващи често срещани стандартни ситуации. Два от тях са свързани с поддържането на IP телефони [24].

- cisco-phone – тази ключова дума се използва при директно свързване на IP телефони. Макросът конфигурира порта с отделен VLAN за глас, VLAN за данни, port security, spanning-tree portfast и качество на услугите
- cisco-switch – този макрос се използва при трънк портове, свързващи разпределителния слой и слоя за достъп на потребителските станции. Чрез

него се конфигурира използване на dot1q, задава се връзка тип point-to-point и се активират механизми за качество на услугите.

Съдържанието на макросите може да бъде видяно чрез командата **show parser macro**:

```
Switch #show parser macro name cisco-phone

# Cisco IP phone + desktop template
# macro keywords $access_vlan $voice_vlan
# VoIP enabled interface - Enable data VLAN
# and voice VLAN
# Recommended value for access vlan should not be 1
switchport access vlan $access_vlan
switchport mode access

# Update the Voice VLAN value which should be
# different from data VLAN
# Recommended value for voice vlan should not be 1
switchport voice vlan $voice_vlan

# Enable port security limiting port to a 2 MAC
# addressess - - One for desktop on data vlan and
# one for phone on voice vlan
switchport port-security
switchport port-security maximum 2

# Ensure port.security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

Използването на макросите става чрез задаване на конкретни стойности на параметрите в тях, които в долния пример са идентификаторите на VLAN мрежите:

```
Switch#configure terminal
Switch(config)#interface gigabitethernet 2/5
Switch(config.if)#macro apply $access_vlan 10 $voice_vlan 20
```

За предаване на маркираните с идентификатор за VLAN принадлежност данни към маршрутизатор Router1 е необходимо конфигуриране на трънк порт. Това може да бъде направено чрез следните команди:

```
Switch #configure terminal
Switch(config)#interface gigabitethernet 0/0
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

7.3. Конфигуриране на предаване на гласови данни през наета линия

Маршрутизатор Router2 е свързан към централния офис през наета линия с капацитет 256 Kbps. Правило при планиране на честотната лента на WAN връзки е използване на не повече от 75 процента от максималния капацитет на връзката за комбинирано предаване на глас и данни. За междуофисни комуникации е препоръчително използване на кодеци, изискващи по-малка честотна лента, като приложения в примера кодек G.729. Конфигурирането на връзката включва задаване на избрания номерационен план, осигуряване свързаността между телефонните постове и активиране на механизми за качество на услугите.

7.3.1. Конфигуриране на номерационен план

При конфигуриране на номерационен план за аналогови телефони без използване на CallManager или друг вид сървър за управление на повикванията е необходимо ръчно конфигуриране на свързаността между отделни телефонни абонати или групи абонати. Офис2 е снабден единствено с аналогови телефонни апарати. При IP телефоните сигналът “избирай” се съхранява локално в телефона, под формата на WAV файл. За разлика от тях, при аналоговите апарати той трябва да бъде подаден от порта на FXS модула, към който те са свързани [3].

Необходимото конфигуриране на мрежовите устройства, към които са свързани аналоговите телефони, може да бъде разделено на две основни стъпки. Първата касае физическите портове и типа сигнализация, използвана между двете устройства. Командата, с която се преминава в режим за конфигуриране на гласовия FXS порт е:

```
Router(config)#voice-port slot/subunit/port
```

където *slot* е номерът на слота на маршрутизатора, в който е инсталиран мрежовия модул с разположени на него FXS карти. Ключовата дума *subunit* отговаря на номера на слота на мрежовия модул, отделен за конкретната FXS карта. *Port* съответства на номера на порта на FXS картата, който ще бъде конфигуриран. За задаване на типа сигнализация се използва командата:

```
Router(config-voiceport)# signal {loop-start | ground-start}
```

където при използване на ключовата дума **ground-start** разговорът може да бъде прекратен от всяка от участващите страни, докато при **loop-start** това може да направи само страната, инициирала разговора. Втората стъпка е свързана с конфигурирането на логическите постове, асоцииращи физическите гласови портове с телефонни номера. За целта е необходимо преминаване в режим за конфигуриране на логически пост. Синтаксисът на командата е:

```
Router(config)#dial-peer voice tag {voip | pots}
```

