ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Телекоммуникациялық жүйелер
кафедрасы

«Қорғауға жіберілді»
Кафедра меңгерушісі
т.ғ.к. Шашахметов Д.Р.
(аты-жөні, ғылыми дәрежесі, атағы)
_____ «_____» _____ 20___ ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: „3A Engineering" ЖШС Asterisk негізінде корпоративті VoIP жүйесін жобалау
5В071900 - Радиотехника, электроника және телекоммуникация
мамандығы бойынша

Орындаған Нарманхан Шынар Нұржанқызы
(аты - жөні) (тобы)

Жетекші ТЖЖ кафедрасының аға оқытушысы Темірханов Д.О.
(аты-жөні, ғылыми дәрежесі, атағы)

Кеңесшілер :

Экономикалық бөлім бойынша : Э.Ғ.К. профессор В. Базылов
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «20» 05 2014 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
аға оқытушы Торраев Э.О.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «15» 05 2014 ж.
(қолы)

Есептеу техникасын қолдану бойынша :
аға оқытушы Сейсенова Д.О.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2014 ж.
(қолы)

Жетекші: ТЖЖ кафедрасының аға оқытушысы Темірханов Д.О.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «26» 05 2014 ж.
(қолы)

Мөлшер бақылаушы:
ТЖЖ кафедрасының аға оқытушысы Темірханова Э.К.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2014 ж.
(қолы)

Пікір жазушы :
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 20____ ж.
(қолы)

Алматы 2014

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Радиотехника, телекоммуникация және байланыс факультеті
Радиотехника, электроника және телекоммуникация мамандығы
Телекоммуникациялық жүйелер кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Нарманхан Шолпан Нұржанқызы
(аты - жөні)

Жоба тақырыбы „3A Engineering ТШС Asterisk негізінде корпоративті VoIP желісін жобалау
ректордың «24» қаркүйек № 115 бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «25» мамыр 2014 ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері)

1. А - күш түсірудің интенсивтілігі, Asterisk серверіндегі орта күш түсіру күніне 120 шақырудан түседі.
2. N - жұмыс уақытындағы кіріс және шығыс шақырулар саны
3. С - перекті арна арқылы байланыс жіберілу қолданылады

Диплом жобасындағы әзірленуі тиіс сұрақтар тізімі немесе диплом жобасының қысқаша мазмұны:

1. интенсивті түсетін күш пен қамтамасыз ету корпоративті VoIP желісі бойынша сапалы дыбыстық мәлімет арқылы
2. қауіпсіздіктің маршрутизациясы
3. VoIP желілеріне fDoS шабуылдарды зерттеу

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі

1. Корпоративті телефон желісінің жалпы сұлбасы
2. IBM System x 3250 сервері
3. E1 агрегатының платасы Орт VOxD110P
4. FXS шлюзі
5. ICMP Redirect жолбарышты тазартқыш
6. Redirect комегімен жаңарым бағдарлаушыны мәлметтер
7. VPN технологиясы

Негізгі ұсынылатын әдебиеттер

1. Мегглен Д., Мадсен Л., Смит Д. Asterisk будущее телефонии. Символ, 2009 – 656 б.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети – СПб.: Питер, 2002
3. Базанов Ж.Ф., Алибаева С.А., Бабич А.А. – Методические указания для экономической части выпускной работы – 2009г
4. Дюсебаев М.К. – Безопасность жизнедеятельности – Алматы, АИЭС, 2001 г.

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
Экономика	Базылев Ж	24.4 – 28.04.14	
СТҚ бөлімі	Гордеев Э.О.	02.05 – 15.05	
Жетекші: негізгі бөлім	Темирханов Д.О.	05.03.13 – 20.05.14	
Есептеу тех қолдану	Сейсенова Д.О.	12.05 – 19.05.14	

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Негізгі бөлім	18.10 - 20.11.13	
2	Нақты жағдайға талдау жасау	25.11 - 20.12.13	
3	Құрылғыға талдау жасау	24.02 - 10.03.14	
4.	Есептеу бөлімі	12.03.14 - 27.03.14	
5	Өндірістік қауіпсіздік	24.04 - 15.05.14	
6.	Технологиялық-экономикалық талдау	22.04 - 20.05.14	

Тапсырманың берілген уақыты «18» қазан 2013 ж.

Кафедра меңгерушісі _____ т.ғ.к. Шаншахметов Д.Р.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Жоба жетекшісі _____ аға оқытушы Темірханов Д.О.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Орындалатын тапсырманы қабылдаған студент _____ Нарманхан Шынар Нұрсаұқызы
(қолы) (аты -жөні)

Аңдатпа

Дипломдық жобамның тақырыбы корпоративтік VoIP желісін Asterisk базасында ТОО «3A ENGINEERING»фирмасында жобалау болып табылады. Жобада АТС IP-PBX, VoIP желілері мен интернет телефонияның даму тенденциялары қарастырылады.

Жобада каналдың таратылу мүмкіндіктерін есептеу, каналды пайдалану, пайдаланылатын жабдықтарға сипаттама беру қарастырылған. Қауіпсіздікті сақтау қарастырылған: жарықпен қамтамасыз етуге, бөлме желдетуіне мән берілген.

Жобаланып отырған VoIP желісін пайдалану арқылы фирма халықаралық телефон байланысына, кететін шығынды төмендетуге қол жеткізе алады.

Аннотация

В данной дипломной работе рассматриваются вопросы «Построения корпоративной VoIP сети в ТОО «3A ENGINEERING» на базе Asterisk». А также рассматривались вопросы описания VoIP сети, протоколы VoIP сети и выбор IP – АТС для построения сети.

В расчетной части был расчитан расчет канала связи.

В экономической части был определен срок окупаемости, а также и с учетом дисконта.

В безопасности жизнедеятельности рассмотрен анализ условия для данной фирмы при проектирования сети.

Abstract

In this this diploma work deals with building a corporate VoIP network company 3A ENGINEERING based on Asterisk. And also addressed describe VoIP network, VoIP protocols and network choice for IP–PBX networking.

As part of the settlement payment was targeted communication channel.

In the economic part of the payback period was determined, as well as taking into account the discount.

In life safety debated the analysis of the conditions for the firm in the network design.

МАЗМҰНЫ

КІРІСПЕ 7
1 НЕГІЗГІ БӨЛІМ 8
1.1 Нақты жағдайға талдау жасау 8
1.2 Жобаның міндеттері 9
1.3 VoIP желісінің сипаттамалары 9
1.4 VoIP желісінің хаттамалары 13
1.5 Желіге IP – АТС таңдау 20
1.6 Жабдық таңдау 23
2 ЕСЕПТЕУ БӨЛІМІ 39
2.1 Байланыс арнасының есебі 39
2.2 Қоңыраулардың маршрутизациясы 41
2.3 VoIP желілеріне FdoS шабуылдарын зерттеу 47
3 ЭКОНОМИКАЛЫҚ БӨЛІМІ 61
3.1 Техникалық – экономикалық негізделулер 61
3.2 Күрделі қаржы шығыны 61
3.3 Шартты кірістер 62
3.4 Бір жыл ішіндегі желіге қызмет ететін шығындар 63
4 ӨМІРТІРШІЛІК ҚАУІПСІЗДІГІ БӨЛІМІ 65
4.1 Байланыс желілеріндегі еңбек шарттарының талабы 65
4.2 Электр қауіпсіздігіне баға беру 67
4.3 Бөлме желдетуінің есептелуі 68
4.4 Шешімі 71
ҚОРЫТЫНДЫ 72
ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ 73
ҚОСЫМША 74

КІРІСПЕ

Интернет желілерінің қарқынды дамуы және оның жаппай сұранысқа ие болуы интернет хаттамалары мен IP серверлерді пайдалануда жаңа байланыс түрлерінің шығуына әсерін тигізуде. Бұл байланыс жүйелері әдетте пайдаланып жүрген дауыс дыбыстарын сандық форматқа алмастыруға мүмкіндік береді. Бұл байланыс жүйесі IP немесе VoIP телефониясы деп аталады. Аталмыш технологияның ерекшелігі халықаралық телефон байланыстарын тиімді, сапалы, әмбебап, ең негізгісі су арзан және қолжетімділігі болып табылады.

IP – телефония өз абоненттеріне әлемнің қай нүктесінен де жоғары, сапалы телефон байланысын қамтамасыз ете алады. Қазіргі кезеңдегі телефонмен сөйлесу (байланысу) көп жағдайда коммутатор станцияларының мүмкіндіктеріне сай кез келген уақытта сенімді, тиімді қызмет көрсете алмайды. Біз жоғарыда атап өткен желі тұрақты және сапалы байланыс түрлерін ұсына алады.

VoIP–дің басқа желілерден ерекшелігі (ЖҚТЖ немесе Public Switched Telephone Network, PSTN) – қалааралық, халықаралық телефон байланысының бағасының төмендігінде, арзандылығында. IP – телефония желісінде линиядаақаулар болмайды.

Корпоративті клиенттер жеке корпоративті телефон желісін құра алады, аймақтағы бөлімдермен байланысу арзанға түседі. VoIP – технологиясын пайдалану арқылы мекеме әр түрлі сервистерге қол жеткізе алады: 1) дауыс поштасы; 2) қоңыраулар тұрағы; 3) көпарналылиниялар (бағыттар).

IP – телефонияның тарифі қолданылып жүрген классикалық телефон байланыс жүйелерінен көп арзанға түседі. Жаһанды интернет жүйесі ресурстары қандай да ақпарат алмасуда форматын өзгертпейді. Бұл байланыс түрі өте ыңғайлы, сапалы, ең бастысы экономикалық жағынан тиімді.

Алайда, IP – телефонияға қондыру үшін арнайы жабдықтарды пайдалануды көздейді, ондай жабдықтар әлі кеңінен тарала қоймаған, қолжетімді болмаған. Дегенмен, жаңа технологиялар пайда болып, аппараттық құралдардың сапасы жоғарылап, оңтайландырылуда.

Бұл өз кезегінде бұқара халыққа сапалы қызмет көрсетудің басты көзі. IP АТС бұл күнде барлық Батыс мемлекеттерінде сұранысқа ие болып отыр, бірте – бірте біздің отандық нарықта да пайда болып, сұранысқа ие болуда.

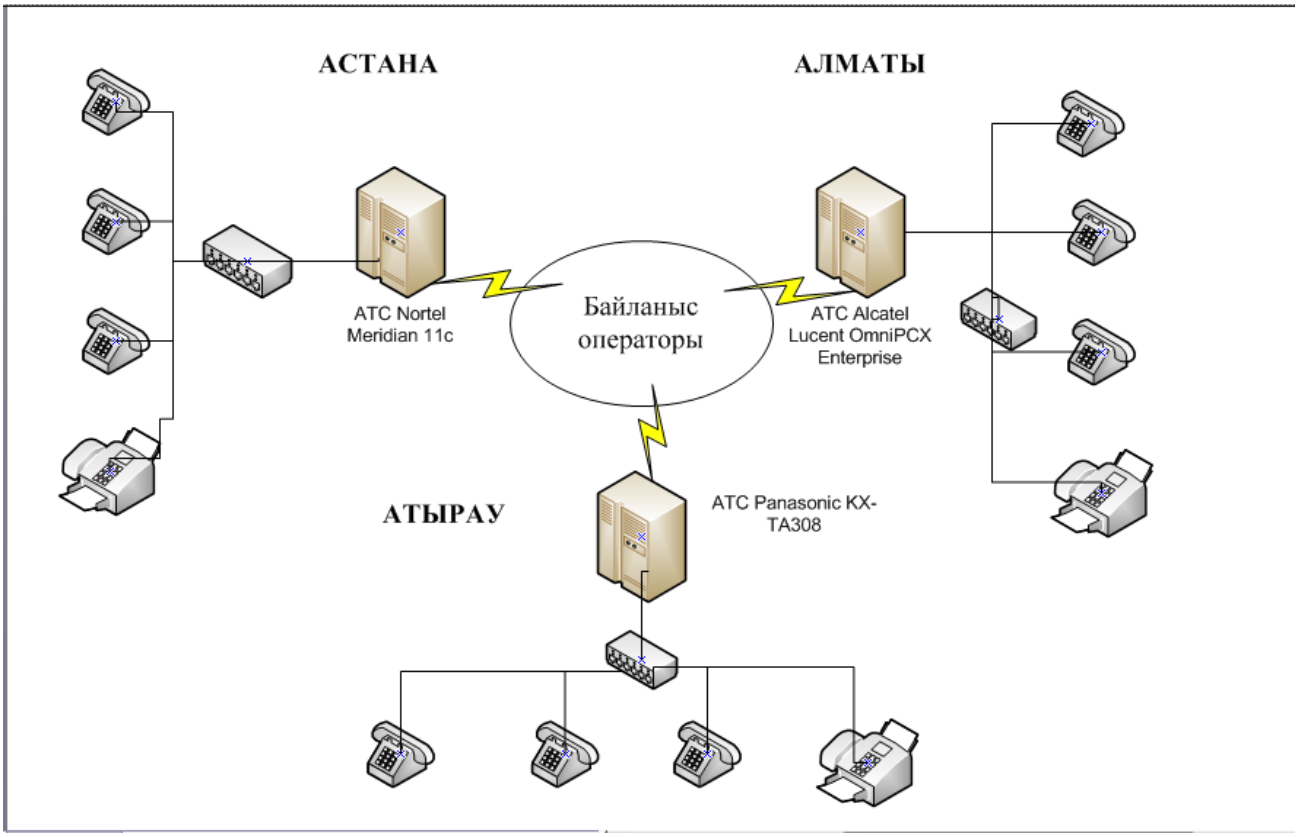
IP – телефонияның мүмкіндіктері шектеусіз. Бұл күрделі және жоғары-интеллектуалды технологияны жоғары кәсіби деңгейде орнатылуы қажет.

1 НЕГІЗГІ БӨЛІМ

1.1 Нақты жағдайға анализ жасау

Диплом жобасының нысаны ретінде ЖШС «3A ENGINEERING»фирмасы алынды. 3A ENGINEERING фирмасының негізінде жобалау, инжиниринг, құрылыстағы техникалық қолдау, құрылыс материалдарын таңдау және құрылғылар таңдау болып табылады. Фирманың артықшылығы болып сапалылық, тапқырлық, әдісқойлық, жобаның экологиясы мен экономикасы табылады. Қазіргі таңда фирма қарқынды даму кезеңінде тұр, тұтынушының күрделі сұрауларына кәсіптік жауапкершілікпен, эстетикалық шешімдерін және сұраулардың техникалық шешімдерін басқарудың эффективті тәсілдері арқылы табжылмай қызмет етеді. Фирманың негізгі бөлімі Алматы қаласында орналасқан, ал бөлімшелері Астана, Атырау қалаларында.

Фирмаға орнатылған корпоративті телефон желісінің жалпы сұлбасы 1.1 суретте көрсетілген.



1.1 Сурет–Корпоративті телефон желісінің жалпы сұлбасы

1.2 Жобаның міндеттері

Жобаның міндеті IP – PBX Asterisk базасында VoIP желісін жобаландыру ісін «3A ENGINEERING»фирмасында жүргізу.

Аталған VoIP желісі келесі функцияларды атқарады:

- фирманы бірыңғай корпоративті желіге шоғырландыру;
- фирманың қалааралық қоңыраулар жұмсалатын шығындарын азайту;
- видеоқоңыраулар;
- аудиоконференциялар;
-корпоративті VoIP желісі істен шыққан жағдайда байланыс операторлары арқылы балама маршруттарды қолдану.

1.3VoIP желісіне сипаттама

VoIP (ағыл. Voice over IP; IP – телефония) – байланыс жүйесі, негізгі қызметі тілдік дабылдарды Интернет желісі немесе басқа да IP – желілер арқылы жіберу, тасымалдау. Дабыл байланыс каналдары арқылы сандық түрде беріліп, жіберілер алдында өзгертіліп, артығы алынады.

Дауыстық және видеобайланыстың компьютерлер арқылы берілуі бүкіл әлемде XXI ғасырдың басынан танымал болып, тез арада сұранысқа ие болды. Қазірге кезде жеке тұтынушылармен қатар корпоративтік секторлар да бұл қызмет түрлеріне жүгінуде. IP телефония жүйесін пайдалану фирма операторларына қоңырау бағаларын (әсіресе, халықаралық қоңыраулар) мүмкіндік жасайды және телефонияны интернет сервисімен кірістіру арқылы интеллектуалды қызмет түрлерін көрсете алады.

VoIP технологиясы PSTN (Public Switched Telephone Network) ЖҚТЖжелісі арқылы күрделі, қымбат, қиындау қызмет түрлерін оңтайлы міндеттер мен шешімдер арқылы жүзеге асыруды көздейді.

Мысал келтіре кетсек:

- жоғары жылдамдықта телефонға қосылу арқылы бірнеше телефон қоңырауларын шалуға болады, ол VoIP технологиясының қолжетімділігін дәлелдейді және үйде, офисте еш қиындықсыз телефон линиясын қосуға мүмкіндік береді;
- VoIP технология желісінде қоңырау шалулар қауіпсіз (SRTP сияқты), себебі, дабылдар шифрленеді, ал дәстүрлі телефон линияларында қауіпсіздік сақтала бермейді;
- қандай қашықтықта болса да VoIP провайдеріне интернет – байланыс арқылы қосылуға болады. Мәселен, қоңырау шалу орталықтарының операторлары VoIP телефондар көмегімен кез келген офисте жұмыс істей алады, ең бастысы, тиімді, тұрақты және тез интернет-қосылу болуы қажет;
- басқалармен интернет арқылы байланыс операторлармен кірістіру арқылы: видеоқоңырау, хабарламалармен алмасу, аудиоконференциялар, мекен-жай кітабын басқару т.б. қызмет түрлері;

- қосымша қызмет түрлері: қоңырау маршрутын анықтау, GSM – роумингі IVR–ді енгізу.

IP – желіде адам дауысы импульсті – кодты модуляция көмегімен цифрленіп, кодталып дестелерге бөлінеді. Қабылдау жағында – мәліметтер пакеттерден алынып, қайтадан дауыс дабылына айналады.

Тілдік мәліметтерді кодтау 15–45 мс қосымша кешіктірулер туғызуы мүмкін, оның себептері:

- дабыл жинақтау үшін қолданылатын буфер (алгоритмикалық кешігу);
- математикалық өзгерістер (тілдік сигнал беру үшін процессорлық уақыт талап етеді).

Бұндай кідіріс сөзді басқа жақта декодтау кезінде пайда болады. Кодектің кідірісін «сквозной» кідірістерді санауда ескеру керек. Сонымен қатар, күрделі кодтау/декодтау алгоритмдері есептеуші жүйенің ресурстарына тиянақты шығындарды талап етеді.

Тілдік мәліметтерді интернет арқылы берудің сапасына зерттеу анализін жүргізу арқылы синтезделген тіл мәліметтерінің бұзылуы, сапасының төмендеуі көп жағдайға байланысты:

- пакеттердің байланыс желілеріне жіберілген кезде жоғалып кетуі;
- берілген уақытта пакеттердің жеткізілмеуі.

Мұндай жағдайларды болдырмау үшін тілдің алгоритмдік компрессиясын желіде оңтайландыру, сонда пакет жоғалғанда да, қайтадан дестені орнына келтіруге болады.

Мәліметтерді кодтау үшін кодектер пайдаланылады. Дауысты қысу алгоритмі IP – желі арқылы тасымалдау түрлері әр түрлі болып келеді. Кейбір кодектер дауысқа қысым түсірмей, оны импульстік – кодтық модуляция деңгейінде қалдырады (секундына 64 кбит). Басқа кодектер 8 немесе одан да көп рет кодтық алгоритмдерді пайдалана отырып дауыс ағынын қысады. Лицензия талап етпейтін жақсы, еркін кодектермен қатар сертификатталған, лицензиясы бар кодектер пайдаланылады.

Ашық:

- GSM
- G.711 μ-law
- G.711 a-Law
- G.722
- G.726
- Speex
- iLBC

Проприетарлық:

- G.729
- G.729A
- G.723

1.1К е с т е – VoIP–кодектердің салыстырмалы сипаттамалары

Кодек	Дестенің пайдалы жүгі, байт	Жіберілу жылдамдығы, кбит/с	Алгоритмикалық кідіріс, миллисекунд	Бос емес ағын, кбит/с	
				IP-дестелері	Ethernet-фреймдері
G.711	160	64	20	64.8	80
G.723.1(6.3)	24	6.3	37.5	6.9	17.1
G.723.1(5.3)	20	5.3	37.5	5.9	16
G.726-32	160	32	20	32.8	42.7
G.726-24	160	24	20	24.8	34.7
G.726-16	160	16	20	16.8	26.7
G.729(8)	20	8	25	8.8	18.7
G.729 (6.4)	16	6.4	25	7.2	17.1

Біздің жобамызда дауыс сигналдарын жақсы, сапалы беру, тасымалдау үшін мынадай кодектерді пайдаландық: G.711 және G.729.

G.711 – бұл ITU–T стандартты аудиокомпандирование үшін қолданылады. Негізінен, телефонияда қолданылады, алғаш рет 1972 жылы пайдаланылған.

G.711 – стандарты 8 битті компрессия PCM дауыс жиілігін 8000 кадр секундына және 8бит/кадр стандарты. Осыған орай, G.711 кодегі 64кбит/сек – НЦК (негізгі сандық канал) құрайды.