където *tag* е идентификатор на логическия пост в интервала 1-2147483647. Изборът на този идентификатор е свободен, но при възможност е препоръчително той да съвпада с съответстващия му телефонен номер. Това се прави с цел улеснение при проверка на конфигурацията или при отстраняване на проблеми. Ключовите думи **voip** и **pots** дефинират метода за енкапсулация на гласовите данни, като при конфигуриране на аналогови телефони се използва **pots**, а при IP телефони съответно **voip**. След преминаване в режим за конфигуриране config-dial-peer, изпълнението на команда **destination-pattern** задава телефонния номер отговарящ на създадения логически пост.

```
Router(config-dial-peer)#destination-pattern [+]string[T]
```

където незадължителния символ "**+**" указва, че символният низ, намиращ се след него, е стандартен E.164 телефонен номер. Думата ***string*** съответства на символен низ, отговарящ на телефонен номер от частен номерационен план или стандартен E.164 номер. Допустими символи при задаването на този низ са цифрите от 0 до 9, буквите от A до D, както и специалните символни (*) (#) (,) (.) (%) (+) (^) ($) (\) (?) ([]) и (()). При проверка на конфигурирания с командата **destination-pattern** символен низ за съвпадение с избран телефонен номер, специалният символ (.) замества произволна избрана цифра. Незадължителният управляващ символ "**T**" указва произволна дължина на символния низ. Това дава възможност на маршрутизатора да изчака набирането на всички символи преди пренасочване на обаждането.

За указване на конкретен мрежови адрес за получаване на обаждания от текущо конфигурирания VoIP логически пост се използва командата:

```
Router(config-dial-peer)#session target {ipv4:destination-address |
dns:[$s$. | $d$. | $e$. | $u$.] host-name | enum:table-num | loopback:rtp | ras
| sip-server}
```

където чрез опция **ipv4** се задава IP адреса на получаващия обажданията маршрутизатор. Командата **port** служи за асоцииране на логическия пост с конкретен физически порт.

```
Router(config-dial-peer)#port slot/subunit/port
```

7.3.2. Конфигуриране на методите за осигуряване качество на услугите

За осигуряване качеството на услугите върху наетата линия е използван RSVP [2]. Този протокол дава възможност за резервиране на честотна лента, необходима за осъществяване на предварително определен брой едновременни разговори. По този начин се гарантира предаването на нужния обем данни, независимо от натовареността на връзката. Командата, активираща RSVP има следният синтаксис:

```
Router(config-if)#ip rsvp-bandwidth [interface-kbps] [single-flow-kbps]
```

където незъдължителните ключови думи **interface-kbps** и **single-flow-kbps** задават съответно частта от честотната лента, която да бъде резервирана и честотната лента, заделена за всеки отделен поток от данни. Така може да бъде резервирана честотна лента, необходима за конкретен брой обаждания и едновременно с това да бъде зададена нужната за едно обаждане част от нея. Други команди, служещи за подобряване на качеството на разговора, са командите за подтискане на ехото в сигнала. Активирането на тези механизми за даден гласов порт се извършва чрез команда **echo-cancel enable**

```
Router(config-voiceport)#echo-cancel enable type [hardware | software]
```

където незадължителните ключови думи **hardware** и **software** определят начина на премахване на ехото, съответно хардуерно или софтуерно. Чрез команда **echo-cancel coverage** се задава продължителността на периода за подтискане на звука, изпратен и получен от един и същи интерфейс.

```
Router(config-voiceport)#echo-cancel coverage {8 | 16 | 24 | 32 | 48 |
64}
```

Цялостната конфигурация на маршрутизатор Router2, свързана с предаването на гласови данни, се получава след прилагане на изброените по-горе команди:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router2
!
logging buffered 10000 debugging
enable secret 5 $1$MYS3$TZ6bwrhPl76b2cVpE0kLP65
!
ip subnet-zero
!
memory-size iomem 20
!
dial-peer voice 7101 pots
  destination-pattern +9897101
  port 1/0/0
!-- Създаване на логически пост 7101, обслужващ телефонен абонат с номер
!-- 9897101, директно свързан към FXS порт 1/0/0
!
dial-peer voice 7102 pots
  destination-pattern +9897102
  port 1/0/1
!-- Създаване на логически пост 7102, обслужващ телефонен абонат с номер
!-- 9897102, директно свързан към FXS порт 1/0/1
!
dial-peer voice 72 voip
  destination-pattern +98972..
  session target ipv4:192.168.11.1
!-- Създаване на логически пост за връзка с телефонните постове, обслужвани
!-- от съществуващата УТЦ в централния офис
!
dial-peer voice 75 voip
```