G.729 – таржолақты тілдік кодек таржолақты телефон тілін тиімді жеткізу үшін қолданылады. Оның сипаттамасы 300–3400Гц жиілігі 8кГц.

G.729 – кеңінен қолданылып жүрген кодек түрі, жылдамдығы 8кбит/сек. Теорияға сүйенетін болсақ, бір секунд ұзақтығы бар тілдік дабылды 60 байт/сек ағынымен толық сипаттауға болады, яғни, сандау, тарату, сандық түрде сақтау, қайтадан қалпына келтіру т.б.. Нөмірлеу және тарату идеясы сандық күйінде сақтау дабылдың өзі емес, оның параметрі (нөл арқылы өткізу саны, спектрлік сипаттамалар т.б.). Осы параметрлер арқылы дауысы трактінің моделін таңдауға болады. Синтездеу мүмкіндігі пайда болады, «вокодерлер» (Voice CODER) негізінде шығыс дабылдар жатады.

Кодектердің барлық түрлерінің есте сақтайтын ережесі сандық ағынның тығыздығы төмен болған сайын қайта қалпына келтірілген дыбыстық түпнұсқадан айырмашылығы болады. Дегенмен, қайта қалпына келтірілген гибридті кодектердің дабылдарының сипаттамалары жоғары көрсеткішке ие, себебі, тілдік дабылдың тембрі, оның динамикалық сипаттамалары қалпына келтіріледі. Яғни, дауысты тануға мүмкіндік болады. Бұл алгоритм кодтық модельдік линияныңбағыты алгебралық кодтық кітапқа сүйену арқылы жасалған (CELP – моделі). Кодер ұзындығы 10мс тілдік дабылдың дискреттелген жиілігі 8кГЦ–ке сүйенеді. Ол өз кезегінде 80–16 битті линиялық заңына бағынады. Әрбір кадр үшін дауыстық дабылдың анализі орындалады

және модельдің параметрлері ажыратылады (сызықтық болжамының фильтрінің коэффициенттері, индекстері және адаптивті және тіркелген кодтық кітаптардың күшейту коэффициенттері). Арықарай бұл параметрлер кодталып, арнаға жіберіледі.

Декодерде биттік жіберілу дабылдыңқозуы мен синтездеуші фильтрдің коэффициенттерінің қалпына келуі үшін қолданылады.

Синтездеуші фильтрде полюстік жіберуші 10 – дық реттік функциясы бар. Негізгі тондық синтезатор үшін адаптивті постфильтрация арқылы жақсарылады.

Кодер жіберетін биттік сәлемдемежоғалған кезде, сөздік синтезатор үшін жіберілген мәліметтер оның алдындағы мәліметтердің жақсы кадрларын интерполяциясы болады, бірақ интерполирлік сөздік дабыл ақырындап азаяды, ол тыңдаушыға ыңғайсыздықты тудырмайды.

Вокодер сөздік дабылдың кадрларын 10мс ұзындықта өңдейді. Қосымша 5мс ұзындыққа тең кідіріс те бар (look – ahead buffer), ол сомада алгоритмдік кідірісте 15мс («10+5») болып шығады. Сөздік дабылдың кідірістері осы алгоритмдегі қашықтық қосымшыларында уақытпен де анықтала алады:

-кодтау мен декодтау процесі;

-арна арқылы жіберілуі;

-аудио мәліметтерді басқа мәліметтермен мультиплекстеу кезінде;

IP – телефонияның негізгі ұтымдылығы – оның статистикалық сипаттамаларға талаптардың төмендігінде;

-кідірістерді тежеу (диалогтық, буындық және т.б.);

-сөздік дабылды ауқымдылығы мен сапасын қысу кезінде жоғалтпауы.

VoIP үшін дестелерді желіде тежеу – сын, себебі, бұл технология өзінің тұрақтылығымен ерекшеленеді. VoIP технологиясы телефон трафигін таратқанда, ISO 9000 сапа менеджмент стандарты талаптарын қатаң ұстану қажет:

-байланысты жылдам орнату сапасы;

-байланыстыру сапасы тұтынушының сұраныстарына жауап беруі тиіс.

Стандарт бойынша, кідіріс 250 миллисекундтан аспауы тиіс. IP желісіндегі кідірістер көп жағдайда дестелерді транспорттау ерекшеліктеріне байланысты болады. TCP хаттамасы дестелерді жеткізуді бақылайды, бірақ, бұл хаттама баяу жүретіндіктен дауысты таратуға қолданылмайды. Ал, UDP хаттамасы дестелерді тез жібереді, бірақ дестелер жоғалмауына кепілдік бермейді.

Кез келген VoIP қосылудың өзіндік параметрлері бар, сапалы бағалаудың нақты параметрлері бар. IP телефонияның көптеген операторлары қызмет көрсетуде қоңырау айырығын таңдағанда оның бағасы ғана емес, сапасына үлкен мән береді:

ASR/ABR – шалынған қоңыраулар пайызын шығарады.

ACD – хабарласу барысында тұрақты байланыс орнатуды көздейді.

Байланыс операторлары кей – кезде бағыттарды бағалауда статистикалық параметрлерге сүйенеді. Олар Эрланг нөмірді тергеннен кейінгі кідіріс (PDD), дестелерді жоғалту пайызы (QoS), қоңырау шалулардың максималды артуы секундпен санағанда (Calls per seconds, CPS).

1.4 VoIP желісінің хаттамалары

Хаттамалардың негізгі міндеті IP құрылғылардытіркеу (шлюз, терминал, қоңырауды абонентке жіберу, дауысты дабыл қою немесе видеобайланыс орнату, тарату, абонент нөмірін немесе атын көрсету). Қазіргі кезеңде сұранысқа ие VoIP хаттамалары:

-SIP – сеанстық байланыс орнату хаттамасы, бұл хаттама дауысты, видеоны, хабарламалармен алмасуды қамтамасыз етеді. 5060 UDP портын пайдаланады;

-H.323 – дәстүрлі телефония жүйесіне бағындырылған хаттама, SIP хаттамасына қарағанда. Порт сигнализациясы 1720 TCP және 1719 TCP гейткиперде терминалдарды тіркеу үшін қолданылады;

-IAX2 – 4569 UDP арқылы порт және сигнализация, медиатрафик;

-MGCP (Media Gateway Control Protocol) – медиашлюздерді басқару хаттамасы;

-Megaco/H.248 – медиашлюздерді басқару хаттамасы, MGCP–ны дамыту;

-SIGTRAN – PSTNсигнализация ОКС – 7 хаттамасын туннельдеу IP арқылы бағдарламалы коммутаторға (SoftSwitch);

- SCTP (Stream Control Transmission Protocol) IP-желілеріне дестелерді кепілді жеткізуді ұйымдастыру;

- SGCP;

- SCCP (Skinny Call Control Protocol) – жабық хаттама терминалдарды(IP-телефондар мен медиашлюздерді) Cisco компаниясы өнімдерінде басқару.

Unistim – жабық хаттама Nortel компаниясы өнімдерінің дабылды трафигін басқаруы.

1.4.1 SIP хаттамасы

SIP (ағыл. Session Initiation Protocol – сеансты өткізетін хаттама) тұтынушы интернет-сеансты өткізетін, аяқтайтын, оның мультимедиялық құрылымына (видео және аудиоконференция, жылдам хабарламалар, онлайн ойындар) кіреді. Ашық жүйелер моделінде SIP қолданбалы деңгейдегі желілік хаттама болып табылады. Хаттама тұтынушы тіркемелеріне жауап береді (мысалы, софтфон). Мұның мәні – тұтынушы осы желіде, бірақ алыс аймақтағы тұтынушымен байланысқа түсуді кідіріссіз жеңіл байланыстыру. Сонымен қатар, тұтынушылардың басқа хаттамаларды пайдалана отырып, мәліметтер жіберу үшін арналармен алмасуға да болады (мысалы, RTP). Сондай–ақ, қосымша арналарды қосуға немесе алып тастауға, қосымша тұтынушыларды

қосуға, алып тастауға болады (яғни, екіжақты конференцбайланыс өткізуге болады). Бұл хаттама сеанстың аяқталуын да қадағалайды.

Бұл хаттаманы әзірлеумен IETF MMUSIC Working Group ұйымы айналысты. Хенингом Шулзри (Henning Schulzrinne, Колумбиялық университет) және Марком Хэндли (Лондонның Университеттік колледжі) 1996 жылы қолға алып дайындады. H.323, SIP – хаттамаларымен қатар, Voice over IP негізін құрайды.

MMUSIC жұмыс тобы хаттаманың негізгі қағидаларын атап көрсетті:

- қарапайым, 6 әдіске (функциялар) сүйенеді;

- транспорттық деңгейге тәуелді емес UDP, TCP, ATM–дерді қолдана береді;

-тұтынушылардың жеке мобильдігі. Тұтынушылар желі ішінде кедергісіз қозғала береді. Себебі, тұтынушының өзіндік ерекшелігі бар идентификаторы бар. Қызмет көрсету жоғары деңгейде сақталады. Тұтынушы желі ішіндегі қозғалысын REGISTER хабарламасы арқылы жеткізіп отырады;

-желінің масштабтылығы. SIP хаттамасы желі құрылыс элементтерін кеңейтуге, ұлғайтуға мүмкіндік береді;

-хаттаманың кеңейтілу мүмкіндігі. Жаңа қызмет түрлерінен, жаңа функциялармен толықтырып алады;

-интернет хаттамаларымен кіріктірілуі. IETF комитеті әзірлеп шығарған SIP хаттамасы жаһанды мультимедиа архитектурасының бір бөлігі болып саналады. Бұл архитектураға SIP – тен басқа RSVP, RTP, RTSP, SDP хаттамалары кіреді.

-сигнализацияның басқа хаттамаларымен өзара әрекеттесуі. Интеллектуалды желілермен байланысқа түсу үшін IP – телефонияның басқа хаттамалармен және ЖҚТЖ хаттамаларымен бірге қолданылады.

SIP желісі элементтерін қосу үшін SIP тұтынушылары порт 5060 TCP және UDP пайдаланылады. Негізінен, SIPдауыстық және видеоқоңырауларды қосу, айыру үшін қолданылады. Сонымен қатар, басқа тіркемелерде де қоданылуы мүмкін. Мысалы, байланысты қосу, жүйені ақпараттандыру, мобильдік терминалдар т.б.. SIPхаттамаларына RFC нұсқаулары арқылы тіркемелерін реттеп отырады. Дауыстық және видеомәліметтерді тарату үшін транспорттық хаттамалар қолданылады. Жиі қолданылатыны Real – time Transport Protocol (RTP) хаттамасы.

SIP–тің негізгі міндеті IP базасының негізінде сигналды хаттама жасау, ол өз кезегінде шақыру мен қызмет түрлерін өңдеуде кең көлемдегі функциялар ЖҚТЖ арқылы ұсынады. SIP хаттамасы өздігінен бұл функцияларды анықтай алмайды. Қоңырау және сигнализация орнатуға бағытталған. SIP желінің функционалдық элементтері прокси – серверлер (Proxy Servers) және тұтынушы агенттері (User Agents) арқылы жобаланып, қолдауға ие болып отырады. Бұл элементтер базалық қызмет түрлерін ұсынады: нөмірді теру, телефон аппаратына қоңырау шалу, шалынған қоңыраудың дәрежесі жайлы абонентке дыбыстық мәлімет беру: SIP–тің негізінде телефон желілері заманауи қызмет

түрлерін көрсете алады, оны ОКС – 7 арқылы алу мүмкіндігі бар. ОКС – 7 күрделі, бір орталыққа бағындырылған интеллектуалдық желі болса да қарапайым, интеллектуалды емес, терминалдармен (дәстүрлі телефон аппараттары) қолдана береді.

SIP басқа да бірнеше хаттамалармен бірге байланыс сессиясының сигналдық бөлігіне пайдаланылады. SIPSDP үшін тасымалдаушы рөлін атқарады. Сессия барысында медиамәліметтерді жіберу парметрлерін сипаттайды. Мысалы, пайдаланылатын IP порттары мен кодектері. Әдетте, SIPсессиялары – ол RTP дестелерінің ағыны RTP дауыстық және видеомәліметтердің тасымалдаушысы рөлін атқарады.

IP – желілер тіркемелерімен өзара әрекеттесу үшін SIP электронды поштаға балама адресті пайдаланады, ол тұтынушылардың мобильдігін қамтамасыз етеді. Жұмыс станцияларының адрестері ретінде URL әмбебап ресурстар сілтемелері, яғни, SIP URL қолданылады:

- есімі@домен;
- есімі@хост;
- есімі@IP-адрес;
-телефонның №@шлюз.

SIP адрестің бас жағында (мәтінде) SIP сөзі қойылуы, SIP адрес екендігінің дәлелі ретінде, басқа адрестермен шатастырмас үшін (электрондық пошта адресі, mailto:-мен белгіленеді).

Адрес 2 бөлімнен тұрады. Бірінші бөлігі – тұтынушының аты доменде немесе жұмыс станциясында көрсетіледі. Бірінші бөлігінде абоненттің телефон нөмірі берілсе, екінші бөлігінде қандай да бір шлюз идентифитталады. Адрестің екінші бөлігінде желі доменінің аты, хост немесе IP-адрестікі беріледі.

Тұтынушылардың аттары алфавиттік – сандық идентификатор арқылы беріледі. IP – телефонияда цифрлік идентификаторлар (нөмірлер) қолданылады, бұлар классикалық телефон желілерін кеңейту және ауыстыру үшін қолданылады. Жергілікті байланыс нөмірлері, әдетте, 2–3–4 белгілік болып келеді.

Шлюзде берілетін телефон нөмірі және басқа да қолжетімді байланыс түрі жергілікті байланыс нөмірі, ұялы телефон немесе қалалық телефон нөмірі болуы мүмкін. Шлюздің адресі (IP – адресі немес доменнің аты) телефонға немесе клиент – бағдарламасына ендіріледі, тұтынушыға тек нөмірді теру ғана қалады.

SIP хаттамасы клиент – сервері архитектурада беріледі. Тұтынушы сұранысын сервер орындайды. Сервер сұранысты қабылдайды, оны өңдейді. Сұраныстың тиімді орындалуына өз жауабын береді, мәліметтер береді.

SIP желісінде қоңыраулар қызметі желінің элементтері арасында бөлінеді. Негізгі байланыс жүйесіне жауапты абоненттік терминал болып саналады. Басқа желі элементтері қоңыраулар маршруттарына жауап берумен қатар, қосалқы сервис қызметтерін атқарады.

Терминал. Клиент пен сервер жабдықтарда өзара әрекеттескеннен кейін тұтынушыларға тікелей қызмет көрсету басталады – ол тұтынушылық агенттік деп аталады – User Agent Client (UAC) – тұтынушының агенттік сервері деп аталады – User Agent Server (UAS). Егер құрылымда UAC және UAS бірге қондырылса, онда – ол тұтынушылық агент деп аталады – User Agent (UA). Жалпы алғанда SIP терминалдық жабдықтары деп атайды.

UAS сервері және UAC клиенті тұтынушымен тікелей әрекеттестікте болады. Басқа клиенттер мен SIP серверлері оны жасай алмайды.

Прокси – сервер (ағыл. proxy – өкіл) тұтынушының желідегі мүддесін жақтайды. Клиент сұраныстарын қабылдайды, өңдейді, іске асырады. Прокси – сервер клиенттік және серверлік бөлімдерден тұрады, сондықтан, сұраныстарды қабылдап, қоңырауларға жауап бере алады.

Прокси – сервердің 2 типі бар:

-жағдайды есте сақтау (stateful). Сервер барлық сұраныстарды есте сақтайды, транзакция аяқталғанша жоймайды;

-күйді сақтамайды (stateless). Бұл сервер сұраныстарды тек өңдеумен айналысады. Күрделі интеллектуалды қызмет атқармайды.

«Переадресация» сервері тұтынушының орналасқан жерін көрсету үшін қолданылады. Бұл сервер қажетті терминалдың немесе прокси-сервердің хабарлауымен шектеледі. Шектің тұрғылықты орнын анықтайтын сервермен жұмыс істейді.

Алайда, қосылу үшін тұтынушы «Переадресация» серверін қолданбауына болады, егер керекті тұтынушының адресін білген болса.

Тұтынушының тұратын жерін анықтайтын – сервер. Тұтынушы SIP желісінің ішінде үнемі қозғалыста болуы мүмкін, сондықтан, нақты уақыт кезеңінде оның қай жерден қоңырау шалғанын анықтауға болады. Бұл сервер адрестік-мәлімет беру қызметін атқарады, тұтынушының орнын анықтап, оның адресін ұзақ уақытқа дейін сақтайды. Егер тұтынушыға адрестік мәлімет қажет болса, ол тікелей орнын анықтау серверінен мәлімет ала алмайды. Бұл функцияны басқа SIP серверлер LDAP, RWHOIS немесе басқа хаттамалар көмегімен алуға болады.

1.2 К е с т е – SIP және H.323

Салыстыру параметрі	SIP	H.323
Қосымша қызметтер	Екі хаттамада да бірдей қамтамасыздандырылған қызмет жиынтығы	
Тұтынушының жеке мобильдігі	Мобильдікті сақтау үшін бар жақсы сүйеніштер	Жеке мобильдік қамтамасыздандырылған, бірақ аздау
Хаттаманың кеңейтілуі	Алдыңғы нұсқалармен жай қарапайым, ыңғайлы	қамтамасыздандырылаған, бірақ қиыншылықтар да бар
Желінің масштабтығы	Екі хаттама да желінің сапалы масштабтығын қамтамасыз етеді	
Байланыстың қосылу уақыты	Бір транзакция ғана жетеді	бірнеше транзакция қажет
Хаттаманың күрделілігі	Хаттың мәтіндік форматы, күрделі емес, сұранысы аз	Қиын, хаттама сұраулары көп, хаттың екі түрлілігі

SIP хаттамасы қондырғыларды сигнализациялау және тіркеу үшін сұраныстарды пайдаланады. SIP хаттамасының (RFC 3261) бастапқы нұсқасында сұраныстың 6 типі қарастырылған. Сұраныстар арқылы тұтынушы тұрғылықты жері туралы мәліметтер ала алады, тұтынушыларды байланыс сеанстарына шақырады, тұрақты сеанстарды модификациялайды, аяқтайды т.б.. Сұраныс түрлері старттық жолдарда көрсетіледі:

- INVITE – тұтынушыны байланыс сеансына шақырады.SDP – сеанс сипаттамасы бар.
- ACK – INVITE сұранысына жауап береді.
- BYE – байланыс сеансын анықтайды. Сеансқа қатысушылардың екі жағынан тарата береді.
- CANCEL – өңделген сұраныстарды қайтарады, кейбір сұраныстарды қарастырмайды.
- REGISTER – адрестік мәліметті орынды анықтайтын сервер тұтынушының регистрациясы үшін ауыстырылады.
- OPTIONS – терминалдың функционалдық мүмкіндіктерінің ақпаратын сұрастырады.

Бірақ, даму процесінде хаттамаға тағы бірнеше сұраныс типтері қосылды, олар оның функционалдығын толықтырды:

- PRACK – уақытша растама;
- SUBSCRIBE – оқиғаның жетуінің жазылуы;
- NOTIFY – оқиға туралы жазылушының хабарламасы;
- PUBLISH – INFO серверіндегі оқиғаның баспаға шығуы – сессияның жағдайын өзгертпейтін ақпараттың жіберілуі;
- REFER – SIP сұранысының жіберілуі туралы қаабылдаушының сұрауы;

- MESSAGE – SIP арқылы мезетте хаттардың жіберілуі;

-UPDATE—диалог жағдайының өзгеріссіз сессия қалпының модификацияланы.

1.4.2 H.323 хаттамасы

ITU – T телекоммуникациялық желілері арқылы аудио және видеоконференцияларды жіберу мақсатымен H.32x рекомендацияларының сериясын шығарды:

- H.320 – ISDN желілері арқылы;
- H.321 – Ш-ЦСИО және ATM арқылы;
- H.322 – пакет коммутациялары желілері арқылы кепілденген өткізу қабілетімен;
- H.323 – пакет коммутациялары желілері арқылы кепілденбеген өткізу қабілетімен;
- H.324 – жалпы қолданыстағы телефон желілерімен;
- H.324/C – мобильдік байланыс желілері арқылы.

Бұл серия өзіне видеоконференцияларды өткізудің қамтамасыздандыру стандарттарын енгізеді.

H.323 стандартына кіретін ITU – T кепілдемесінқолдану сапасына кепілдік бермейтін (QoS) бөлінетін ресурстық желідегі абоненттік терминалдардың кезегін анықтайды. H.323 стандарты IP хаттамасымен байланысты емес, бірақ, көптеген орындалулар осы хаттамаға негізделген. Кепілдеме жиынтығы пакеттік желіде мультимедиабайланысты ұйымдастыратын желілік компоненттерді, хаттамаларды және процедураларды анықтайды. H.323 стандарты төрт басты компонентті анықтайды, сонымен қатар, олар байланыс құрылымымен бірге екіжақты (нүкте – нүкте) және көпжақты (нүкте – көп нүкте) мультимедиа конференцияларды өткізе алады.