```
  description "calls to IP Phones/CallManager"
  codec g723r63
  destination-pattern +98975..
  session target ipv4:192.168.101.100
!-- Създаване на логически пост за връзка с всички IP телефони, управлявани от
CCM
!
dial-peer voice 50 pots
  destination-pattern .T
  session targrt ipv4:192.168.11.2
!-- Създаване на два логически поста за връзка с обществената телефона мрежа
!
num-exp 7 +9897...
!-- Активиране на механизма за автоматично добавяне на префикс към избран
!-- номер. Въведена от потребител начална цифра 7 бива тълкувана от
!-- маршрутизатора като 9897. Това позволява използване на кратки вътрешни
!-- номера между потребители в мрежата.
!
voice-port 1/0/0
  description << This voice port is FXS >>
  signal loop-start
  echo-cancel coverage 16
  echo-cancel enable
  req-qos controlled-load
!-- Конфигуриране на FXS порт 1/0/0 с описание на връзката, типа сигнализация,
!-- активиране и задаване на параметри за премахване на ехото и указване на
!-- приоритет на гласовия трафик, гарантиран чрез RSVP
!
voice-port 1/0/1
  description << This voice port is FXS >>
  echo-cancel coverage 16
  echo-cancel enable
  req-qos controlled-load
!-- Конфигуриране на FXS порт 1/0/1 с описание на връзката, типа сигнализация,
!-- активиране и задаване на параметри за премахване на ехото и указване на
!-- приоритет на гласовия трафик гарантиран чрез RSVP
!
interface Ethernet0/0
  ip address 172.16.4.1 255.255.255.0
!
interface Serial0/0
  bandwidth 256
```

```
  ip address 192.168.11.2 255.255.255.252
  encapsulation ppp
  no ip mroute-cache
  fair-queue
  ip rtp-header-compression
  ip rsvp-bandwidth 48 24
!-- Конфигуриране на сериен интерфейс 0/0, служещ за връзка с маршрутизатор
!-- Router0 през наета линия. Задаване на честотна лента 256 Kbps, енкапсулация
!-- PPP,компресия на RTP хедърите и резервиране на честотна лента за два
!-- телефонни разговора
!
ip classless
!
router rip
  network 192.168.11.0
  network 172.16.4.0
```

7.4. Конфигуриране на връзка между IP телефонна мрежа и аналогова УТЦ

Преминаването към IPT в централния офис на компанията ще бъде извършено на по-късен етап спрямо разглежданата конфигурация. Към момента, за функционирането на обединената мрежа е необходимо да бъде осигурена гласова свързаност с отдалечените офиси, както и да бъде изградена връзка към съществуващата УТЦ.

Съществуват няколко възможни начина за свързване на IPT мрежа към аналогова телефонна централа. Те могат да бъдат разделени в две основни категории – аналогови трънкове и цифрови трънкове. Примери за аналогови трънкове са FXS и E&M, а за цифрови ISDN [3]. Изборът на конкретен вид трънк зависи в най-голяма степен от предлаганите от производителя на УТЦ видове комуникационни модули. Също така производителят на наличната УТЦ трябва да предостави нужните материали за препрограмиране на телефонната централа при свързването й с IPT мрежата. Основната разлика между аналоговите и цифровите трънкове е в поддържания от тях брой телефонни линии. Аналоговите трънкове осигуряват една телефонна линя за всеки техен интерфейс, докато един ISDN или

E1 интерфейс може да поддържа до 30 линии. За нуждите на разглеждания пример е използван един E&M модул. Важно условие за успешното конфигуриране на свързаността между УТЦ и маршрутизатор Router0 е параметрите, описващи връзката, да бъдат еднакво зададени и на двете устройства [3]. Тези параметри включват типа сигнализация, използването на дву или четири проводен кабел, задаване на импеданса и други. За настройването им е необходимо преминаване в режим за конфигуриране на гласовия порт:

```
Router(config)#voice port slot/subunit/port
```

Командата **dial-type** определя типа на набиране на телефонен номер:

```
Router(config-voiceport)#dial-type {dtmf | pulse | mf}
```

където опциите са съответно тонално, импулсно или мултичестотно избиране. За задаване на типа сигнализация при E&M порт се използва командата **signal**:

```
Router(config-voiceport)#signal {wink-start | immediate | delay-dial | lmr}
```

където опцията използвана по подразбиране е *wink-star*. Типът на използвания за връзка кабел се определя с командата **operation.**

```
Router(config-voiceport)#operation {2-wire | 4-wire}
```

където вариантите са използване на дву или четири проводен кабел. Команда **impedance** определя прекъсващия импеданс при аналогови телефонни интерфейси:

```
Router(config-voiceport)#impedance {600c | 600r | 900c | 900r | complex1 | complex2 | complex3 | complex4 | complex5 | complex6}
```

където стойността по подразбиране е *600r*. Командата **type** определя типа E&M интерфейс за конкретен гласов порт:

```
Router(config-voiceport)#type {1 | 2 | 3 | 5}
```

Като бъдат взети предвид принципите и командите, използвани за конфигуриране на маршрутизатор Router1 и Router2, както и разгледаните по-горе команди за осигуряване на връзка със съществуващата УТЦ, конфигурацията на маршрутизатор Router0 от гледна точка на предаването на гласови данни е следната:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router0
!
boot system flash slot1:c3640-is-mz.122-6a.bin
logging buffered 1000000 debugging
!
ip subnet-zero
!
class-map match-all voice-signaling
  match access-group 103
class-map match-all voice-traffic
  match access-group 102
!
policy-map voice-policy
  class voice-signaling
  bandwidth 8
  class voice-traffic
  priority 45
  class class-default
  fair-queue
!
interface Ethernet0/0
  ip address 172.22.100.1 255.255.255.0
!-- интерфейс към мрежата за данни
!
interface Ethernet0/1
  ip address 192.168.101.1 255.255.255.252
```

```
!-- Интерфейс към Cisco CallManager (CCM)
!
interface Serial0/0
  bandwidth 128
  no ip address
  encapsulation frame-relay
  no ip mroute-cache
  no fair-queue
  frame-relay traffic-shaping
  frame-relay ip rtp header-compression
!
interface Serial0/0.1 point-to-point
  bandwidth 128
  ip address 192.168.10.1 255.255.255.252
  frame-relay interface-dlci 300
  class VOIPovFR
!-- Конфигуриране на сериен интерфейс 0/0, осигуряващ връзка с маршрутизатор
!-- Router2
!
interface Serial0/1
  bandwidth 256
  ip address 192.168.11.1 255.255.255.252
  encapsulation ppp
  no ip mroute-cache
  fair-queue
  ip rtp-header-compression
  ip rsvp-bandwidth 48 24
!-- Конфигуриране на сериен интерфейс 0/1, служещ за връзка с маршрутизатор
!-- Router2 през наета линия. Задаване на честотна лента 256 Kbps, енкапсулация
!-- PPP,компресия на RTP хедърите и резервиране на честотна лента за два
!-- телефонни разговора
!
ip classless
!
map-class frame-relay VOIPovFR
  no frame-relay adaptive-shaping
  frame-relay cir 64000
  frame-relay bc 640
  frame-relay be 0
  frame-relay mincir 64000
  service-policy output voice-policy
  frame-relay fragment 80
```

```
!
access-list 102 permit udp any any range 16384 32767
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
!
voice-port 1/1/0
  description << This Voice Port is E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
  echo-cancel coverage 16
  echo-cancel enable
!
voice-port 1/1/1
  description << This Voice Port is E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
  echo-cancel coverage 16
  echo-cancel enable
!-- Конфигуриране на E&M портове към УТЦ, активиране на механизмите за
!-- премахване на ехото в сигнала и задаване на продължителността на периода на
!-- подтискане на звука, изпратен и получен от един и същи интерфейс
!
dial-peer voice 71 pots
  destination-pattern +98971..
  session target ipv4:192.168.11.2
!-- Създаване на логически пост за връзка с телефонните абонати, свързани към
!-- маршрутизатор Router2
!
dial-peer voice 75 voip
  description "calls to IP Phones/CallManager"
  codec g723r63
  destination-pattern +98975..
  session target ipv4:192.168.101.100
!-- Създаване на логически пост за връзка с всички IP телефони, управлявани от
!-- CCM
!
dial-peer voice 720 pots
  destination-pattern 98972..
```

```
  port 1/1/0
!
dial-peer voice 721 pots
  destination-pattern 98972..
  port 1/1/1
!-- Създаване на два логически поста за връзка с телефонните постове, обслужвани
!-- от съществуващата УТЦ в централния офис
!
dial-peer voice 50 pots
  destination-pattern .T
  port 1/1/0
!
dial-peer voice 50 pots
  destination-pattern .T
  port 1/1/1
!-- Създаване на два логически поста за връзка с обществената телефонна мрежа
!
num-exp 7 +9897...
!
router rip
network 192.168.10.0
network 192.168.11.0
network 192.168.101.0
network 172.22.100.0
```