Терминал өзін ЖК немесе автономдық құрылғы ретінде ұстай алады, мультимедиалық қосымшаларды орындай алады. Ол байланыс жүйесі мен қосымша видео немесе мәлімет жіберуді қамтамасыз етуі шарт. Соған орай, терминалдың басты функциясы дыбыс жіберу болғандықтан, ол IP – телефония қызметінде маңызды рөл ойнайды. H.323 терминалы келесі хаттамаларды қамтуы тиіс:

- H.245 – байланыс параметрлерін келістіру үшін;
- Q.931 – байланысты қондыру мен контролі үшін;
- RAS – қақпашымен байланыс орнату үшін;
- RTP/RTCP – ағындық аудио (видео) жеткізу оптимизациясы үшін;

-H.450 хаттамасының отбасы үшін – H.323–ке міндетті қосымшалары үшін.

Қосымша компоненттерге басқа да аудио және видеокодектер кіруі мүмкін (H.261, H.263, MPEG).

Шлюз H.323 желісіндегі маңызды компоненттеріне кірмейді. Ол тек басқа стандартты терминалмен қосу кезінде ғана қолданылады. Бұл байланыс

хаттамалардың көрсетілуінің қосылуы мен байланысты ажыратудың қамтамасыз етеді, мәлімет жіберу форматын да қамтамасыз етеді. H.323 желілерінің шлюздері IP телефонияда IP желілері мен сандық пен аналогтық коммутацияланған телефон желілерінде кеңінен қолданыс тапқан.

Қақпашы(gatekeeper) өзінің зонасындағы шақыруларды өңдейтін орта болып шығады және шақырулардың маңызды функцияларын орындайды. Аймақ барлық терминалдардың біріктірілгені болып есептелінеді, шлюздердің және MCU ретінде берілген қақпашыныңбасшылығымен. Қақпашы – H.323 желісінің қажет емес компоненті болып табылады, бірақ, егер ол желіде болған жағдайда, терминалдар мен шлюздер оның қызметтерін пайдалануы қажет.

1.4.3 IAX2 хаттамасы

Хаттама Asterisk үшін альтернативті хаттама болып құрылған. Хаттаманың бірінші версиясы UDP 5036 портын қолданған. Берілген IAX хаттамасының түрі ескірді және кеңінен қолданылмады, сондықтан, IAX және IAX2 терминдері көбіне хаттаманың екінші түрін білдіреді. Өңдеушілер тобына: Марк Спенсер, Фрэнк Миллер, Кенни Шумард, Эд Гай және Брайан Капоч IETF–ке сұрау жіберді және 20-ақпан 2009 жылы хаттама RFC 5456 расталды.

IAX2 – Inter-Asterisk eXchange protocol – айырбас хаттамасы VoIP мәліметтерімен IP – PBX Asterisk аралығында. Көбіне NAT желілік адрестерін трансляциялауға бейімделген, SIP және H.323–ке қарағанда UDP хаттамасының бір 4569 портын сигнализация мен медиа ағынға ғана қолданады, сонда соңғылары осы мақсаттарға әр түрлі порттарды қолданады. Берілген хаттама SIP хаттамасымен салыстырғанда желілік трафикті үнемдеуге мүмкіндік береді, бұл дыбыстық мәліметті биттік өрісте мәтінсіз жіберілуімен түсіндіріледі.

Сонымен қатар, хаттама көптеген дыбыстық ағындарды біріктіре алады және бір ішкі транкке жібере алады, яғни, IP пакеттердің аттарын жіберумен байланысты шығындарды азайтады.

2 версиялы IAX хаттамасы Asterisk VOIP PBX-те IAX хаттамасында қолданыла алатын SIP, H.323 және т.б. хаттамаларының альтернативасы ретінде қолданылады. Қазіргі уақытта олардың саны аз, бірақ, тез өсіп келе жатыр.

Техникалық ерекшеліктері:

- толығымен бинарлыхаттама (SIP–ке қарағанда) – трафиктің үнемделуі;
- жалғыз ғана UDP – порт 4569 қолданылады, ол файрволдың конфигурациясын жеңілдетедіжәне NAT арқылы жұмысты жеңілдетеді;
-транкингті қолдана алады, сонда, әрбір пакетте мәліметтер бірден бірнеше параллельді каналдармен жіберіледі – трафиктің үнемделуі.

Артықшылықтары:

- SIP–ке қарағанда трафиктің талаптарына үнемді;
- NAT пен файрволдың конфигурациялары жеңіл;

-күтілмеген келеңсіздіктер аз (файрволдың барында, әлбетте, байланыс орнатылып, ал дыбыстық мәліметтер өткізіле алмайды, SIP–ке қарағанда);

- IAX2 эффекивті RTP (SIP) әрбір бір уақыттық байланыс саны үшін және кез келген кодекті қолданғанда да. Үнемділігі 2.4k–ден бастап, жалғыз шақыру үшін, trunk modeG.729 үшін қолданған кезде бір мезетте байланыстардың үш еселенуіне.

VoIP желісін құрастыру үшін дипломдық жобамызда тек SIP хаттамасы ғана қолданылатын болады, өйткені, ол құрау үшін жеңілдірек.

1.5 IP – АТС-ті желіні құрастыру үшін таңдау

IP – PBX (IP – АТС) қысқартылғанда PBX – Private Branch Exchange (УАТС) IP желіаралық хаттамасының негізіндегі телефондық станция.

Кәдімгі УАТС сияқты, IP – PBX басқа да функцияларды орындауға тиесілі. Өйткені, барлық функциялар программалық қамтамасыздандыру арқылы жасалғандықтан, IP PBX–те функционалды өсіру, оларды модернизациялау, қателерін түзету оңай. IP – PBX кәдімгі компьютердегі программа немесе мамандандырылған бағдарламалық – аппараттық комплекс, олар түрлендіруді қамтамасыз етеді және абоненттер арасындағы телефондық сөйлесулердің бөлінуін қамтамасыз етеді, кез келген IP – желі арқылы қосылған, сонымен қатар, локальді желі немесе ғаламтор арқылы.

Коммерциялық IP – PBX–пен қатар, шешімдері де бар, олар ашық кілті бар программалық қамтамасыздандыруға негізделген. Революциялық жаңалық болып табылатын БҚ–ға мысал ретінде PBX үшін Asterisk – Open Source болып табылады, Digium компаниясының проектісі. Коммерциялық шешімдері танымал вендорлармен ұсынылады: AddPac, Alcatel, Avaya, Cisco, Nortel, Panasonic және басқаларымен.

IP – PBX–тің негізгі функциялары:

Auto Attendant – автохатшы;

Call Blocking – қажетсіз шақыруларды құрсаулау;

Call Detail Records – CDR файл немесе мәлімет базасына жазуды жалғау;

Call Forwarding – өзге номерге автоматты түрде бағыттау;

Call Pick-up – шақыруды ұстап қалу;

CallQueuing – шақыруларды кезекпен қою;

CallTransfer – шақыруды аудару;

Call Waiting – егер линия бос болмаса,онда екінші шақыруға күту режимі;

Caller ID – нөмірді анықтау;

Conferencing – конференцбайланыс;

Conversation Recording – сөйлесуді жазу;

Interactive Voice Response (IVR) – интерактивті дауыстық мәзірдің жүйесі;

MusicOnHold – күту режиміндегі әуен;

ProtocolBridging–әр түрлі хаттамалардың арасындағы желілердің мәліметтерінең түрлендіруін жүзеге асыратын функция;

VoicemailSystem – дауыстық пошта.

IP – АТС–ке телефондық линиялардың қосылу түрлері:

-қалалық телефон –VoIP-шлюз арқылы FXO–портымен, яғнилиния саны порт санымен теңеседі;

- сандық ағынE1 (ISDNPRI) – сандықVoIP–шлюз немесеE1 портты плата арқылы;

- интернет желісі арқылы қалалық номер – IP – АТС тура қосылады;

- мобильдік оператордың GSM-номері – VoIP – GSM-шлюз арқылы немесе GSM – шлюз VoIP – шлюз арқылы;

- VoIP – CDMA – шлюз арқылы CDMA – нөмір;

-Skype жүйесінде шақыруды қабылдау – Skype – шлюз арқылы шақыру сіздің кез келген абоненттік IP – АТС–іңізге келіп түседі;

- сайтта шақыру – IP – АТС – тікелей түседі.

Сонымен қатар жоғарыда айтылған каналдардың барлығы сыртқы және ішкі байланысты қамтамасыз етеді, яғни телефондық байланысқа кеткен шығынды азайтады. Барлық телефондық шақырулар жүйеге қалай түскеніне байланыссыз IP – АТС–ке түседі, одан әрі түрленіп белгілі бір ережемен операторларға және абоненттерге таратылады.

1.5.1 Asterisk

Asterisk IP – PBX – Digium компаниясы атынан компьютерлік телефонияны ашық сыртқы кодымен жеңіл шешімін алғашында Марк Спенсер ойлап тапқан. Бұл қосымша Linux операциондық жүйесінде жұмыс істейді, FreeBSD және Solaris. Проекттің аты жұлдызша символына негізделіп шығарылған"*" (жұлдызша, астериск).

Asterisk классикалық АТС–тің барлық мүмкіндіктерін қамтамасыз етеді, көбіне VoIP протоколын қолдайды және шақыруларды басқаратын функциялары көп:

- дауыстық пошта;
- конференция;
- интерактивті дауыстық мәзір (IVR);
- шақыруларды өңдеу орталығы (шақыруларды ретке тұрғызу және тарату);
- жазу (CDR);

Қосымша функционалдықты қалыптастыру үшін Asterisk–тің өзінің тілін жоспарды нөмірлеу үшін қолдануға болады, модульді С тілінде жазып немесе AGI–ді қолданып ыңғайлы және жан – жақты интерфейсі ішкі жүйедегі мәліметтерді өңдеу интегрециясы үшін болады. AGI арқылы орындалатын модульдер программалаудың кез келген тілінде жазылуына болады.

Asterisk екілік лицензия шарттарына байланысты таралады, соның көмегімен негізгі кодпен бір уақытта GNU GPL ашық лицензияларымен таралатын жабық модульдердің шығарылуы мүмкін, оның ішіне лицензиялық код: мысалы, G.729 кодегін тірейтін модуль.

Asterisk лицензиясына орай белсенді дамып, дүние жүзіндегі мыңдаған адам қолдануда. Соңғы екі жылда Asterisk АҚШ–да белсенді дамып, IT – технологияда өзінің нық орнын тапқан (мыңнан аса компаниялар, қолдау орталықтары, online – консультациялар). Көптеген компаниялар Asterisk–ті өздерінің VoIP – құрылғыларында қолданады, мысалы, Linksys, Nateks компаниялары.

Asterisk аналогты линиялармен қатар (FXO/FXS модули), сандық линияларменде жұмыс істей алады (ISDN BRI және PRI – T1/E1 ағындары). Белгілі компьютерлік платалар көмегімен (белгілі шығарушылар қатарына Digium, Sangoma, OpenVox, Rhino, AudioCodes жатады) Asterisk–ті T1/E1 жоғары өткізгішті линияларғақосуға болады, олар ондаған және жүздеген телефондық байланыстармен параллель жұмыс істеуге мүмкіндік береді.

FXO/FXS модульдері – бұл порттардың аты, оларға аналогті телефон линияларыЖҚТЖ.

FXS интерфейсі – порт, абонентті аналогты телефон линиясынақосуға мүмкіндік береді. Басқа сөзбен айтқанда, «розетка в стене» станцияның сигналын береді, линияныңқоңырауға қажетті батареялық қорегін және кернеуін қамтамасыз етеді.

FXO интерфейсі – ажыратқыш, ішіне аналогты телефон линиясыкіреді.Бұлажыратқыш телефондықнемесе факсимильді аппараттанемесеажыратқыштары аналогтікіші – АТС–те болады. Бұндай порт тұтқа қойылды/тұтқа телефонда деген индекацияларды қамтиды. Порттар құрылғының бөлігі болғандықтан, мысалы, телефонның немесе факстің бұндай құрылғыны жиірек «FXO құрылғысы» немесе «аналогты құрылғы» деп атайды.

FXO шлюзі. Аналогты телефон линиясынIP кіші АТС – ке қосу үшінFXO шлюзіқажет. Бұл шлюздегі FXS портын FXO портына қосуға мүмкіндік береді, аналогты телефон линиясынVOIP шақыру дабылына түрлендіре алады.

FXS шлюзі бір немесе бірнеше дәстүрлі аналогты кіші – АТС–ті VOIP кіші – АТС немесе провайдерге қосылу үшін қолданылады. FXS шлюзі FXO портына қосылу үшін (көбіне телефон компанияларымен қосылады)ғаламтормен немесе VOIP кіші – АТС қажет.

Келесідей хаттамаларды қарастырады:

- SIP;
- H.323;
- IAX2;
- MGCP;
- Skinny/SCCP;
- XMPP (Google Talk);
- UNIStim;
- Skyрекоммерциялыққаналы арқылы.

Мәтін мен видеодабылды көрсетуге болады (мысалы, видеофонды қолдана отырып). Сонымен қатар, басқа да компьютерлік хаттамалармен жұмыс жасалған:

- DUNDi – хаттама, оны да Digium шығарған;
- OSP;
- T.38, факс жіберуге болады.

Құрылғылардың кеңінен таралу қолданысы және компьютерлік хаттамалардың қолданылуы көптеген желілердің бір – бірімен байланысын орнатып, хабарды алуға және өңдеуге мүмкіндік береді.

1.6 Құрылғыны таңдау

Толыққанды жұмыс үшін Asterisk–тен басқа келесідей құрылғылар қажет болады:
- сервер түріндегі аппараттық қамтамасыздандыру;
- E1ағынының платасы;
- FXS шлюздері.

1.6.1 Серверлер

Сервер (ағыл. server to serve дегеннен шыққан – қызмет көрсету) – аппараттық қамтамасыздандыру, сервистік ақпараттық қамтамасыздандыружекешеленгенжәне/немесемамандандырылған (соның ішінде осы немесе басқа есептеулердегі серверлер).

Сервер деп жеке компьютерлердегі топтан жекешеленген компьютер, адам көмегінсіз сервистік есептеулерді жүргізу үшін қолданылады. Сервер мен жұмыстық станция бірдей аппараттық конфигурацияны иемденуі мүмкін, олар тек адамның жұмысының консолью үшін қатысынан ғана ерекшеленеді.

Кейбір сервистік есептер жұмыс станциясында тұтынушы жұмысымен параллель жүргізіле алады. Бұндай жұмыс станциясын белгіленбеген сервер деп атайды.

Консоль (әдетте – монитор/пернетақта/тышқан) және адамның қатысы серверлерге тек біріншілік құрау үшін ғана, аппараттық – техникалық қызмет көрсетуде және штаттан тыс жағдайларда қажет (штатта көптеген серверлер өшіріліп басқарылады).

Стандартты шассиге орнатылатын (19 – дюймдік шкафтар) серверлер (және басқа да құрылғы), стандартты өлшемдерге келіп, керекті элементтермен қамтамасыз етіледі.

Жоғары өнімділік пен көптеген ішкі құрылғыларды қажет етпейтін серверлерді көлемдерін көбіне азайтады. Жиірек бұл кішірею ресурстардың азаюына әкеледі.

«Индустриялық орындау» дегенде азайған өлшемдерден басқа, корпустың үлкен мықтылығы бар, шаңнан қорғаныш бар (ауыспалы фильтрмен жабдықтарлған), ылғал мен дірілден сақтанған, сонымен қатар, кездейсоқ басып қалуды болдырмайтын батырмалар дизайны бар.

Конструктивті аппарат серверлерінің түрлері: стол үстінде, жерде, тұрып және қабырғада. Соңғы нұсқасы, бірлік ауданға саналатын қуаттың ең үлкен

тығыздықта орналасуын қамтамасыз етеді, сонымен қатар, максималды масштабтықты да қамтиды.

Ресурстар бойынша (жиілік пен процессорлар саны, есте сақтау саны, қатты дисктердің саны мен шығарылуы, желілік адаптерлердің шығарылуы), серверлер екі қарама-қарсы бағытта мамандандырылады-ресурстардың өсуі мен олардың азаюы.

Ресурстардың өсуі сыйымдылықтың өсуін мақсат етеді (мысалы, файл – сервер үшін мамандандырылу) және сервердің өнімділігі. Өнімділік қажетті шекке жеткен кезде келесі өсу басқа амалдармен жүзеге аса бастайды, мысалы, бірнеше серверлар арасындағы есептерді параллельдеумен.

Ресурстардың азаюы серверлердің өлшемінің азаюы мен энергия жұмсауын мақсат етеді.

Берілген жобамызда IBM System x3250 серверлерін қолдану ұсынылады, өйткені, берілген құрылғы өзінің техникалық және бағасының сипаттамасымен IP – PBX–ке келіп тұр.

1.2Сурет – IBM System x3250 сервері

Сипаттамасы:

-Шығарушы – IBM ;

- Модель – System x3250

Құрылғының негізгі сипаттамасы А қосымшасында келтірілген.

1.6.2 E1 ағынының платасы

E1 – бұл мәлімет жіберудің сандық каналы, ол PDH иерархиясының еуропалық бірінші деңгейлік стандартына сай. Американдық T1-ге қарағанда, E1 әрқайсысы дауыс немесе мәліметтер мен 2 канал сигнализация (30B+D+H) үшін 64 кбит/сек – тан тұратын 30 B каналға ие.

Біреуі соңғы құрылғыны синхрондауға арналған, яғни кодтық синхро сөзден және сигнализациялық биттен тұрады, ал екіншісі орнатылған қосылу туралы мәлімет жібереді. Жалпы өткізу қабілеті E1 = 2048 кбит/с (2 Мбит/с).

Интерфейстің негізгі қызметтік сипаттамасы:

- төменгі биттік жылдамдығы 2048 кбит/с;

- кодтау сұлбасы HDB3 (екі өрісті жоғарытығыздалған сұлба);

Қабылдағыш пен таратқыштың жеке линиясы:

- қабылдағыш пен таратқышқа бір бірден коаксиалды кабелі (кедергісі = 75 Ом)
- бір симметриялық өрілген жұптан қабылдағыш пен жіберуге (кедергі = 120 Ом)

OpenVox D110P платасы – бұл жоғары өнімді, үнемдіжәнеыңғайлы интерфейсі T1, E1 немесе J1. D110P – бұл универсалды PCI платасы, 3.3 және 5.0 вольт режимдерінде жұмыс істейді,T1біріншілік топтарының түрленуіне арналған (24 негізгі сандық канал), E1 (32 негізгі сандық канал) немесе J1 (24 негізгі сандық канал) TDM IP – PBX серверінің трактісіне.

Бұл плата бірнеше цифрлы арнаны қолдануы мүмкін. Сонымен қатар жалпы қолданыстағы телефондық желіге кіруге және бірнеше арнаны пайдаланып мәлімет жіберуге мүмкіндік береді. Бұл жағдайда, сервер IP – PBX Asterisk, D110P–мен жабдықталған, интеллектуалды маршрутизатор ретінде қолдануға болады.

1.3 Сурет – E1 ағынының платасы OpenVox D110P

Берілген E1 ағынының платасы Алматы қаласында Asterisk серверінде фирманың орталық офисінде корпоративтіVoIP желісінеқосылу үшін орнатылады. Өйткені, АТС Nortel Meridian 1 Option 11C қызмет көрсетуінде тұрған VoIP функциясын ұстай алмайды, ал берілген станцияның апгрейді Nortel Communication Sever 1000E деңгейі өте қымбат болып келетін процедура.

1.6.3 FXS шлюзі

FXS интерфейсі – бұл порт, абоненттің аналогты телефон желісіне қосылуға мүмкіндік береді. Басқа сөзбен айтқанда, «розетка в стене» станцияның дабылын береді, линия мен кернеуге батарейлік өнімділікті береді, қоңырау үшін қажет.

1.4Сурет – FXS шлюзі

FXS шлюзі бір немесе одан да көп дәстүрлі аналогты кіші АТС–тіVOIPкіші – АТС–ке немесе провайдерге қосу үшін қолданылады.FXS шлюзі FXO порттарын ғаламтормен немесе VOIP кіші – АТС–ке қосу үшін керек (әдетте телефон компанияларымен байланысады).

Берілген шлюздер Алматы қаласында аналогты телефондарды IP – PBX (Asterisk) қосқанда қажет болады. Өйткені, ескі АТС Panasonic KX – TA308–ті ауыстыру керек болды.

1.6.4 Қауіпсіздікті қамтамасыз ету

Интернет технологиясы жеке меншік мәліметтердің жарияланауына қатер туғызады, маңызды корпоративті қорлар мен мемлекеттік құпиялардың ашылуына қауіпті болуы мүмкін, ал хакерлік шабуылдар барған сайын жетілдірілген және қауіпті болып бара жатыр. Сондықтан, желілік қауіпсіздік сұрақтарына аса көңіл бөлу керек.

Күннен күнге хакерлер көптеген қорларға қауіп төндіруде, арнайы шабуылдар көмегімен мүмкіндік алып отыр. Оған негізгі екі фактор көмектесуде. Біріншіден, интернетке жаппай кіруі. Бүгінгі таңда интернет желісіне миллиондаған құрылғы қосылған. Көптеген миллиондаған құрылғылар болашақта тағы қосылуда. Сондықтан, хакерлердің осал құрылғыларға кіру мүмкіндігі үнемі артуда. Одан басқа, интернеттің кеңінен таралуы хакерлерге жаһандық көлемде ақпарат алмасуға мүмкіндік береді. Қарапайым іздеумен–ақ келесідей кілтті сөздермен мыңнан аса зиянды кодтар мен оларды пайдалану табылады: "хакер", "взлом", "hack", "crack" немесе "phreak".Екіншіден, бұл жалпы қолданыстағы жай, қолданылған операциялық жүйелер. Бұл фактор хакерлерге керекті білім мен тәжірибенің деңгейін азайтады. Бұған дейін хакер тек бағдарламалаудың деңгейін мықты білу керек болатын, ал қазір хакерлік ортаға енуі үшін керекті сайттың IP – адресін білуі ғана қажет, ал шабуыл жасауы үшін тышқанды басқаны болғаны.

Желінің қауіпсіздігі үшін, болуы мүмкін қатерді нақты елестету үшін немесе ақпаратты білу үшін төменде шабуылдардың типі көрсетіледі және оларды болдырмау түрлері айтылады.

Желілік шабуылдар оларға қарсы бағытталған жүйелер сияқты әр түрлі. Кейбір шабуылдар күрделілігімен ерекшеленеді. Басқаларын қарапайым тұтынушы да іске асыра алады. Шабуылдар түрлерін бағалау үшін кейбір шектерді білуі керек, яғни TCP/IP хаттамаларына сай. Интернет желісі мемлекеттік орындар мен университеттер арасындағы байланыс болып оқу процесіне және ғылыми зерттеулер үшін құрылған болатын. Берілген желіні құрушылар оның қаншалықты кең тарайтынын ойлаған жоқ. Нәтижесінде интернет хаттамалардың бастапқы түрлерінде (IP) қауіпсіздік талаптары болмаған. Сондықтан IP–дің көптеген жүзеге асырулары әлсіз болды. Көптеген жылдан кейін жарнамаларға ие болып (RFC – Request for Comments), IP үшін қауіпсіздік тәсілдері енгізіле бастады. Алайда IP хаттамасы үшін қауіпсіздік түрлері шығарылмағандықтан оның барлық мүмкіндіктері әр түрлі желілік процедуралармен, қызметтермен және өнімдермен толықтырыла бастады, яғни, бұл хаттамаға сай қатерлерді азайтты. IP желілеріне қарсы қолданылатын шабуылдар түрлері сипатталады және оларға қарсы тұру тәсілдері беріледі.

Желілік шабуылдар – бұл компьютерді кеңінен пайдаланатын кез келген адамға таныс сөз тіркесі. Оның астарында жеке деректерді, маңызды корпоративтік қорларға рұқсатсыз қатынас құру, мемлекеттік және басқа да құпияларды жария ету қаупі жатыр. Шабуылдарды ұйымдастырып, іске асыру күннен күнге дамып және оны іске асыру жеңілдеп келеді. Оның негізгі екі себебі бар: біріншісі, Интернет жүйесінің кең таралуы арқасында осал құрылғыларға қол жеткізу ықтималдығы арта түсіп, қасгөйлерге ауқымды масштабта өзара ақпарат алмасу мүмкіндігі туып отыр. Ақпараттық жүйеге шабуыл деп осы ақпарат жүйесінің олқылықтарын пайдалану арқылы қауіп-қатерлерді іске асыруға мүмкіндік беретін қасгөйлердің іс – әрекеттерін немесе өзара байланысқан іс – әрекеттер тізбегін айтады.

Шабуылды жүзеге асыру мынадай кезеңдерден тұрады: шабуылға дайындық, яғни шабуыл алдында ақпарат жинау (information gathering),шабуылды іске асыру (expolotation) және шабуылды аяқтау.

Шабуыл болғанын жасыруды білдірмеу үшін қаскөй мынадай іс – әрекеттерге баруы мүмкін:

- Шабуыл жасаушының мекен жайын басқамен ауыстыру;
- Жалған дестелер құру;
- Шабуыл жасаушы түйін ретінде басқа біреудің компьютерін көрсету;
- Шабуылдың стандарттық орындалуын өзгерту;
- Тіркеу журналдарын тазалау;
- Файлдарды жасыру;
- Шабуылды үзінділеу;

Шабуылдар жіктелімінің бірнеше түрлерін көрсететін болсақ**:**

- Қашықтан ену;

- Жергілікті ену;
- Қашықта тұрып қызмет көрсетуден бас тарқызу;
- Жергілікті қызмет көрсетуден бас тартқызу;
- Желілік сканнерлер;
- Осалдықтар сканері;
- Құпиясөз бұзғыштары;
- Хаттамалар талдаушы;

Man – in – the – Middle Attackшабуылы, одан қорғау.

Екі түйіннің (А және В) арасында тасымалданып жатқан деректерге жаңарту енгізу үшін қаскөй деректер тасымалдау арнасына өзін аралық (Х) түйін ретінде енгізуі қажет. Мұндай шабуылдар Man – in – the – Middle Attack деп аталады.

Деректерді жолай ұстау мынадай жағдайларда мүмкін болады:

А, В және Х түйіндері бір IP желіде орналасқан (бұл кезде жалған ARP – жауап шабуылы жүргізіледі);

А және Х түйіндері бір желіде, ал В түйін басқа желіде(бұл кезде жалған бағдарғылауышты міндеттеу шабуылдары жүргізіледі);

А және В түйіндері әр түрлі желілерде, ал Х түйін олардың аралығында орналасқан (бұл кезде шабуыл бағдарлау хаттамаларына жүргізіледі).

Man – in – the – Middle Attack шабуылы кезінде дестелердің сниффері, көліктік хаттамалар және бағдарғылау хаттамалары жиі қолданады. Бұл шабуыл ақпарат ұрлау, ағымдағы хабарды жолай ұстап қалу және жекеше желілік қорларға қатынас құру, трафикке талдау жасау және желі мен оның пайдаланушылары жайында ақпарат жинау, DoS тәрізді шабуылдар жүргізу, тасымалданатын деректерді бұрмалау мақсатымен жүргізіледі.

Man – in – the – Middle Attack тәрізді шабуылдармен тек криптографияны қолдану арқылы ғана нәтижелі күресуге болады. Тек техникалық жолмен жіберілетін деректі криптошифрлау арқылы қауіпсіздендіруге болады. Сонда қаскөй керекті дерек орнына түсініксіз символдар алады (оны супермашинаның өзі аша алмайтын). Егер қаскөйдің жолы болса, онда ол криптографиялық сессиясы жайында ақпарат жолай ұстайды, шифрланған дерек автоматты түрде мағынасын жоғалтады. Сондықтан осындай жағдайларда "алдыңғы өлкеде" күрес "технарьларда" емес, өндірістің кадрлық бөлімі және қауіпсіздік қызметі болуы керек.

Жалған ICMP Redirect хабары

Қаскөй бұл шабуылды өзінің Х түйіні орналасқан желідегі А түйіннен басқа бір желіде орналасқан (мысалы, В) түйінге бағытталған деректер ағынын жолай ұстау үшін пайдалануы мүмкін. Бұл кезде қаскөй Х мекен- жайын А түйіннің деректері жіберілуге тиісті бағдарғалауыштың мекен-жайы ретінде көрсетеді. Сөйтіп А түйінді, өзінің деректер ағынын Х түйінге (жалған бағдарлауышқа) жіберуге міндеттейді. Қаскөйдің түйінінде бұл деректерге талдау жасалынып, керек болса оларға өзгеріс енгізіледі және одан кейін әрі қарай нағыз бағдарлауышқа жіберілуі мүмкін.

Бұл шабуыл әдетте жалған ICMP Redirect хабары арқылы жүзеге асырылады.

8-bit Type	8-bit Code	16-bit Checksum
32-bit Gateway Internet Address		
Internet Header + 64 bits of Original Data Datagram		

1.5 Сурет – ICMP Redirect хабарының тақырыбы

Internet желісінде басқаратын ICMP (Internet Control Message Protocol) хаттамасы бар, оның бір функциясы желінің ішкі сегментінің түйінінде бағдарғылауыштың шалғайдан басқару кестесі болып табылады. Түйіннің бағдарғылауыш кестесі бес колонкадан тұрады: желілік мекен-жай (Network Destination), желілік қалқа(Netmask), бағдарғылауыштың мекен – жайы (Gateway), интерфейс (Interface) және метрик (Metric). Бағдарғылауышты шалғайдан басқару ICMP Redirect хабары түйінінде басқаратын бағдарғылауышпен жіберу түрінде нәтижеленген. Түйінде бағдарғылауышты өзгерту үшін ICMP Redirect хабарының тақырыбының екінші байты 1–ге тең болу керек. Мұнымен бағыттың (Destination) алмасуы үшін керек, түйіннің IP – мекен – жайын бағдарғылауыштың атынан жіберіп, түйіндегі бағдарғылауыштың рұқсат етілмеген өзгеруінің тұтастығымен және бағдарғылауыштың жаңа IP – мекен – жайын пайдалануға болады. Маңыздысы, бағдарғылауыштың жаңа IP – мекен – жайы шабуылдайтын түйін сияқты ішкі желіге жатуы керек болады.

Желінің сегментінде (шабуылдайтын түйіні бар) шабуылдаушыны тапқан кезде, шабуыл сұлбасы келесідей түрде болады:

Жалған ICMP Redirect хабары Datagrams for the Host шабуылдайтын түйінге жіберу.

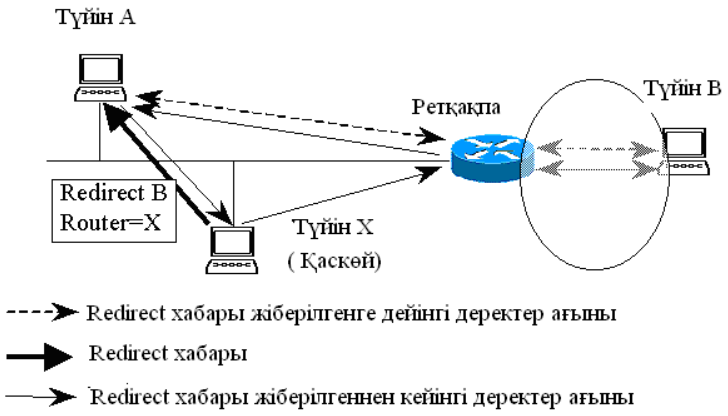
Егер шабуылдайтын түйіннен ARP – сұраныс келсе, онда ARP – жауап жіберіледі.

Егер шабуылдайтын түйіннен десте келсе, онда ол нақты(шын) бағдарғылауышқа қайта бағытталады.

Егер бағдарғылауыштан десте келсе, онда ол шабуылдайтын түйінге қайта бағытталады. Дестені қабылдау кезінде оның мазмұнына әрекет етеді.

ICMP (Internet Control Message Protocol) хаттамасының негізгі міндеттерінің бірі түйіндерге ағымдағы бағдарлауыштың күй – жайы туралы хабардар етіп тұру болып табылады. Бұл хабардың аты redirect (0 кодасы – қабылдаушы желісіне қайта бағыттау). Желі сегментіндегі кез келген түйіннен шабуыл жасалуға таңдап алынған түйінге жалған redirect – хабар жіберуге мүмкіндік бар. Қаскөй жалған ICMP Redirect хабарында өзінің немесе басқа кез келген IP мекен – жайды бағдарғылауыш ретінде көрсете алады. Ал RFC – 1122 құжатының талабы бойынша, кез келген түйін келіп түскен redirect-

хабарлардың бәрін міндетті түрде өңдеуге тиісті. Осының нәтижесінде түйін redirect – хабарын қабылдап алған соң өзінің ағымдағы бағдарғылау кестесіне өзгеріс енгізеді. Сөйтіп, осы түйіннің барлық деректер ағыны енді жалған redirect-хабарды жіберген түйін арқылы өтетін болды(1.10 Сурет).



1.10 Сурет – ICMP Redirect көмегімен жалған бағдарғылауышты міндеттеу.

А түйінінің бағдарғылар кестесінде жалған redirect-хабарын жіберетін түйін В түйініне баратын жолдағы бірінші бағдарғылауыш болуы тиісті және В түйіні А түйіні орналасқан желінің ішіне кірмеуі керек, ал жаңадан пайда болған жалған бағдарғылауыш Х, керісінше, А түйінімен бір IP – желіде болуы қажет.

А түйіні келген redirect – хабарды алдында В түйініне жіберілген дестеге жауап деп санайды. Осы хабардан А түйіні В түйініне жіберілетін дестелердің бағытын ауыстыру керектігін анықтайды да, өзінің бағдарлау кестесіне енді деректер тасымалдауды redirect – хабарда көрсетілген бағдарғылауыш арқылы жүзеге асыру жайында өзгеріс енгізеді.

Сонымен, А және В түйіндері арасындағы деректер ағынын ұстау мақсатымен жалған redirect-хабарын ұйымдастыру үшін қаскүнем А түйінімен бір IP – желіде болуы және А түйінінен В түйініне жіберілген дейтаграмма өтетін бағдарғылауыштың мекен – жайын білуі керек.

Егер желіде бір–ақ ретқақпа болса, онда ол осы керекті бағдарғылауыш болып табылады. Одан кейін қаскөй хабар жіберушінің мекен – жайы ретінде ретқақпаның IP мекен – жайы көрсетілген, ал А түйіні қабылдаушысы болып табылатын IP – десте қалыптастырады. Осы IP – дестенің ішіне redirect – хабары орналастырылады. Бұл redirect – хабарының жаңа бағдарғылауыш мекен-жайы алаңшасында қаскөйдің IP мекен – жайы көрсетіледі, ал одан кейін (А түйінінен В түйініне бұрын жіберілген сымақты) кез келген дестенің бастамасы орналасады. IP жекебөлшегі бұрын жіберілген дестелер туралы ақпаратты сақтамайтын болғандықтан, бұл жерде нақты дестенің бастамасын келтірудің қажеттігі жоқ. Осылайша қалыптастырылғн хабар қабылдаушыға (А түйініне) жіберіледі. А түйіні бұл хабарды ретқақпадан келген деп санайды да өзінің бағдарлау кестесін өзгертеді. В түйініне Х арқылы салынған жаңа

бағдарғы бірнеше минут бойы іске жарайтын болғандықтан, қаскөй оны сақтап тұру үшін мезгіл – мезгіл жалған redirect – хабарын жіберуді қайталап тұруы керек.

Айтып кететін тағы бір жайт – В түйінінің деректер ағыны бұрынғысынша тікелей А түйініне жіберіліп тұрады (яғни, жартылай жолай ұстау жүзеге асырылған). Себебі: ретқақпа мен А түйіні бір желіде орналасқан, сондықтан, дестелерді А түйініне жеткізу үшін ретқақпаға аралық түйіндерді пайдаланудың қажеттігі жоқ. Сондай–ақ қаскөй В түйініне арналып А түйінінен келген дестені әрі қарай В түйініне жібермей, В түйінінің орнына өзі жалған дестемен жауап қайтаруына да болады.

Кейбір жағдайларда жалған бағдарлауышты міндеттеу шабуылын, түйінді пішінүйлесімдіру кезінде, қаскүнем шабуыл жасалынатын түйінге (ICMP Router Advertisement хабары немесе DHCP хаттамасының жалған DHCPOFFER хабары көмегімен) өзінің IP мекен-жайын бағдарғылауыш ретінде көрсету арқылы жүзеге асыра алады.

Жалған ICMP Redirect хабарының алдын –алу, қорғау

Жалған ICMP Redirect хабары арқылы ұйымдастырылған шабуылды болдырмау үшін түйіндерде (RFC – 1122 құжатының талабына қарсы болса да) Redirect хабарын өңдеуге тыйым салу керек. Екінші жағынан қабылданып алынған жалған Redirect хабары бағдарғылау кестесінде кенеттен пайда болған қатар ретінде көрсетімделеді. Сондай – ақ, traceroute бағдарламасы В түйініне баратын жолда қосымша аралық түйін пайда болғанын көрсетеді. Сондықтан, егер пайдаланушы түйіннің бағдарғылау кестесіне назар аударса немесе traceroute бағдарламасын іске қосатын болса, онда қаскөйдің бұл шабуылы байқалып қалар еді.

Мұндай шабуылдан қорғанудың бір әдісі берілген хабарды сүзгілеу(Firewal–ды пайдалана немесе сүзгілейтін бағдарғылауыш), қажет немесе бұл хабарды игноризациялайтын сәйкес желілік ОЖ таңдау қажет. Жалғыз ғана әдіс (мысалға, Linux ОЖ немесе FreeBSD жағдайында) шыққан мәтінді өзгерту және ОЖ ядросын қайта компиляциялау қажет. Мұндай экзотикалық келіс шыққан мәтінмен бірге еркін таралатын ОЖ үшін ғана болуы мүмкін.

Тәжірибелер көрсеткендей, берілген хабар Windows 95 және Windows NT 4.0 ОЖ–де бағдарғылауышты өзгерте алады. Microsoft компаниясының өнімдері мүмкін болатын шабуылдардан ерекше қорғайтындығымен ерекшеленеді. Ізінше, IP – желінің қорғалған сегментінде ОЖ–ні мүмкіндігінше пайдаланбаған дұрыс. Бұл осындай шалғайдағы шабуылды қорғау бойынша әкімшілік шешім болады.

IP – спуфингі

IP – спуфинг – мекеменің ішінде бар болатын немесе одан тыс орналасқан хакер өзін рұқсатты пайдаланушы ретінде ұсынса болады. Мұны екі әдіспен жасауға болады. Біріншіден, хакер рұқсатты IP – мекенжайлардың диапазонының шегінде орналасқан IP – мекенжайды немесе нақты тораптық

ресурстарды қолдануға рұқсаты бар авторланған ішкі мекенжайды қолдануы мүмкін. IP – спуфингтің шабуылдары әдетте басқа шабуылдар үшін жіберілу нүктесі болып табылады. Классикалық мысал – DoS шабуылы, ол хакердің ақиқат тұлғасын жасыратын бөтен мекне – жайдан басталады.

Әдетте, IP – спуфинг клиенттік және серверлік қосымшалар арасында немесе біррангты құрылғылар арасындағы байланыс арнасы бойымен тасымалданатын кәдімгі деректер ағынына жалған ақпаратты немесе қастық командаларды ендірумен шектеледі. Екі жақты байланыс үшін хакер барлық бағдарғылау кестелерін өзгерту қажет, трафикті жалған IP – мекенжайға бағыттау үшін. Егер басты мақсат жүйеден маңызды файлды алу болып табылса, онда қосымшалардың жауаптары еш нәрсені білдірмейді. Егер хакер бағдарғылау кестелерін өзгерте алса және трафикті жалған IP – мекенжайға бағыттай алса, онда хакер барлық дестелерді алады және ол рұқсатты пайдаланушы ретінде оларға жауап қайтара алады.

Спуфингтің қаупін төмендетуге (бірақ жоюға емес) болады келесі шаралардың көмегімен:қолжетерлікті бақылау және RFC 2827 фильтрлеу.

Қолжетерлікті бақылау – IP – спуфингті тойтарудың ең қарапайым әдісі қолжетерлікті дұрыс бапталуында болып табылады. IP – спуфингтің тиімділігін төмендету үшін сіздің торабыңыздың ішінде орналасуы қажетті бастапқы адресі бар сыртқы тораптан келетін кез келген трафикті кесіп тастауға бағытталған қолжетерлікті басқаруды баптаңыз. Бұл тек ішкі мекенжайлар рұқсатты болған кезде ғана IP – спуфингтермен күресуге көмектеседі. Егер сыртқы тораптың кейбір мекенжайлары да рұқсатты болса, онда берілген әдіс тиімсіз болады.

RFC 2827 фильтрлеу – Сіз сіздің торабыңыздың пайдаланушыларымен бөтен тораптардың спуфингтік әрекеттерінің алдын ала аласыз (сөйтіп парасатты “тораптық азамат” бола аласыз). Ол үщін бастапқы мекен – жайы сіздің мкемеңіздің IP – мекенінің біреуі болып табылмайтын кез – келген шығатын трафикті брактап тұру қажет. “RFC 2827” атымен белгілі фильтрациялаудың бұл түрін сіздің провайдеріңіз (ISP) де атқара алады. Мысалыға, егер ISP IP – мекенмен 15.1.1.0/24 байланысты ұсынатын болса, онда ол фильтрді берілген интерфейстен ISP бағдарғылауышына тек 15.1.1.0/24 мекенінен түсетін трафик ғана өте алатындай қылып баптай алады. Барлық провайдерлер фильтрлеудің осы түрін ендірмегенше оның тиімділігі мүмкін мәнінен едәуір төмен боладтынын айта кету қажет. Фильтрлеу құрылғылары неғұрлым алыс болса, соғұрлым нақты фильтрлеуді өткізу қиынырақ болады. Осылайша, мысалыға, RFC 2827 фильтрлеуі бағдарғылауыш рұқсатының деңгейінде бастапқы тораптық мекеннен (10.0.0.0/8) бастап бүкіл трафиктің өтуін қажететеді, ал таралу деңгейінде болса (берілген сәулетте) трафикті нақтырақ шектеуге болады (мекен-жай – 10.1.5.0/24).