8. Заключение

Темповете с които съвременния бизнес внедрява IP телефонни решения надминават и най-смелите очаквания на привържениците и създателите на VoIP технологията.

Представената дипломна работа е разработена и структурирана като обстойно практическо ръководство за изграждане на VoIP комуникационна среда на базата на съществуваща мрежа за данни. Тя представлява детайлен анализ на ползите от внедряването на VoIP, на възможните проблеми и техните решения при обединяване на мрежите за пренос на глас и данни, както и на стимулите за извършване на миграцията. Разгледани са случаите, най-подходящи за извършване на преход, както и варианти за неговата реализация. Описани са също предимствата и възможните проблеми при внедряването на съпътстващите VoIP технологии, като PoE и предаването на глас през Wi-Fi мрежи. Така разработена, дипломната работа дава възможност да бъдат планирани, проектирани и имплементирани цялостни VoIP системи на базата на конкретни потребителски изисквания.

IP телефонията измества все повече традиционните телефонни мрежи. Въпреки съществуването на множество преимущества, много често критичен въпрос при взимане на решения за преминаване към VoIP е възможността за постигане на надеждност на системата, не по-малка от тази на традиционната телефонна мрежа. Поради това в дипломната работа е отделено особено внимание на изискванията за надеждност и методите за повишаването й. Разгледано е реално доказателство на базата на мрежови компоненти на Cisco, показващо че при планиране, проектиране и имплементиране на VoIP системи с оглед на необходимата надеждност се гарантира достигане на показатели, надвишаващи тези, характеризиращи традиционните телефонни системи.

Основен стимул за имплементиране на VoIP е възможността за понижаване на разходите. Финансовите отдели на компаниите все по-често поставят под въпрос нуждата от съществуването на две отделни устройства за гласови и мрежови комуникации, две отделни преносни среди и два различни отдела за тяхната

поддръжка. Така финансовите изгоди налагат преминаването към единна мрежа за глас и данни, а облагодетелствани от това са нейните потребители, получаващи множество нови функции и възможност за моделирането им според техните конкретни изисквания. В настоящата дипломна работа са разгледани основните начини за съкращаване на разходите за телефонни комуникации, като са посочени и ползите, произхождащи директно от имплементирането на VoIP. Разгледан е модел за тяхното оценяване и увеличаването им чрез фокусиране върху разработването на софтуерни приложения, влияещи положително на ключовите за съответната компания бизнес инициативи.

Една от стъпките при внедряване на IP телефонна система е конфигурирането на мрежовите устройства за предаване на гласови данни и необходимите механизми, осигуряващи качество на услугите. В дипломната работа е разгледана примерна съществуваща мрежова инфраструктура и са представени конфигурациите на няколко типични схеми за междуофисна комуникация. Едно разширение на настоящия проект би могло да включва както допълнителни примерни конфигурации при използване на друг вид свързаност, така и описание и конфигуриране на функциите на сървъра за управление на повикванията.

Важен етап в бъдещото развитие на VoIP комуникациите е преминаването към изцяло IP телефонни обаждания, провеждани не само между служителите на една и съща компания, а между произволни два IP телефона. Тогава сигурността при предаване на гласовите данни ще бъде фактор от голямо значение. В отговор на това в изложението на дипломната работа са засегнати основните практики за осигуряване на защитени комуникации, като са набелязани най-разпространените видове атаки и възможности за пробиви. Възможност за развитие на представения проект е разглеждане и прилагане на конкретни начини за конфигуриране на защитни механизми.