IP – спуфингпен күресудің ең тиімді әдісі, сниффинг дестелерінің жағдайындағыдай: шабуылды абсолютті тиімсіз ету қажет. IP – спуфинг аутентификация тек IP – мекендердің базасында жүргізілу шартында ғана

қызмет атқара алады. Сондықтан аутентификациялаудың қосымша әдістерін енгізу шабуылдың бұл түрін пайдасыз қылады. Қосымша аутентификациялаудың қосымша түрінің ең жақсысы криптографиялық болып табылады. Егер ол мүмкін емес болса, онда жақсы нәтижелерді бірретті кілт сөздерді қолданатын екіфакторлы аутентификациялау бере алады.

IP sequence number (IP – spoofing) болжау

Берілгенжағдайдақаскүнемніңмақсаты – басқажүйеболыпқылымсу, қайсына, мысалығажүйе–құрбан "сенеді".әдіссондай-ақбасқамақсаттардадақолданылады – мысалы, құрбанның SMTP жалғанхаттардытасымалдауүшінқолданылады.

TCP – байланысты орнату үш сатыда өтеді: клиент sequence number (оны C – SYN деп атайық) таңдайды және серверге жібереді, осыған жауап ретінде сервер сервер клиентке растауы (C – ACK) және өзінің серверлік sequence number (S – SYN) бар деректер дестесін жібереді. Енді клиент растауды (S – ACK) жіберуі керек. Осыдан кейін байланыс орнатылды деп саналады және деректермен алмасу басталады. Осы кезде әрбір дестенің тақырыбында sequence number және acknowledge number арналған өріс бар болады. Санның мәліметтері деректермен ауысу кезінде ұлғайып тұрады және тасымалдаудың дұрыстығын бақылап тұруға мүкіндік береді.

Қаскүнем сервермен жіберілетін sequence number–дің (сұлба бойынша S – SYN) қандай болатынын болжай алады деп санайық. Мұны TCP/IP – дің нақты орындалуын білу негізінде істеуге болады. Мысалы, 4.3BSD–дакелесі мәнді орнату кезінде қолданылатын sequence number мәні әр секунд сайын 125000–ға үлкейіп тұрады. Осылайша, серверге бір дестені жібере отырып, қаскүнем жауап алады да, келесі байланыс үшін sequence number–ді болжай (мүмкін, бірнеше әрекеттен және байланыс жылдамдығын түзету арқылы) алады. Егер TCP/IP іске асуы sequence number-ді анықтау үшін арнайы алгоритмді қолданатын болса, онда ол серверге бірнеше ондаған дестелерді жіберу арқылы және оның жауаптарын талдау арқылы анықталуы мүмкін.

Сонымен, B жүйесінің пайдаланушысы "rlogin A" істей алатындай және кілт сөзді енгізбей A-ның ішінде бола алатындай A жүйесі B жүйесіне сенеді деп санайық. Қаскүнем C жүйесінде орналасқан деп санайық. A жүйесі сервер ретінде, ал B және C – тұтынушылары болсын.

Қаскүнемнің бірінші мақсаты – B жүйесін тораптық сұрауларға жауап қайтара алмайтын күйге келтіру. Бұл бірнеше әдістермен істелінуі мүмкін, ең қарапайым жағдайда жай ғана B жүйесінің қайта жүктелуін күту қажет. Ол жұмысқа жарамсыз болған бірнеше минут аралығы жеткілікті. Осыдан соң қаскүнем A жүйесіне қолжеткізу үшін (қысқа уақытқа болса да) B жүйесі болып көре алады. Қаскүнем сервердің sequence number ағымдағы күйін анықтау үшін A жүйесіне байланысты инициалдайтын бірнеше IP – дестелерді жібереді. Қаскүнем кері мекен – жайда B жүйесінің иекені көрсетілген IP – дестелерді жібереді. A жүйесі B жүйесіне бағытталатын sequence number–ден дестеге жауап қайтарады. Алайда B жүйесі оны ешқашан алмайды (ол істен шығарылған), сол сияқты қаскүнем де. Бірақ ол алдындағы талдаудың негізінде

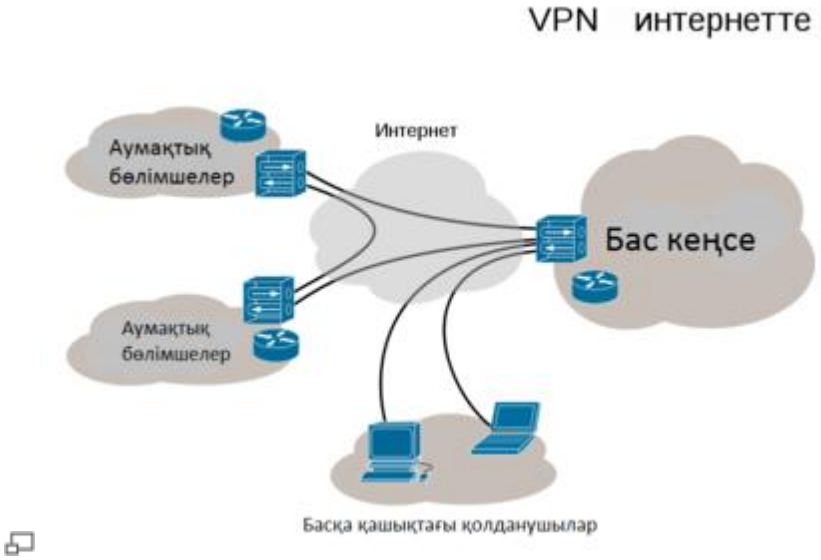
В жүйесіне қандай sequence number жіберілгенін болжай алады. Қаскүнем В атынан шамаланған S – ACK дестесін жібере отырып, А–дан дестені “алғандығын” растайды (егер жүйелер бір сегментте орналасқан болса, онда sequence number–ді анықтау үшін қаскүнемге А жүйесімен жіберілген дестені ұстап қалу жеткілікті болатынын белгілеп кету қажет). Осыдан соң, егер қаскүнемнің жолы болып және сервердің sequence number дұрыс табылған болса, онда байланыс орнатылған болып саналады. Енді қаскүнем кезекті жалған IP – дестені жібере алады, қайсында енді деректер бар болады. Мысалы, егер шабуыл rsh бағытталған болса, онда оның құрамында .rhosts файлды құру командасы немесе қаскүнемге электронды почта арқылы /etc/passwd жіберу бар болуы мүмкін.

Қарсы әрекеттер: IP – spoofing–тің қарапайым дабылы ретінде ішкі дүниеден келген ішкі мекендері бар дестелер болады. Бағдарлауыштың бағдарламалық қамтамасы ол туралы әкімшіні хабардар ете алады. Алайда азғыруға болмайды – шабуыл сіздің торабыңыздың ішінен де жүргізілуі мүмкін. Торапты басқару құралдарын парасаттау, пайдалану жағдайында әкімші қол жетпес күйде тұрған жүйелерден бастап дестелерді қадағалай алады (автоматты режимде). Алайда, қаскүнемге ICMP – дестеге жауап қайтару арқылы В жүйесінің жұмысын еліктеуге не кедергі болып тұр? IP – spoofing–тен қорғану үшін қандай әдістер бар? Біріншіден, sequence number–ді табуды қиындатуға немесе мүмкін емес етуге болады (шабуылдың кілттік элементі). Мысалы, серверде sequence number–дің өзгеру жылдамдығын өзгертуге болады немесе sequence number–дің өзгеру коэффициентін кездейсоқ таңдауға болады (кездейсоқ сандарды генерациялау үшін криптографиялық берік алгоритмді қолданған жақсы). Егер торап firewall–ды (немесе IP – дестелердің басқа бір фильтрін) қолданған болса, онда оған ережелерді қосу қажет, қайсылар бойынша сырттан келген және біздің мекен – жайлық кеңістігінен кері мекені бар барлық дестелерторaптың ішіне өтпеуі қажет. Одан басқа, машиналардың бір – біріне сенімділігін төмендету қажет. Машиналардың біреуіне суперпайдаланушы құқын ала отырып, тораптағы көршілес машинаға тікелей кіру әдістері болмау қажет. Әрине, бұл авторлауды қажет етпейтін сервистерді пайдаланудан сақтамайды, мысалы, IRC (қаскүнем Internet–тің ерікті машинасы ретінде қылымсына алады және ерікті хабарларды және т.б. жіберуші IRC арнасына кіру үшін командалар тізбегін жібере алады). TCP/IP хаттамасын шифрлау жалпы жағдайда IP – spoofing–тің мәселесін шешеді (криптографиялық берік алгоритмдер қолданылады деген шартта). Осындай шабуылдардың санын төмендету үшін, сондай–ақ біздің торабымызбен сыртқа жіберілген, бірақ біздің мекен – жайлық кеңістігімізге жатпайтын мекен – жайлары бар дестелерді фильтрлеу үшін firewall–ды баптауды ұсынады.

1.6.5 VPN

Виртуальды жеке желі(VPNағылш.*Virtual Private Network*) – жалпы қолданыста бар желі базасында құрылатын корпоративті желі(PSIN, ISDN)

және негізгі желіге ұқсас қызмет түрлерін (қоңырауды қайта адрестеу, мәтіндік пошта) көрсетеді. VPN–нің негізгі ерекшеліктері: мәліметтерді жоғары деңгейде қорғау және қысқартылған нөмір терудің көмегі арқылы оперативті қосылуды қамтамасыз ететін өзіндік нөмірлеу жобасы. Виртуалды жеке желі (VPN) – бірінші кезекте Интернет секілді желілерді қоғамдық коммуникациялық құрылымдарды алыс қашықтықта (әсіресе жеке географиялық құрылымдарды) байланыстыратын жеке желі.



1.11 Сурет – VPN технологиясы

Бұл желілер мәліметті шифрлеу сияқты тунельдік хаттамалар және қауіпсіздік шаралары арқылы жеке желілердің қауіпсіздігін қамтамасыз етеді. Мәселен, VPN бас кеңселердің бөлімшелерін желіге қосылу қауіпсіздігін қамтамасыз ету үшін де қолданылуы мүмкін. Сондай–ақ VPN әртекті бірақ бір типті, мысалы IPv6 желісін IPv4 желісі арқылы, байланыстыруы мүмкін.

Жалпы VPN–дердің екі түрі бар: қашықтан басқарылатын VPN және сайт – сайт VPN. Қашықтан басқарылатын VPN жеке қолданушыларға қашықтан басқарылатын желіге қосылуға мүмкіндік береді, мысалы өзінің компаниясының интражелісіне қосылу роумингі. Сайт – сайт VPN бірнеше қолданушының байланысуын қарастырады, мәселен, филиалдардың компания желісіне қосылуы. Виртуалды желілер, әрине, шығындарды азайтады, себебі, қауіпсіздікті күшейте отырып, қолданыстағы құрылымдарды пайдалана отырып, жалға алынатын желілерге деген сұранысты азайтады.

Ереже бойынша, VPN желідегі бөтен тұлғалар арасында жеке мәліметтердің жайылып кетпеуін қадағалау мақсатымен, қашықтан қолданушылардан тіркелу және шифрлеу әдістерін қолдануды талап етіледі.
Виртуалды жеке желілердің көмегімен қолданушылар, файлдар, принтерлер, мәліметтер базасы және желі ішіндегі қауіпсіз веб – сайттар сияқты қашықтықтан басқарылатын ресурстарды пайдалану сияқты желілердің көптеген фунцияларына қол жеткізе алады. VPN қашықтан қолданушылар

орталық желіге нүкте – нүкте сілтеме арқылы тікелей байланысқандығына таңданыстарын жасырмайды.

Виртуалды жеке желілер кадрларды қайта жіберу негізінде жеке желілерге негізделіп келді. IP – VPN-дер қаржылай шығындардың кемуі, өтімділік мүмкіндігінің өсуі және қауіпсіздікке қол сұғушылықтың төмендеуі есебінен тарап кетті. Бұл IP – VPN – дер ақырында кез келген желіден өз орнын табады, мейлі ол ұялыдан ұялыға, спутниктік, сайттан сайтқа немесе корпоративті жергілікті желі болсын.

Қызметтердіңпайдаланушылары:

Мемлекеттік құрылымдар

Қойылған мақсаттарға байланысты, мемлекеттік құрылым желісі барлық бөлімшелердегі ведомство иерархиясы бойынша мақсаттарды орындауды тура бақылауды қамтамасыз етуі тиіс. Қызметтік ақпараттың бөлігінде толық құпиялылықты қамтамасыз ету кезінде, ведомстволық Интернет пайдаланушыларының кең тобы бар интерактивті байланысты ұйымдастыру, басқа мемлекеттік құрылымдармен тез арада өзара әрекет ету мүмкіндігі болуы тиіс. IP VPN–нің көмегімен ведомстволық мемлекеттік желілер бүкіл елдегі құрылымдық бөлімшелерді біріктіре, Интернетке қорғалған шығуды, басқа желілермен байланысты қамтамасыз ете алады.

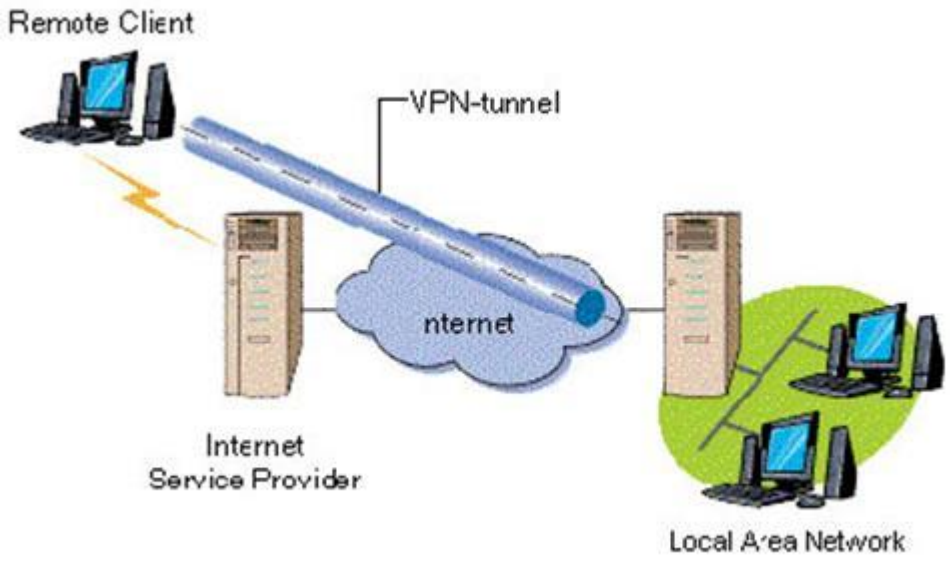
Коммерциялық компаниялар

Виртуалды жеке желі географиялық – тармақтанған құрылымы бар кәсіпорында басқару жүйесін құру мүмкіндігін береді. Кеңселердің өзара алыстығы және аумақтық бөлімшелердің байланысынан тыс, IP VPN олардың толық қисындылығын, жұмысын және кез келген бизнес-қосымшалардың өзара әрекет етуін қамтамасыз етеді.

IP VPN–нің құндылығы

MPLS технологиясының мүмкіншіліктері IP VPN желісіне икемді және көпфункциялық болу мүмкіндігін береді. Виртуалды жеке желіде едәуір шығындарсыз (жалға берумен, әсіресе арналардың аралық қабатымен салыстырғанда) кез келген топология – «жұлдыздан» «әрбірі әрбіріне» дейін жүзеге асырылады. Желіде IP – хаттамасы – яғни, қолданыстағы қосымшалардың басым көпшілігіне қолдау көрсететін кез келген жүйелер жұмыс істейді. Бұл ретте, IP VPN–нің ашық желілерден айырмашылығы байланыс сапасының параметрлеріне кепіл беріледі (Quality of Service). IP VPN ашық желілерден қисынды алыстатылған, яғни клиенттің трафигі сырттан рұқсатсыз кіруден толық қорғалған. IP VPN негізіндегі корпоративтік желісінде қызмет көрсету класы бойынша бөлінген шоғырланған әр түрлі деректер түрлерін беру мүмкін. Пайдаланушы сол немесе басқа бизнес – қосымшаның трафик басымдығын өз бетімен орната және реттей алады. Виртуалды жеке желіде сапалы IP – телефония мен бейнеконференция байланысын ұйымдастыру мүмкіндігі бар, ол корпоративтік желі аясында телефон қоңырауларының құнын едәуір төмендетеді және шешімдерді қабылдау шапшаңдығын арттырады. Берілетін ақпарат көлемінің өсуімен клиенттің

техникалық шешімі өзгермейді: желі гигабиттік жылдамдықтарға дейін оңай ауқымдайды.



1.12 Сурет VPN технологиясы

1.6.6 Желіаралық экран (Firewall)

Желіаралық экран – брандмауэрнемесеfirewallжүйесі деп аталатын арнайыланған желіаралық қорғаныс комплексі. Желіаралық экран ортақ желіні екіге бөлуге және ортақ желінің бір облысынан екінші облысының шекарасынан берілгендер пакетінің өту шаттарын анықтайтын ережелер жиынтығын іске асыруға мүмкіндік береді. Мұндай шекаралар мекеменің жергілікті желісі және Internet ауқымды желісі арасында жүргізіледі.

Әдетте желіаралық экран Internet ауқымды желісінен мекеменің ішкі желісін бұзып кіруден қорғайды, мекеменің жергілікті желісіне қосылған корпоративті интражелідегі шабуылдан қорғау үшін де қолданыла береді. Желіаралық экран технологиясы корпоративті желілерді сыртқы кауіп қатерден қорғайтын ең алғашқы технологиялардың бірі.

Көптеген мекемелерде желіаралық экран – орнату ішкі желіні қорғаудың ең қажетті шарты болып табылады.

Санкцияланбаған желіаралық бұзуға қарсы тұру үшін желіаралық экран ішкі болып табылатын мекеменің қорғалатын желісі және сыртқы қарсылас желінің арасында орналасуы керек . Соған қарамастан осы желілер арасындағы қарым қатынастар желіаралық экран арқылы жүзеге асырылуы тиіс. Желіаралық экран жалпы қорғалатын желі құрамына кіреді.

Бірнеше түйіндерді бірден шешетін желіаралық экран, мыналарды жүзеге асырады:

Корпоративті желінің ішкі ресурстарына сыртқы қолданушылардың кіруін шектеу жұмысы (қорғалатын желіге байланысты). Мұндай пайдаланушыларға серіктестер, жойылған қолданушылар, хакерлер және де сол мекеменің желіаралық экран қорғайтын берілгендер қорын алғысы келетін жұмысшыларын жатқызуға болады.

Сыртқы ресурстарға қорғалатын желінің қолданушыларының кіруін шектемеу мәселесі. Бұл мәселені шешу, мысалы қызмет бабының орындалуын қажет етпейтін серверлерге кіруді қадағалауға мүмкіндік береді.

2 ЕСЕПТЕУ БӨЛІМІ

2.1 Байланыс арнасының есебі

Есептеу бөлімінің негізгі есебі болып интенсивті түсетін күш пен каналдың ені корпоративті VoIP желісі бойынша сапалы дыбыстық мәліметті орындау болып табылады. Жалпы корпоративті желі 100 абоненттен тұрады.

Астана

Серверге түсетін күштің интенсивтілігін есептеу үшін, кестедегі бір ай үшін алынған статистикалық мәліметтер қажет болады (К е с т е 2.1):

2.1 К е с т е - Жұмыс уақытында алынған орташа шақырулар санының статистикасы:

Шақыру уақыты	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00
1сағ ішіндегі қоңырау лар саны	4	7	11	19	19	22	16	13	7	4

Қорытындысында Asterisk серверіндегі орта күш түсіру күніне 120 шақырудан түседі.

Күш түсірудің интенсивтілігін санау үшін келесі формуланы пайдаланамыз:

$$A = \lambda \times T \tag{2.1}$$

Т – кездейсоқ шама, бір шақырудың орташасының уақыт бірліктерінде өлшенетін ұзақтығы.

Λ – шақырудың түсу орташасының шақырусанының уақыттың бірлігіне өлшенетін жиілігі, шақыру/сағ. Шақырудың кездейсоқ ағынының ортақ мінездемесі.

Жүктеменің сипаттамасы –λ шақыруларының түсуінің орташа жиілігі, А трафигі – әдетте, сағаттық интервал үшін бағалайды, байланыс жүйесінің көп жүктемесі кезіндегі периоды болып табылады.

2.1 – кестеден шақырулардың бір сағат ішіндегі орташа санын есептейміз:

$$\lambda = \frac{N}{t_{жум}} \tag{2.2}$$

N– жұмыс уақытындағы кіріс және шығыс шақырулар саны, $t_{жұм}$ – шақырудың бір сағаты.

$$\lambda = \frac{120}{10} = 12$$, шақыру/сағ

Бір шақырудың орташа ұзақтығы (Т) келесі формуламен есептелінеді:

$$T = t_{жр} + t_{сж} + n + t_{қос} + t_{шж/шжк} + t_{сөйл} + t_{бос} \quad (2.3)$$

- $t_{жр}$ = 0,1 с – коммутация жүйелерінің реакция уақыты, абонент арқылы хаттама ретінде «орын алу» сигналының станцияға «станция жауабы» дабылын алған кезіндегі уақыты;
- $t_{сж}$ = 3 с – «станция жауабы» дабылын тыңдауының орта уақыты;
- n – абоненттік нөмірдегі мәндерінің саны, бір символдың сарындық жиынтығы 0,5с құрайды.Астанадан Алматының қалалық нөміріне шақырылуы, терілетін 8727XXXXXXX – 11 символ, 0,5 *11=5,5с ;
- $t_{қос}$ = 2 с – байланыс орнауының орташа уақыты;
- $t_{шж/шжк}$= 7 – 8 с – «шақыруды жіберу» дабылдарын таратудың орташа уақыты және «шақыруды жіберудің тексерілуі»;
- $t_{бос}$ = 1с – телефондық тракттің босауының байланыс үшін орташа уақыты;
- $t_{сөйл}$ – сөйлесудің орташа ұзақтығы.

Статистикалық мәліметтерге сүйенетін болсақ, сөйлесудің орташа ұзақтығы 194 секунд. Алатынымыз:

$$T = 0{,}1 + 3 + 5{,}5 + 2 + 8 + 194 + 1 = 213{,}6c$$

Секундты сағатқа айналдырамыз, 213,6сек= 0,06 сағат.Енді берілгендерді 2.1 – формулаға қоямыз:

$$A = 12 \times 0{,}06 = 0{,}71$$ Эрланг

Мәлімет жіберудің жылдамдығы оның шығарылуына тікелей байланысты, яғни, кодтау мен декодтауға. Берілген арнадағы ең көп мәлімет жіберілуі оның өткізгіштік қабілеті деп аталады. Арнаның өткізу қабілеті берілген арна үшін ең жақсы деген көздерін тауып қолдануы кезіндегі мәлімет жіберу болып табылады, кодер мен декодер үшін, сондықтан ол тек арнаны сипаттайды.

Шақыруларды жіберу ортасы болып интернет табылатындықтан, немесе кез келген IP желісі болғандықтан, желі арқылы сапалы дауыс жіберу үшін каналдың жылдамдығын санау қажет. Санау үшін келесі негізгілерді білу

қажет: қолданылатын кодектің сипаттамалары мен бір сағат ішіндегі шақырулардың орта саны. Керекті арна арқылы байланыс жіберілу жылдамдығын есептейік:

$$C = \lambda \times R \tag{2.4}$$

мұндағы,R – кодектің жіберілу жылдамдығы, кбит/с.

Регламент бойынша G.729 кодегі көмегімен пайдалы мәліметті кодтау 8 кбит/с–ті құрайды, шын мәнінде пайдалы ақпараттан басқа, қызметтік ақпарат кодталады, кодектің жіберу жылдамдығы 16 – 20 кбит/с–ті құрайды.

$C = 12 \times 20 = 240$ кбит/с

Есептеу жүргізу барысында анықталғандай, байланыс арнасы арқылы шақырулардың орташа саны сағатына 240 кбит/с жылдамдықпен таралуы керек. Бұл жылдамдық Астана қаласының серверлеры үшін 256 кбит/с–ты құрайды.

2.2 Қоңыраулардың маршрутизациясы

Маршрутизатор (англ. Routing) – байланыс желісіндегі ақпараттың маршрутын анықтау.

Маршруттар әкімшілікті қойылуы мүмкін (статистикалық маршрут), немесе маршрутизация алгоритмі көмегімен есептеледі, желі жағдайы және топологиясы туралы ақпаратқа негізделген, маршрутизация хаттамасының көмегімен алынған (динамикалық маршрут).

Статистикалық маршруттар былай бөлінеді:

- уақыт бойынша өзгермейтін маршрут;
- кесте бойынша өзгеретін маршрут;
- жағдай бойынша өзгеретін маршрут – қалыпты жағдайда пайда болады.

Маршрутизация хаттамасы тек дестелермен жұмыс жасауы мүмкін, мысалы, IP, IPX немесе Xerox Network System, AppleTalk. Маршрутталған хаттамалар дестенің пішімін, маңызды ақпаратты анықтайды. Маршрутизацияны қолдамайтын хаттамалар желілер арасында туннельдің көмегімен жіберілуі мүмкін.Бұндай мүмкіндіктерді, әдетте, бағдарламалық маршрутизаторлар және кейбір аппараттық маршрутизаторлар береді.

Алғашқы маршрутизаторлар өзіне негізделген БҚ (бағдарламалық қамтамасыздандыру) ұсынды, өңделетін кіріс IP – дестесітүрінде. Бұл БҚ компьютерде жұмыс жасады, кейбірлерінде бірнеше желілік интерфейстер болған, шығыс құрамы әртүрлі желілерден (олардың арасында маршрутизация орындалады). Одан кейін мамандандырылған құрылғы түріндегі маршрутизаторлар пайда болды. Маршрутизацияланған БҚ компьютерлерді – бағдарламалық маршрутизаторлар, жабдықты – аппараттық маршрутизатор деп атайды.

Қазіргі аппараттық маршрутизаторларда, маршрутизация кестесін құруға мамандандырылған БҚ, ал IP – дестені өңдеуге коммутациялық матрица қолданылады (немесе аппараттық коммутацияның басқа түрі).

Маршрутизацияның екі түрі болады: аппараттық және бағдарламалық маршрутизация.

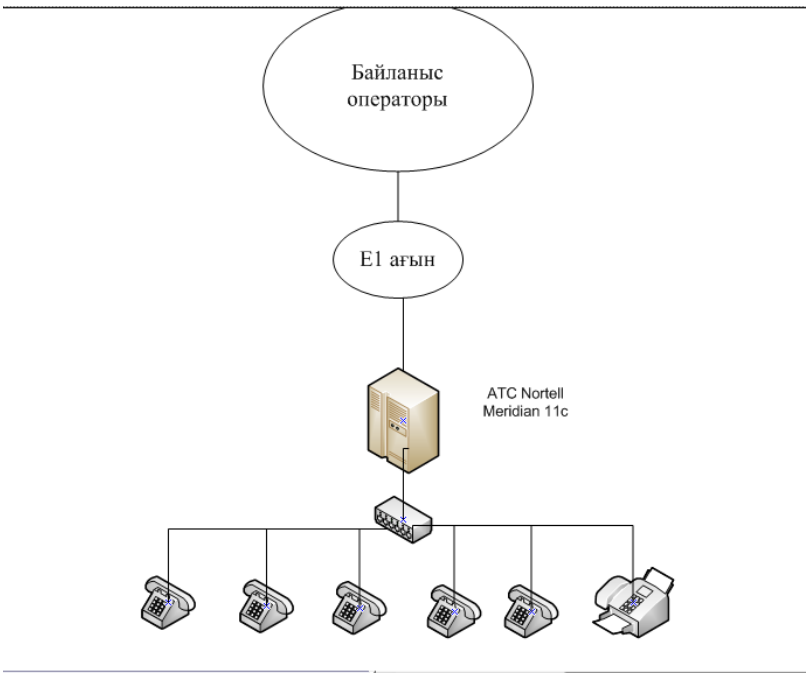
Аппараттық маршрутизация екі түрге бөлінген: ағындардың статистикалық үлгілері және динамикалық бейімделген кестелері.

Ағындардың статистикалық үлгілері IP – дестелердің кіріс маршрутизаторларына кіретін виртуалды ағындарына бөлінген; әрбір ағын пакеттер үшін келесідей сипатталады: жіберуші/қабылдаушының IP – адрестері; жіберуші/қабылдаушы TCP/UDP – порттары (4 деңгейлі ақпарат негізінде маршрутизацияны қолдау), порт арқылы келген десте. Маршрутизацияның оптимизациясы келесідей ойда тұрғызылады: барлық дестелер бірдей белгілерімен бірдей өңделу керек(бірдей ережелермен), олар ағындағы тек бірінші десте үшін ғана тексеріледі(белгілері бар десте шыққанда, жаңа ағын құрылады), осы дестеге жасалған анализдің нәтижесінде статистикалық үлгі құрылады, ол келіп түскен десте коммутациясының ережелерін анықтайды (ағын ішіндегі). Әдетте қолданылмаған үлгілердің сақталу мерзімі шектеулі болады. Динамикалық адаптерлі кесте маршрутизация ережесін тікелей қолданады, маршрутизация кестесіндегі масканы және желі нөмірін қолдана отырып десте жіберуге арналған портты анықтайды. Сонымен бірге маршрутизация кестесіндегі өзгеріс (жұмыстың нәтижесінде, мысалы, маршрутизация хаттамалары/резервтеу) өңдеуге жаңа келген барлық дестелерге бірден әсер етеді. Сонымен қатар динамикалық адаптерлі кесте рұқсат тізімін жеңіл тексеруге мүмкіндік береді.

Бағдарламалық маршрутизация мамандандырылған БҚ (бағдарламалық қамтамасыздандыру) маршрутизаторлармен толықтырылады (аппараттық әдіс қолданылмаған жағдайда, мысалы туннель ұйымдастыру жағдайында), немесе компьютерді бағдарламалық қамтамасыз етеді. Жалпы жағдайда кез келген компьютер маршрутизацияны өзінің жеке кіріс дестелерінде қолданады (ең болмағанда дестелерді бөлуде, шлюзға жіберілген дестелерде). Басқа IP – дестесін маршрутизациялауда, сонымен қатар маршрутизация кестесін құруда әр түрлі БҚ қолданылады:

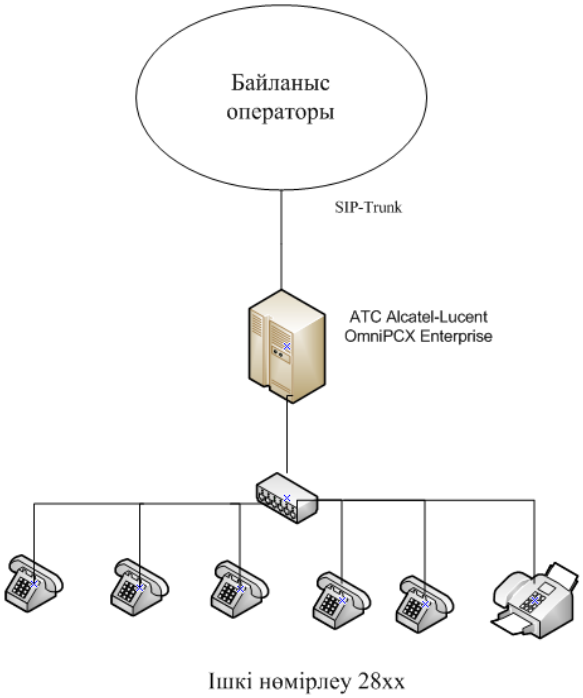
- Сервис RRAS (ағыл. routing and remote access service) Windows Server де
- Демоны routed, gated, quagga Unix – белгілі операциялық жүйеде (Linux, FreeBSD және т.б.)

Фирмадағы қолданыстағы шақырулар маршрутизациясын қарастырайық. АТС Meridian 11C компанияның басты бөлімшесі байланыс ағыны Е 1 операторына қосылғанжәне сыйымдылығы 20 қалалық нөмірге ие (7172) XXXX00 – (7172) XXXX19, компанияның корпоративті шақыруларында ішкі белгілеу қолданылады 25XX. Барлық шақырулар байланыс операторына бағытталады (Сурет 2.1)



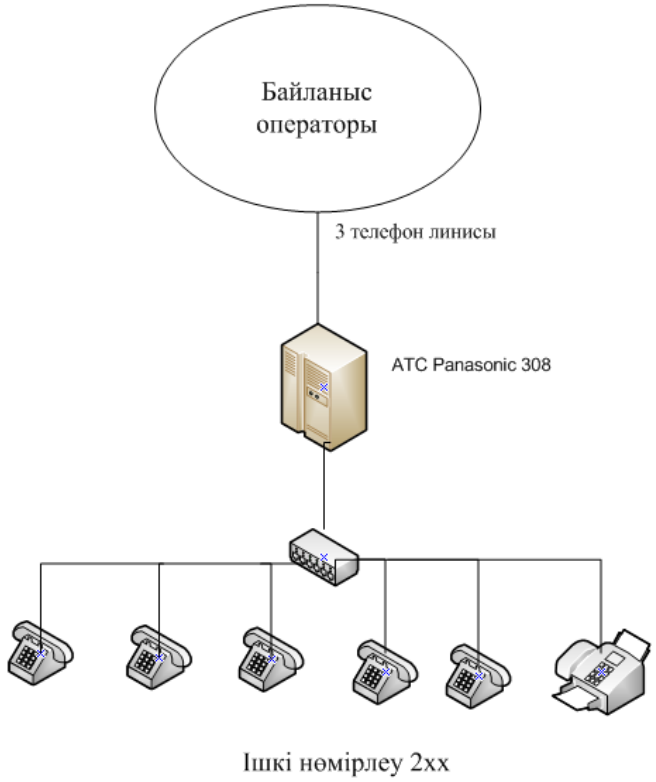
2.1 Сурет – Астана қаласындағы телефон байланысының сұлбасы

Алматы қаласындағы филиалындағы АТС Alcatel байланыс операторына SIP – транкіне қосылған және 10 қалалық нөмірге ие (7272) XXXXX0 - (7272) XXXXXX9, сонымен қатар, корпоративті қоңыраулар үшін ішкі 28XX нөмірлену қолданылады. Барлық қоңыраулар байланыс операторына бір маршрутпен бағытталады(Сурет 2.2).



2.2 Сурет – Алматы қаласының телефондық байланысының сұлбасы

Атыраудағы филиалдың АТС Panasonic 308–і байланыс операторына 3 қалалық нөмірлермен қосылған болатын, ал, ішкі нөмірлену 20Х–мен қосылды. Берілген АТС–ті алып тастап, Asterisk серверін VoIP шлюздерімен FXS аналогты телефондарды қондыру шешімі қабыланды, ал байланыс операторына қосылуды SIP–транкімен жүзеге асыру шешілді (Сурет 2.3).



2.3 Сурет – Атырау қаласының телефон байланысының сұлбасы

Барлық 3 IP – PBX Asterisk–терді орнатып болған соң және олардың арасында SIP – транктерді әрбірімен орнатқан соң, АТС–ке қоңыраулардың маршрутизациясы келесі түрдей өзгертіледі.

11С Меридиан АТС–ке терген кезде:

- 87272XXXXXX Алматы;
- 87273XXXXXX Алматы;
- 87122XXXXXX Атырау, қоңырауларды Астана қаласының Asterisk серверіне ауыстыру қажет болды, себебі, VoIP желісі арқылы қоңырау бағытталуы үшін, альтернативасы ретінде байланыс операторы IP – PBX серверінде қиындықтар туғанда қажет.

Сонымен қатар, ішкі нөмірлері Asterisk станциясына альтернативасыз негізгі маршрут негізінде, қысқа терулер үшін:

- 28XX Алматы қаласындағы филиалдарға қысқа терулер үшін
- 20X Атырау қаласындағы филиалдарға қысқа терулер үшін

Alcatel АТС–іне келесі бағыттарды аудару қажет – Asterisk серверін, ал альтернативаны Asterisk серверлерінде қиындықтар туғанда байланыс операторы арқылы қолдану қажеттігі:

- 87172XXXXXX Астана;
- 87122XXXXXX Атырау.

Сонымен қатар, ішкі нөмірлері альтернативасы жоқ негізгі маршрут негізінде қысқа терулер үшін:

- 25XX Алматы қаласындағы филиалдарға қысқа терулер үшін
- 20X Атырау қаласындағы филиалдарға қысқа терулер үшін

Атыраудың Asterisk серверіне келесідей бағыттарды құру керек, негізгі маршрут ретінде – Астана мен Алматының Asterisk серверлері, ал альтернативаны байланыс операторы арқылы қолданып, қиындық туған жағдайда Asterisk серверлеріне:

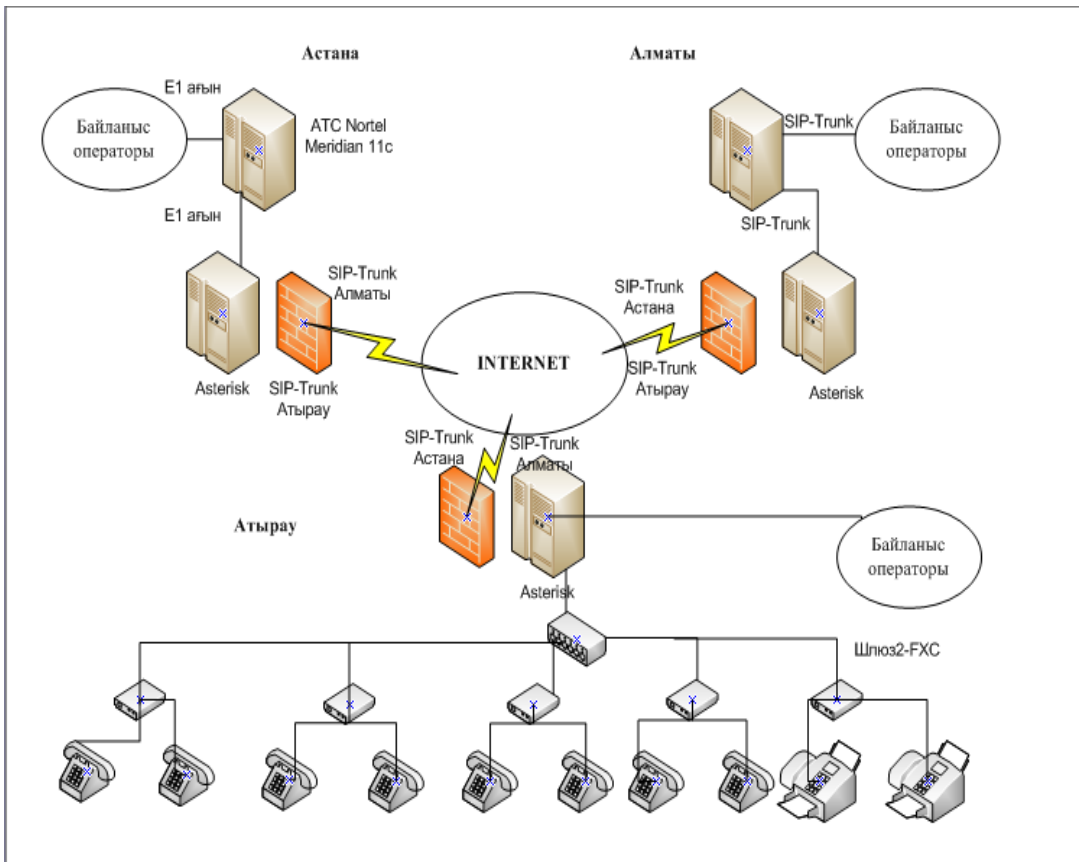
- 87172XXXXXX Астана;
- 87272XXXXXX Алматы;
- 87273XXXXXX Алматы.

Сонымен қатар, ішкі нөмірлері альтернативасы жоқ негізгі маршрут негізінде қысқа терулер үшін:

- 25XX Алматы қаласындағы филиалдарға қысқа терулер үшін
- 28X Атырау қаласындағы филиалдарға қысқа терулер үшін

Келешекте мемлекет аралық қоңырауларды үнемдеу үшін үлкен VoIP провайдерлеріне қосылу ойластырылып жатыр, мысалы, SIPNET және т.б..

Asterisk базасында VoIP корпоративті желісінің жалпы сұлбасы 2.4 суретте көрсетілген.



2.4 Сурет – Asteriskбазасында VoIPкорпоративті желісінің жалпы сұлбасы

2.3 VoIP желілеріне FDoS шабуылдарды зерттеу

VoIP хаттамасының доминантты хаттамасы SIP, алайда ол шабуылдардың көптеген түріне төтеп бере алмайды. Алуан түрлі шабуылдардың ішінен SIP хаттамасы үшін ең қатерлісі флудинг – шабуылдар, сұраныстың көптігінен туындаған, қызмет көрсетуден бас тартулар. Осы жұмыстың мақсаты «жағымсыз» дестелердің санын азайтуға және заңды пайдаланушыларға QoS жақсы параметрлерін ұсынатын, флудинг – шабуылдарды жеңілдету шешімдерін іздеу болып табылады. SIP – серверіне негізделген VoIP жүйелеріне флудинг – шабуылдардың әсері талданады.

Бұл жүйеде SIP прокси – сервері сәйкес абоненттерге сұраныстар мен жауаптар тасымалдауға жауап береді. Сервер әрбір кіріс сұранысты өңдейді. Өңдеу үшін генерациялау, сақтау және аутентификациялауға сұраныстар керек болуы мүмкін, кейбір сұраныстар флудингке пайдаланыла алынады. Сондықтан, SIP прокси – серверлер флудинг шабуылдарға осал болып келеді. Зерттеу екі этапта жүргізілді.

Эксперименттің бірінші этапында брандмауэрмен қорғалмаған желіге флудинг шабуылдардың әсері қарастырылды. Екінші этапта шабуылдарды басудың бар тәсілдері және де олардың тиімділігін арттырудың мүмкін тәсілдері сынақтан өткізілді.

Коммуникация үшін SIP – хаттамасы HTTP хаттамасына ұқсас хабарлама тақырыбын пайдаланады. Хабарламаның денесі не сессия талаптарын сипаттау, не әртүрлі сигнализацияның типтерін инкапсуляциялау үшін қолданылады. IP – желілердің бар қосымшаларымен әрекеттесуді ұйымдастыру және пайдаланушылардың ұтымдылығын қамтамасыз ету үшін SIP электронды пошта адресі сияқты адресті пайдаланады. Жұмыс станцияларының адресі ретінде SIP URL деп аталатын әмбебап қор көсеткіштері URL, пайдаланылады:

аты@домен;

аты@хост;

аты@IP-адрес;

телефон№@шлюз.