Друга насока за развитие на разгледаната примерна VoIP мрежа е добавянето на видео данни, пренасяни през единната мрежова инфраструктура. Ползите от това са безпрепятственото осъществяване на видеоконферентни връзки между всеки две точки в компанията и премахване на необходимостта от

инвестиране и поддръжка на специализирано оборудване, достъпно само за отделни служители.

Бъдещото развитие на VoIP технологии е ограничено единствено от въображението на потребителите и техните изисквания. Процесът на постепенно сливане на функционалността на преносимите и персоналните компютри и телефонните апарати набира скорост. Новите решения ще бъдат както финансово по-изгодни, така и по-функционални. Дните, в които на едно и също бюро ще стоят редом интелигентните, постоянно еволюиращи персонални компютри, стационарните аналогови телефони и мобилните GSM апарати са преброени. Това е вече остарял, скъпо струващ модел за комуникация, чиято реална алтернатива е VoIP. И неговата съдба ще бъде като тази на други велики изобретения, напълно изместени от новите технологии. Единствено времето ще покаже, колко бързо ще се случи това.

Използвана литература

[1] Ramesh Kaza, Salman Asadullah; Cisco IP Telephony: Planning, Design, Implementation, Operation and Optimization; Cisco Press (2005);

[2] Robert Padjen, Larry Keefer, Sean Thurston, Jeff Bankston, Michael E. Flannagan; Cisco AVVID and IP Telephony Design & Implementation; Syngress Publishing Inc. (2001);

[3] Paul J. Fong, Eric Knipp, David Gary, Scott M. Harris. Larry Keefer Jr., Charles Riley, Stuart Ruwet, Robert Thorstensen, Vincent Tillirson; Configuring Cisco Voice over IP, Second Edition; Syngress Publishing Inc. (2002);

[4] Jonathan Davidson, James Peters; Voice over IP Fundaments; Cisco Press (2000);

[5] Kevin Brown; IP Telephony Unveiled; Cisco Press (2004);

[6] Sean Christensen; Voice over IP Solutions; Juniper Networks Inc. (2001);
http://cn.juniper.net/solutions/literature/white_papers/200011.pdf

[7] Patrick Scheckel; When and How to Migrate to IP Telephony; Berbee Information Networks Corporation (2005);
http://www.berbee.com/public/learning/MigrateToIPTelephony.aspx

[8] Understanding VoIP; Avaya Inc. (2005);
http://www.invictusnetworks.com/faq/Voice over IP VoIP/Avaya VoIP White Paper.pdf

[9] Designing converged enterprise networks for IP telephony; Nortel Networks (2002);
http://www.nortel.com/solutions/pt/es/collateral/nn102460-110602.pdf

[10] IP Telephony: The Five Nines Story; Cisco Systems (2002);
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_white_paper09186a00800a113e.shtml

[11] Enterprise VoIP Security: Potential Threats and Best Practices; Global Knowledge Network Inc. (2005);
http://www.itdepartment.com/VoIP/VoipSecurityThreats and Best Practices.pdf

[12] Network Security Best Practices for IP Telephony; ShoreTel Inc. (2005);
http://www.baysidemedia.com/ShoreTel/Security_Best_Practices.pdf

[13] The Real World of VoIP; NetworkWorld

[14] Strategies for IP Telephony Evaluation and Migration; InfoTech (2005);
http://www.voicepro.com/_files/user/InfoTech Building Client Value1.pdf

[15] Selecting VoIP for Your Enterprise; Global Knowledge Network Inc. (2005);
http://images.globalknowledge.com/wwwimages/whitepaperpdf/SelectingVoIP.PDF

[16] Jim Seals; Voice over IP; MoreNet, Network Consulting (2001);
http://www.more.net/technical/research/voip/voip.pdf

[17] Susan Andersen; Voice over IP (VoIP) Basics for IT Technicians; Fluke Networks (2005);
http://www.s-t.pl/pub/VoIP_Basics.pdf

[18] Understanding Packet Voice Protocols; Cisco Systems Inc. (2002);
http://www.sipcenter.com/sip.nsf/html/WEBB5YP4SU/$FILE/Cisco_UPVP_wp.pdf