Адрес екі бөліктен тұрады.Бірінші бөлігі – жұмыс станциясында немесе доменде тіркелген пайдаланушының аты. Егер екінші бөлік қандай да болмасын шлюзді анықтайтын болса, бірінші бөлікте абоненттің телефон нөмірі көрсетіледі.Адрестің екінші бөлігінде желі доменінің, хосттың аты немесе IP – адрес көрсетіледі.

SIP хабарламасының мәтіндік түрде болуы, оны шабуылдарға осал етеді. 2.5 және 2.6 – суреттерде «INVITE» және «REGISTER» хабарламалары көрсетілген.

```
REGISTER sip:registrar.protei.ru SIP/2.0
Via: SIP/2.0/UDP serv3.protei.ru:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: Bob <sip:vladimir@protei.ru>
From: Bob <sip:vladimir@protei.ru>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Contact: <sip:vladimir@192.0.2.4>
Expires: 7200
Content-Length: 0
```

2.5 Сурет – Әдеттегі «REGISTER» хабарламасы

```
INVITE sip: watson@boston.bell-tel.com SIP/2.0
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip: a.g.bell@bell-tel.com>
To: T. Watson <sip: watson@bell-tel.com>
Call-ID: 3298420296@kton.bell-tel.com
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: ...
v=0
o=bell 53655765 2353687637 IN IP4 12&.3.4.5
C=IN IP4 kton.bell-tel.com
m=audio 3456 RTP/AVP 0345
```

2.6 Сурет – Әдеттегі «INVITE» хабарламасы

2.2 К е с т е – Жалпы SIP сұраныстары келтірілген.

SIP-сұраныс	Мәні
INVITE	Сессияның инициациясы
BYE	Бар сессияны тоқтату
OPTIONS	Абонент немесе сервер түсінетін SIP-хабарламалар мен кодектерді анықтау
REGISTER	SIP пайдаланушының орналасқан орнын тіркеу
SIP-сұраныс	Мәні
ACK	INVITE-сұранысқажауаптықұптау
CANCEL	INVITE- сұранысынжою
SUBSCRIBE	Келесі NOTIFY- сұраныстарғабелгі
NOTIFY	Нақты сессиямен байланысты емес өзгерістер туралы ақппарат беру
REFER	Сыртқы ресурстардың қоңыраулары мен контактарын тасымалдау

SIP жауаптар – бірінші саны жауаптардың категориясын көрсететін, үштаңбалы кодтар.

Жауаптардың 6 категориясы бар: ақпарат жауаптар (1xx), сәтті жауаптар (2xx), жауаптарды қайта бағыттау(3xx), жеткіліксіздік сұранысы (4xx), сервердің шалыс кетуі(5xx) және глобальды сәтсіздіктер(6xx). Жауап хабарламалардың ондаған түрі бар. Ең кең таралғандары 2.3 – кестеде көрсетілген.

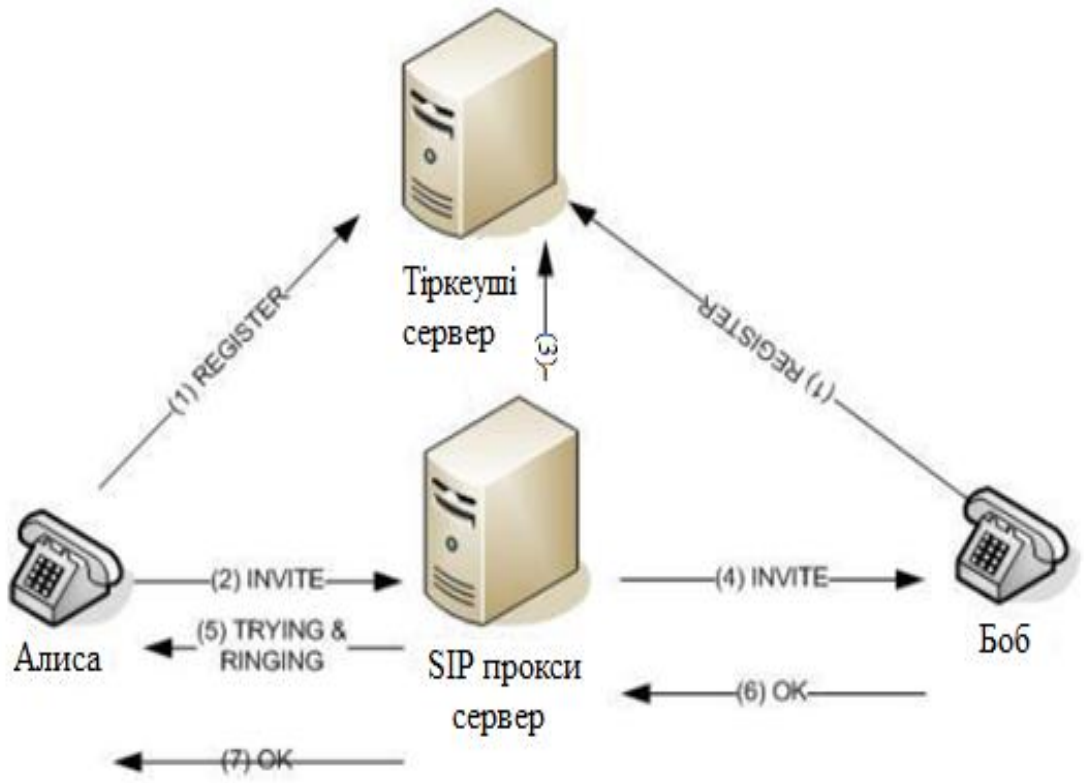
2.3 К е с т е – SIP жауаптары

SIP- жауаптар	Мәні
100 Trying	Прокси INVITE-сұранысын алды және оны өңдеуде деп хабарлау
180 Ringing	INVITE баратын жеріне жіберілді
200 OK	Сессия орнатылды
401 Unauthorized	Дұрыс емес аутентификациялау кезіндегі REGISTER сұранысына жауап
407ProxyAuthentication Required	Проксиге аутентификация қосылған немесе пайдаланушы дұрыс ақпарат бермеген жағдайда INVITE сұранысына жауап
408Requesttimeout	Белгілі уақыт ішінде сұранысқа жауап жоқ
503 Serviceunavailable	Ағымдағы сұраныс өңделе алмайды

2.7 Суретте – SIP компоненттерінің бір – бірімен өзара әрекет етуі көрсетілген.

Егер абонент қоңыраулар алып тұрғысы келсе, оның тіркелуі және REGISTER сұранысын жіберуі керек. Пайдаланушы байланысты ұйымдастырғысы келсе INVITE сұранысы жіберіледі. Прокси – сервер сұраныстарды өңдеп, шақырылатын абонентке жібереді. Шақырылатын абонент тұтқаны көтергенде қоңырау шалушы абонент ОК жауабын алады. Сессия орнатылады.

IP технологияға негізделген басқалар сияқты VoIP әр түрлі қауіп – қатерлерге ұшырағыш. Қарастырылатын технологияға қауіп – қатердердің келесі типтері тән: тың – тыңдау, флудинг тудырған, қызмет көрсетуден бас тарту (флудинг – шабуылдар), дестелерді фрагментациялау негізіндегі шабуылдар, интернет телефония арқылы спам, дауысты фишинг және басқалары. IP бойынша дауысты тасымалдау жүйелері үшін ең көп қауіп – қатер төндіретін, флудинг шабуылдар немесе FDoS (flooding – based DoS) қызығушылық тудырады.



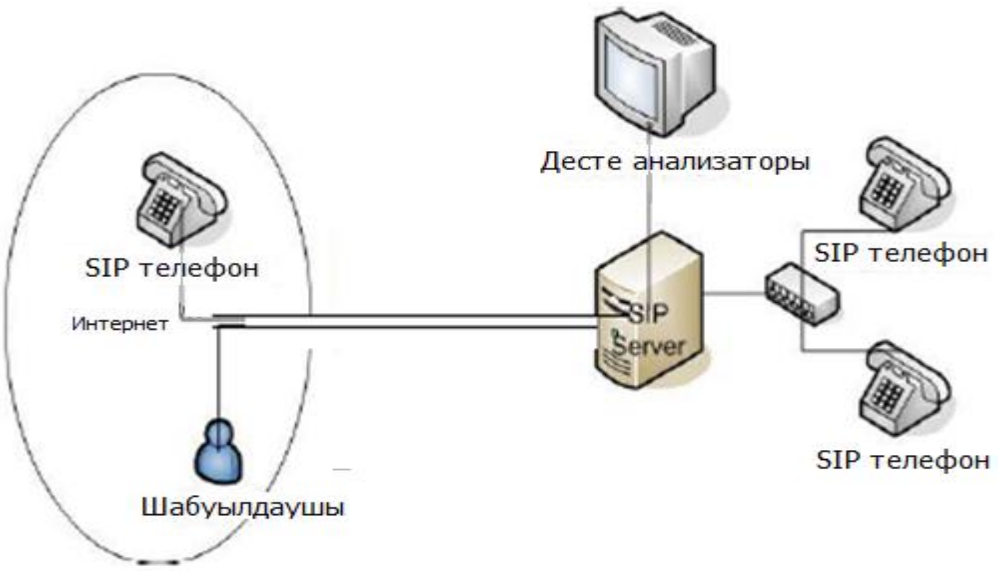
2.7 Сурет – SIP компоненттерінің өзара әрекеттесуі

Шабуыл кезінде қастық қылған адам ауыстырылған IP адрестерден көп INVITE немесе REGISTER сұрыныстарын жібереді. SIP сұраныстарының басқа типтері де бар, алайда INVITE және REGISTER басым болып табылады және өңдеуге жүйенің көп ресурстарын талап етеді.

FDoS шабуылдарының нәтижесі әдетте, жадының толып кетуін, орталық процессордың толып кетуін және соның әсерінен қызмет көрсету сапасының төмендеуіне әкеледі.

Флудинг шабуылдарының әсер етуін зерттеу үшін сұлбасы 2.8 – суретте көрсетілген сынақтық желі құрастырылды.Келтірілген желіде ешқандай қорғаныс құралдары қолданылған жоқ.

Құрастырылған желіде Windows XP professional және 512МбОЗУ операционды жүйе қондырылған төрт стационарлы компьютер бар. SIP прокси сервері ретінде Asterisk пайдаланылады. SIP клиенті үшін SIP софтфон X – lite бағдарламалық қамтамасыз ету таңдалды. Тәжірибеде шабуылды жасау үшін арнайы көп сұраныстар жіберу үшін құрастырылған iFlood сайманы пайдаланылды. Дестелер анализаторынан wireshark таңдалды.



2.8 Сурет – Сынақтық желі

Тәжірибе кезінде SIP сервер 60000 INVITE сұраныстары бар дестелер алды. Қастық қылған адам секундына 30 мың десте жіберіп отырды.

Біз, тәжірибе жүргізу кезінде, жасырын дестелердің саны шақыру кідірісіне қалай әсер ететінін көрдік. 2.9 – суретте флудингтің желіге қалай әсер ететінін көрнекі түрде көрсететін, анализатор құрастырған график берілген. Дестелердің саны 10 мыңнан асқанда байланыс орнату кезіндегі кідіріс лезде көбейеді. Байланыс орнату уақыты 25мс – тенжоғары болғанда байланыс сапасына әсер етеді.

2.9 Сурет – FDoS шабуылдардың желі жұмысына әсері

Жоғарыда көрсетілген қатерлерді азайту үшін желілерде әр түрлі шешімдер қолданылады, олардың кең тарағаны – брандмауэрлер. Оларға толығырақ тоқталайық және олардың шабуылды қалай жеңілдететінін қарастырайық.

Бұрын құрастырылған желіге DFL – 1800 (D – Link) брандмауэрі ретінде пайдаланылатын тағы бір компьютер қосамыз (2.10 – сурет).

2.10 Сурет – Брандмауэр пайдаланылатын сынақтық желі

Тәжірибенің осы сериясында біз, DFL 1800 (D – Link) стандартты брандмауэрін пайдаландық. Брандмауэрдің сыртқы интерфейсі тек өзінің ішкі желісіндегі пайдаланушылардың ғана сұраныстарын қабылдайды. Қастық қылған адамға желінің IP адрестерінің диапазоны белгілі деп санаймыз. DFL 1800 (D – Link) жалған IP адрестері бар дестелерді анықтауға және оларды блоктауға мүмкіндік беретін спуфинг-шабуылдарды блоктау опциясы бар. Біз сипатталған функцияны қосып, SIP серверге 60 мың сұраныс жібердік. Анализатор байланыс орнатудағы кідірістердің санын және брандмауэр арқылы өтетін жалған дестелердің санын анықтады. 2.11 және 2.12 – суреттерде олардың графиктері көрсетілген.

2.11 Сурет – Флудинг кезінде байланыс орнатудағы кідіріс

Бұл диаграммадан жалған дестелердің көбеюі, байланыс орнатудағы кідіріс уақытын көбейтетінін көреміз. Жалған дестелердің саны 8 мыңға жеткенде және асқанда, VoIP сервисті қамтамасыз ете алмайды, клиент «500 – server internal error» - сервердің ішкі қатесі жауап хабарламасын ала бастайды. Жалған дестелердің саны 10 мыңнан асқанда, «500 – server internal error» жауабы 85% - ға жетті.

2.12 Сурет – Брандмауэр арқылы өткізілген жалған дестелер саны

Диаграммадан жалған сұраныстардың көбі, спуфингті блоктау функциясы қосылып тұрғанда да, файерволдан өтіп кететіні көрініп тұр. Бұл тәжірибе, осы тәсіл SIP сервердің сенімді жұмысын қамтамасыз етуге

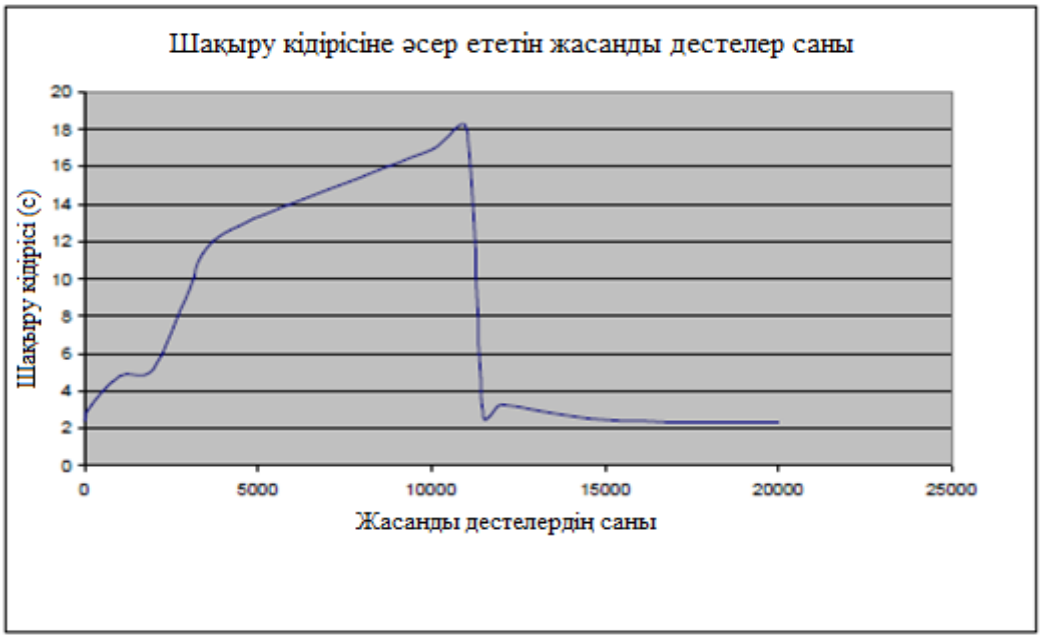
жеткіліксіз екендігін көрсетті. «Ақылдырақ» PIX 520 (Cisco) брандмауэрін пайдаланып тағы бір сәйкес тәжірибе жүргізейік.

2.13 – суретте жалған дестелерге қатысты байланыс орнатудағы кідіріс көрсетілген. 2.14 – сурет брандмауэр арқылы өткізілген дестелердің санын көрсетеді.

Алдыңғы тәжірибе сияқты нәтижелер көңілге қонбайды. Жалған дестелердің бір бөлігі файервол арқылы өтеді және желінің жұмыс қабілеттігі төмендейді. Байланыс орнату уақыты алдыңғы графикпен салыстырғанда жалған дестелердің саны 10 мыңнан асқанда 75% азаяды. Бұдан шығатын қорытынды SIP серверді FDoS шабулдардан қорғау үшін тиімді және сенімді брадмауэрлер пайдаланған дұрыс.

Алынған мәліметтер және теориялық мағлұматтарға сүйеніп, SIP негізінде VoIP желісінің кеңейтілген қауіпсіздік жүйесін құрастыруға талпыныс етілді.

Жұмыстың бұл бөлімінде сұраныстарды өңдеу басымдылығын құру мақсатында, брандмауэр мен заңды пайдаланушылардың адресін «білетін» жүйеден құралатын SIP қорғалынған жүйе ұсынылады.



2.13 Сурет – Жалған дестелер саны мен байланыс орнатудағы кідіріс

2.14 Сурет – Өткізілген жалған дестелер саны

Кеңейтілген функциялы SIP прокси – сервер брандмауэрді пайдаланушылардың ағымдағы IP – адрестеріне сәйкес жаңартып отырады. Жетілдірілген брандмауэр SIP серверден түскен ақпарат бойынша ережелерді өзгертіп отырғандықтан, осы уақыттағы белгісіз пайдаланушыларды интеллектуалды тексеруге мүмкіндік туады.

SIP қабылдайтын IP – адрестерді DHCP беретіндіктен, өзгеріп тұра алады. Сондықтан, біздің жүйеде қандай да бір «уақыт өту» тізімі, тізімнің келісуге боларлық өлшемі сақталынады және тізімге сәйкес ескірген адрестер алынып тасталынады деп жорамалдауымызға болады. Сипатталған механизм жұмыс жасауы үшін белгілі адрестерді синхронизациялау хаттамасы пайдаланылады.

Ұсынылған тәсіл INVITE және REGISTER сұраныстары негізіндегі шабуылдарға сәтті тойтарыс беруге мүмкіндік береді.

Тәжірибе JAIN SLEE ортасында жүргізілді. JAIN SLEE желіні жобалауға, құрастыруға және дамыту үшін жетілдірілген сервистердің бірі. JAIN SLEE таңдау себебі, оның кідірісі төмен және өткізу қабілеті жоғары телекоммуникациялық желілер үшін спецификасында.

Келесі обьектілер құрастырылды:IP адресі, таймері және сұранысты өңдеудің ағымдағы уақыты бар пайдаланушы;

Тізімнен пайдаланушыны табуға жауапты таймер. Тізімнен пайдаланушыны табу уақыты өткеннен кейін, таймер жазуды өшіру функциясын шақырады. Пайдаланушылардың екі тізімі бар: «Жиі Пайдаланушылар Тізімі» және «Пайдаланушылар Тізімі». «Жиі

Пайдаланушылар Тізімінен» шығарылған пайдаланушы «Пайдаланушылар Тізіміне» өтеді. «Пайдаланушылар Тізімінен» шығарылған абонент белгісіз пайдаланушылар тобына өтеді. «Жиі Пайдаланушылар Тізімінің» өмір сүру уақыты «Пайдаланушылар Тізімінің» өмір сүру уақытынан қысқа. Сынақта өмір сүру уақыты тиісінше 10 және 15 минут. Брандмауэр ретінде LinuxIptables пайдаланамыз.

Сынақ нәтижесі 2.15-суретте диаграмма түрінде көрсетілген.

2.15 Сурет – Қорғаныс деңгейі әр қалай әр түрлі пайдаланушылар үшін кідірістің орташа ұзақтығы

Алынған мәліметтер негізінде ұсынылған қорғаныс жүйесі тиімдірек жұмыс жасайды деп қорытынды жасауға болады.

Өкінішке орай, жүйенің тиімділігі тек қана INVITE және REGISTER негізделген шабуылдарға ғана тексерілді.

2.3.1 Қорғансыз желілердегі VoIP трафиктің қауіпсіздігін ZRTP хаттамасының көмегімен қамтамасыз ету

ZRTP – VoIP желілерімен тасымалдауда дауысты кілт алмасуды пайдаланып шифрлейтін хаттама. ZRTP Secure Real – time Transport Protocol (SRTP) ұйымдастыру үшін Диффи – Хелман алгоритмі бойынша кілт алмасу тәсілін сипаттайды.