[19] IP Telephony Design Guide; Alcatel-Lucent (2003);
http://www1.alcatel-lucent.com/enterprise/en/resource_library/pdf/wp/wp_IPT_Design-Guide.pdf;jsessionid=1KOVIEHHCETR1LAWFRUE1DFMCYWGI3GC

[20] D. Richard Kuhn, Tomas J. Walsh, Steffen Fries; Security Considerations for Voice over IP Systems; National Institute of Standards and Technology (2005);
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[21] Robert Heger, Michelle Le, Dana Nartea, Assaf Maoz; Voice over Internet Protocol; IS-311 in Business (2002);
http://www.csun.edu/~vcact00f/311/termProjects/700class/IS 311 VoIP.doc

[22] Todd Leinberger, David Rytzarev; The Future Internet Telephony Standard: H.323 or Session Initiation Protocol; Ohio University (2004);
http://oak.cats.ohiou.edu/~tl277601/esp/review_voip_protocols.htm

[23] VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority); Cisco Systems (2006);
http://www.cisco.com/warp/public/788/voice-qos/voip-ov-fr-qos.pdf

[24] Configure IOS Catalyst Switches to Connect Cisco IP Phones Configuration Example; Cisco Systems (2006);
http://www.cisco.com/warp/public/473/configuring-cat-ip-phone.pdf

Речник на използваните съкращения

AF - Assured Forwarding

CAC - Call Admission Control

CDP - Cisco Discovery Protocol

CIR - Committed Information Rate

CCM - Cisco CallManager

CoS - Class of Service

DC - Direct Current

DE - Default Forwarding

DHCP - Dynamic Host Configuration Protocol

DID - Direct Inward Dial

DiffServ - Differentiated Services

DoS - Denial of Service

DSCP - Differentiated Service Code Point

DSL - Digital Subscriber Line

EF - Expedited Forwarding

E&M - Ear&Mouth, transMit&rEceive

FDM - Frequency Division Multiplexing

FRTS - Frame Relay Traffic Shaping

FXS - Foreign Exchange Station

GSM - Global System for Mobile Communications, Groupe Spécial Mobile

HSRP - Hot Standby Router Protocol

HTTP - Hypertext Transfer Protocol

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IOS - Internetworking Operating System

IP - Internet Protocol

IPT - Internet Protocol Telephony

IPSec - IP Security

ISDN - Integrated Services Digital Network

ITU - International Telecommunication Union

LAN - Local Area Network

LLQ - Low Latency Queue

MAC - Media Access Control

MOS - Mean Opinion Score

MTP - Message Transfer Parts

OSI - Open System Interconnection

PCM - Pulse Code Modulation

PDA - Personal Digital Assistant

PESQ - Perceptual Evaluation of Speech Quality

PHB - Per-Hop Behavior

PoE - Power over Ethernet

POTS - Plain Old Telephone Service

PQ/CBWFQ - Priority Queue /Class Based Weighted Fair Queuing

PQ/WFQ - Priority Queue/Weighted Fair Queuing

PRI - Prime Rate Interface

PSTN - Public Switched Telephone Network

PVC - Permanent Virtual Circuit

QoS - Quality of Service

RFC - Request For Comments

ROI - Return on Investments

RSVP - Resource Reservation Protocol

RTCP - Real Time Control Protocol

RTCP XR - RTP Control Protocol Extended Reports

RTP - Real-time Transport Protocol

SCCP - Skinny Client Control Protocol

SCP - Service Control Point

SDP - Session Description Protocol

SMTP - Simple Message Transfer Protocol

SNMP - Simple Network Management Protocol

SS7 - Signaling System Seven

SSL - Secure Sockets Layer

SSP - Signaling Switching Points

STP - Signal Transfer Points

TCI - Tag Control Information

TCP - Transport Control Protocol

TDM - Time Division Multiplexing

ToS - Type of Service

UDP - User Datagram Protocol

UPS - Uninterruptible Power Supply

URL - Uniform Resource Locator

VAD - Voice Activity Detection

VLAN - Virtual Local Area Network

VoIP - Voice over Internet Protocol

VPN - Virtual Private Network

WAN - Wide Area Network

WAV - Waveform

Wi-Fi - Wireless Fidelity

ИТ - Информационни технологии

СВМО - Средното Време Между Отказите

СВР - Средно Време за Ремонт

УТЦ - Учрежденска Телефонна Централа