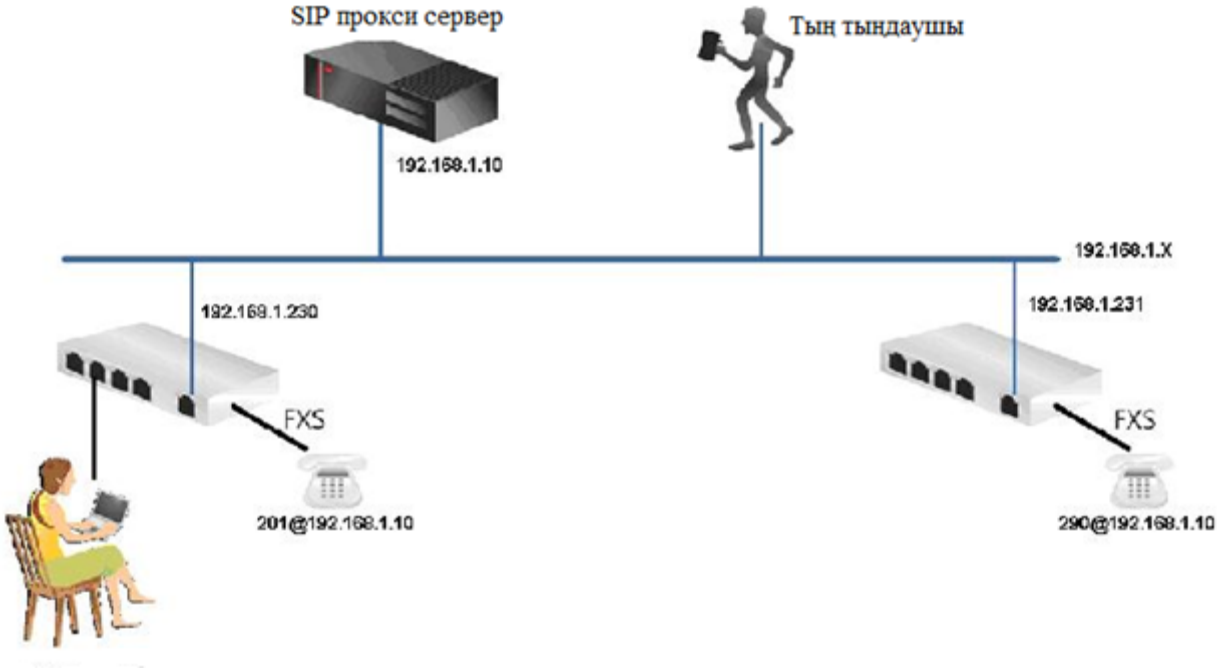
ZRTP Session Initiation Protocol (SIP)хаттамасының сигнализациясы кезінде, қоңырау шалуды инициализациялау уақытында, Диффи – Хеллман кілттер алмасу тәсілін пайдаланып, шифрлау тәсілі ретінде ұсынылады. Қоңырау жіберілген уақытта, хэширлеу функциясын пайдаланып, сөйлесулердің медиа ағыны шифрленетін кілттер құрастырылатын көпшілік ID жасалынады. Сондықтан, кілттер жұбы тек қана бір сөйлесудің уақытында күшінде болады. Осылай, Secure RTP (SRTP) сессиясы құрылады. Осылайша, осы механизмді жұмыс істеп тұрған VoIP бағдарламалық өнімдер, шлюздер және IP телефондарға енгізу мүмкіндігі бар.

Дауысты сессия болсын, немесе интернет – банкпен https қосылысы болсын, шифр каналды ұйымдастырудың басты мақсаты адамды ортада

болдырмай (man – in – the – middle), IP желілерінің кез келген екі нүктесінің арасында біртұтас криптоқорғанысты қамтамасыз ету. Теориялық тұрғыдан ZRTP–ні SIP, H.323, SCCP, MGCP Unistim және Jingle қоса алғанда медиа ағынды тасымалдауға RTP пайдаланатын кез келген сигналды хаттамалармен бірге пайдалануға болады. Себебі, теорияда ZRTP RTP медиа сессиясында кілттер алмасуды жүзеге асыра отырып, сигнализацияға тәуелді емес.

Zfone программасының көмегімен сөйлесулердің құпиялығын қамтамасыз етуді қарастырайық. Zfone – Интернетпен (VoIP) дауысты мәліметтерді қауіпсіз тасымалдау үшін жаңа бағдарламалық қамтамасыз ету. Бағдарлама кез келген жерде, кіммен болсын, қашан болсын жеке сөйлесулерге мүмкіндік береді.

Zfone кез келген Zfone Windows, Mac OS X немесе Linux PC жүйелерінде жұмыс жасайды, барлық VoIP дестелерді ұстап алып сүзгілейді және нақты уақыт режимінде қоңыраудың қауіпсіздігін қамтамасыз етеді. Zfone программалық қамтамасыз етуі қоңыраудың басталған уақытын анықтайды және жақтар арасындағы криптографиялық кілттердің сәйкестігін тексеруді бастайды, сосын дауыстық дестелерді шифрлеуге көшіреді. Zfone кез келген стандартты IP телефонымен бірге жұмыс жасай алады, бірақ қоңырауларды тек пайдаланушы басқа ZRTP клиентке қоңырау шалғанда ғана шифрлейді. Жұмыс істеп тұрған VoIP клиенттердің ауқымды спекторын, VoIP каналымен мәліметтерді қорғалған тасымалдау функциясымен қамтамасыз ете отырып, Zfone әмбебап «кеңею» ретінде қол жетімді. 2.16 – суретте SIP Proxy Server және Zfone программасын пайдаланатын екі клиенттен тұратын тәжірибелік желі көрсетілген.

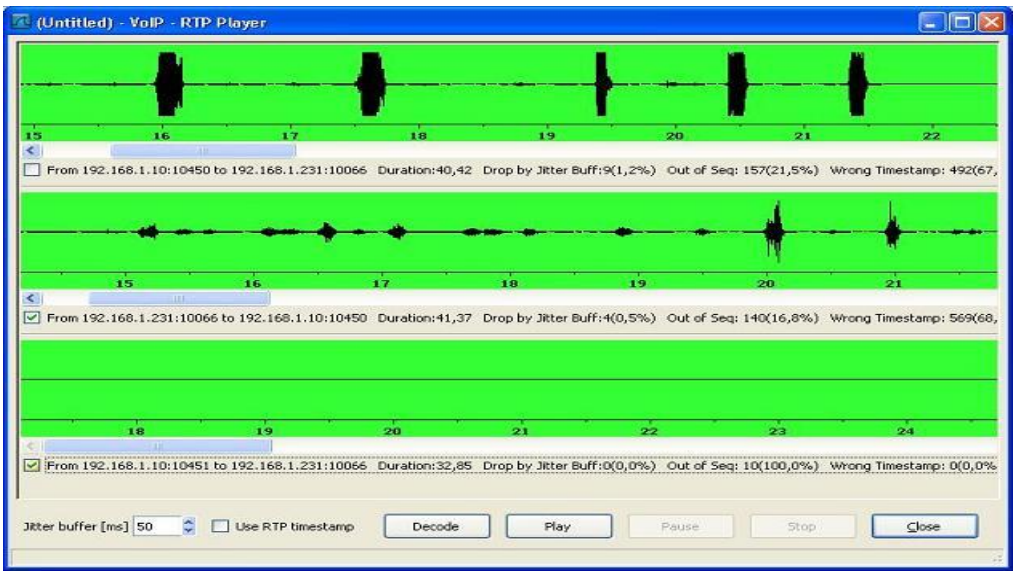


2.16 Сурет – Сынақтық желі

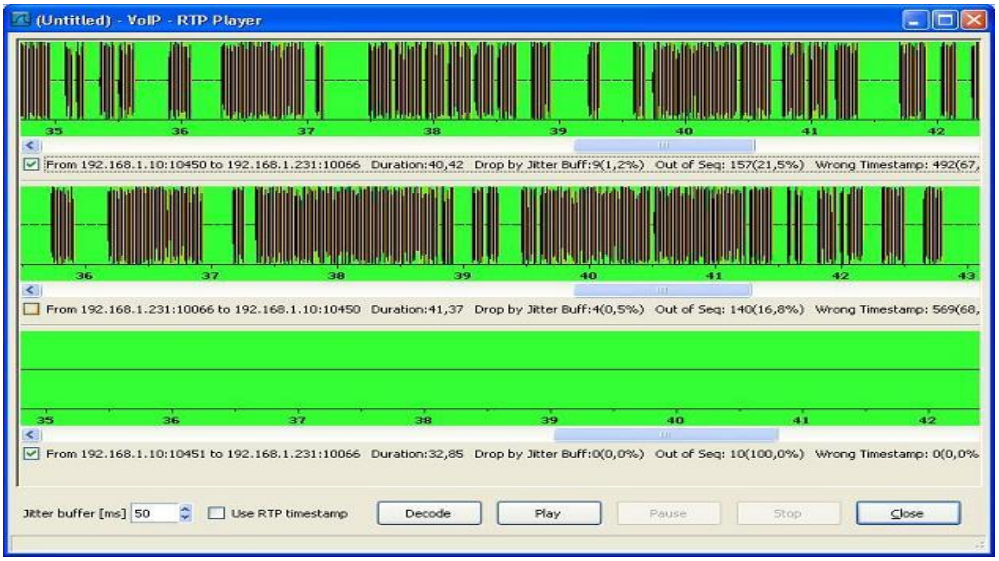
Телефондар ретінде X – lite бағдарламалық телефоны пайдаланылды (2.17 – сурет).

2.17 Сурет – X – Lite бағдарламалық телефоны

Сөйлесуді тыңдаудың мүмкін еместігін, RTP трафигін ұстап алып, оны аудио файлға түрлендіру нәтижесінде алынған уақыттық диаграммаларды қарап, көрнекі түрде көз жеткізуге болады. 2.18 – суретте қауіпсіздікті қамтамасыз ететін құралдарды пайдаланбай сөйлескен кездегі диаграмма көрсетілген. Бұл жағдайда, қастық қылған адам, мәліметтер тасымалдау ортасына оңай қол жеткізіп, әңгімені тыңдай алады. 2.19 – суретте қорғалынған сөйлесудің уақыттық диаграммасы көрсетілген. Бұл байланысқа пайдаланылған RTP ағынды ұстап алып, аудио файлға түрлендіргенде шудан басқа ештеме естілмейді.



2.18 Сурет – Қорғалынбаған дауыстың уақыттық диаграммасы



2.19 Сурет – Қорғалынған дауыстың уақыттық диаграммасы

VoIP трафикті тасымалдау үшін Zfone бағдарламасы көмегімен қорғалынған байланыс каналын құрастыруға болатынын көреміз.

3 ЭКОНОМИКАЛЫҚ БӨЛІМ

3.1 Техникалық – экономикалықнегізделулер

Жобада АТС IP-PBX, VoIP желілері мен интернет телефониясының даму үрдістері қарастырылған. Өткізу қабілеттілігінің, арнаның қолданылу дәрежесі мен қолданылған құрылғының сипаттамасы есептелінген. Жобаланған VoIP желісін қолдану фирманың мемлекет аралық қоңыраулар шығынын азайтуға мүмкіндік береді. IP – телефонияның тарифтері ақша өнімдерінің үнемдеуіне телефон желілерінің жүйелеріне қарағанда мүмкіндік береді. Оған себеп болып, жаһанды интернет желісі болып табылады, оның қорлары ақпарат пішіміне қарамастан алмасуға мүмкіндік береді. Бұл өте ыңғайлы және сенімді, бастысы үнемді.

Техникалық – экономикалық негізделуі (ТЭН, ағыл. business case) – құжат, ақпараты өнім шығаратын немесе қызмет көрсететін мүддені қамтиды. ТЭН шығын саралау мен қандай да бір жобаның нәтижесін қамтиды. ТЭН инвесторге ақшаны берілген жобаға салуға болатын-болмайтынын анықтауға мүмкіндік береді.

ТЭН келесі бір әсер нәтижесінде пайда болады:

- нарықтың талаптары;
- ұйымның мұқтаждығы;
- тапсырыс берушінің талаптары;
- технологиялықозықтық;
- құқықтық талаптар;
- экологиялық әсерлер;
- әлеуметтік мұқтаждықтар.

ТЭН бизнес-жоспарға ұқсайтынына қарамастан, айырмашылығы ТЭН жобаның негіздеуі болып табылады, ал бизнес – жоспар міндеттер мен ұйымның мақсаттарын қамтиды, яғни, кәсіпорынның негізі болып табылады.

3.2 Күрделі қаржы шығыны

Күрделі қаржы шығыны (ағыл. CAPital EXpenditure, CAPEX) – капитал, фирмалар қолданатын физикалық активтердің алынуы мен модернизациясы үшін (тұрғындары бар және өнеркәсіптік жылжымайтын мүлік, құрылғы, технология).

Жиірек CAPEX атты анықтаманы кездестіреміз – негізгі фондтардың сатып алуына кететін шығындар, сонымен қатар, кредиттердің қызмет көрсету шығындарын есептейді.

Капиталдық шығындар инвестициялық өнеркәсіптің жұмыстарын атқарады және құрылғыны сатып алуды қарастырады. Капиталдық шығындар шатырдағы терезелерді ауыстыруға және судай жаңа фабрикаларды тұрғызуға

жұмсалады. Жалпы жағдайда капиталдық шығындар негізгі әдістің уақыт бойынша өсуімен есептеледі. Көптеген кәсіпорындар негізгі құралдарға көптеген салым салады, қаншалықты салым салса соншалықты жұмыстың өнімділігі 60 % артады. Капиталдық шығындар VoIP желісінің құрылысына, яғни құрылғының өзін алуға және оны орнатуға жұмсалады.

Капиталдық шығындардың есептелуі төмендегі кестеде көрсетілген

3.1 К е с т е – капиталдық шығындардың сметасы

Шығынның атауы	Өлш.бір.	Саны	Бірліктің құны (тг)	Жалпы құны (мың тг)
1. Сервер	дана	3	200 000	600,0
2. FXS шлюзі	дана	5	35 000	175,0
3. E1 платасы	дана	1	102 000	102,0
4. Монтаждық жұмыс	%	10		87,7
Барлығы:				964,7

3.3Шартты кірістер

Компаниялардың филиалдары арасында жүргізілген анализдер нәтижесінде 1 жылдың қорытындысы шықты, яғни 70% қоңыраулар Астана, Алматы, Атырау қалаларына бағытталған. Желінің жобалануына байланысты осы бағыттардағы қоңыраулар тегін болады. Байланысты қамтамасыз ету үшін интернет қорлары қолданылады.

3.2 – кестеде шығыс айырбастың салыстырмалы кестесі көрсетілген.

3.2К е с т е – бір ай ішіндегі шығыс айырбасты салыстыру

Бағыт	Өлш. бір.	Байланысқа кеткен шығындар		
		Корпоративті VoIP желісін құрғанға дейін	Корпоративті VoIP желісін құрғаннан кейін	Үнем
Астана	Теңге	50 000	10 000	40 000
Алматы	Теңге	30 000	7 000	23 000
Атырау	Теңге	15 000	6 000	9 000
Барлығы:		95 000	23 000	72 000

Бір жыл ішіндегі желіні құруға кеткен шығынның үнемділігі:

$$\text{Үнем} * \text{ай} = 72000*12 = 864000 \text{ тг} \quad (3.1)$$

Шығынның үнемділігін пайда деп білейік ($Д_{шарт}$).

3.4 Бір жыл ішіндегі желіге қызмет ететін шығындар

Шығындар – қорлардың өлшемі (ақша түрінде оңайлатып өлшенген), белгілі уақыт кезеңінде шаруашылық процесі кезінде қолданылған.

Ағымдағы шығындар (ағыл. current expenses) – есепшінің есебінде ұйымның шығыны,әрине өнімнің шығуымен байланысты, жұмыстың орындалуымен байланысты, қызмет көрсетуімен байланысты, технологиямен серттелген және ұйымның өндіруімен, сонымен қоса, материалдық шығындар және жұмысшылардың жалақыларының шығыны, өнімнің сапалылығы, эксплуатация кезіндегі шыққан кемшіліктерге де байланысты болып келеді.

Электроэнергия (Э):

1 квт/сағ құны 2014 жылға орта есеппен 19,56 тг құрайды. Желінің қондырғылары күндіз – түні жұмыс істейді, оның қуаты шамамен 700Вт құрайды.

Электроэнергияның жылына шаққандағы шығыны:

0,7 квт*24сағ*30күн*12ай*19,56тг = 118298,88 тг.

Материалдардың шығыны(М) :

Материалдардың шығынын есептеу үшін 0,5% жылына капиталдық шығындарды есептеу алынады (К). Формула арқылы есептейік:

$$М= 0,5\% * К = 0,5\% * 967000 = 4800 \text{ тг} \qquad (3.2)$$

Амортизация (латын. Amortisatio – өтеу; франц. Arnor – tir – бәсеңдету, жұмсарту) – жалпы ұлттық өнімдіөндіру барысында тозған немесе пайдаланылған (тұтынылған) капиталдыңкөлемін бағалау; негізгі қорлардың тозуына қарай олардың құнын өндірілетін өнімге (орындалатын жұмысқа, көрсетілетін қызметке) бірте – бірте көшіру жолымен олардың құнын өтеу үдерісі. Амортизация аударымының сомасы тозымпұл нормаларына сәйкес өндіріс пен айналыс шығынына енгізіледі, негізгі қорлардың тозуы дәрежесін сипаттайды және олардың толық қалпына келтірілуі (ұдайы өндірілуі) үшін ақшалай өтемпұл қорын құрады. Тозымпұл бейматериалдық активтердің тозуын есептеу кезінде де есептеледі. Тозымпұл термині басқа мағыналарда да қолданылады: жеке адамның немесе ұйымның дүркіндік жарналар төлеу немесе міндеттемелерді сатып алу жолымен борышты бірте – бірте өтеуі; борышқорлық міндеттеменің ұрлануы, жоғалуы, т.б. себепті оны жарамсыз деп тану; машиналарда, құрылғыларда – машиналардың конструкцияларындағы арнаулы қондырғылардың (тербелістерді өшіргіштердің), оларды салмақтан қорғайтын құрылғылардың көмегімен соққының, серпудің күшін жұмсарту, бәсеңдету.

Амортизациялық аударымдар амортизация нормалары бойынша жасалынады. Амортизация нормасы – бұл амортизациялық аударымдардың

жылдық сомасының негізгі құралдардың жылдық орташа құнына қатынасы.Негізгі құралдарға амортизация (тозуын) есептеудің басты мақсаты олардың құнын өтеу көзін таба білуден тұрады. Бұл көз амортизацияны шығыстарға, шығындарға қосу есебінен жасалады. Амортизациялық жарналардың сомасын көбейту немесе азайту шығыстарды бұрмалауға алып келеді, мұнан жиынтық жылдық кірістің көлемін, кірістерді бұрмалау орын алады, демек, салық салудағыдәлсіздіктерге әкеліп соғады.Жұмыс істеген бүкіл кезең ішіндегі амортизациялық жарналардың жалпы мөлшері амортизацияланатын құнға немесе бастапқы және тарату құндары арасындағы айырмаға теңестірілуі тиіс. Желі жобасы үшін амортизацияның нормасы ретінде 15% көлемінде аламыз. Формуламен есептесек:

А = К * 15% = 964700 * 15% = 144700 тг(3.3)

Барлық шығын (Ш):

Ш = А + Э + М= 144700 + 55400 + 4800= 203900 тг(3.4)

Шартты пайда (П) бір жыл ішінде жобада:

$П_{шарт} = Д_{шарт} – Ш = 864000 – 203900 = 660100$ тг (3.5)

Жобаның өзін – өзі ақтауы (А) капиталды шығындар мен шартты пайда арқылы табылады:

$$A = \frac{K}{Дшарт} = \frac{964000}{660100} = 1.5ж \qquad (3.6)$$

Берілген жоба өзін 1.5 жылда ақтайды, жобаның өзін ақтау уақыты 1.5 жыл, жобаның пайдасы үнемділікте болуы алғы шарты болғандықтан жобаның келешегі әбден мүмкін және сенімділігі мол.

4 ӨМІРТІРШІЛІК ҚАУІПСІЗДІГІ БӨЛІМІ

4.1 Байланыс желілерінде жұмыс істеу кезіндегі еңбек шарттарының талдауы

Жазылып отырған дипломдық жұмыста IP телефондама мәліметтерінің тарату желісін тұрғызу мүмкіншілігі қарастырылады. Оператордың жұмыс орны отырып жұмыс істеу үшін талаптарға сәйкес болуы керек.Дипломдық жұмыстың мақсаты, интернетпен басқару жүйесі бар компьютердің түйісу блогын енгізу болып табылады. Бұның жұмысы жеке компьютер арқылы іске асады.

Жұмыс орнының кеңістігінің ұйымы қолайлы жұмыс жағдайын қамтамасыз ету керек:

адам басы 10 – 20 градусқа иіледі;

арқа тірегі болады, иық пен білек аралығы және бөксе мен сирак аралығы тік бұрышты болып орналасуы керек.

Жүйеге салынатын жұмысшы орны негізгі параметрлерге тиісті болып тұруы қажет. Осы арқылы әр адамға қолайлы шарттар жасау мүмкіндігі қамтамасыз етіледі. Дербес компьютермен жабдықталған жұмыс орынның негізгі сипаттамалары (4.1 сурет):

– отыру биіктігі 42 – 45 см ;

– еденнен пернетақтаға дейінгі биіктік 70 – 85 см ;

– пернетақтаның көлденең орналасқан бұрышы 7 – 15 градус ;

– пернетақтаның үстел бұрышынан алшақтығы 10 – 26 см ;

– экран орталығынан еденге дейінгі арақашықтық 90 – 115 см ;

– экранның тігінен иілуі 0 – 30 градус (қолайлы 15);

– экранның үстел бұрышынан жоюлуы 50 – 75 см ;

– жазу істеріне арналған жұмыс бетінің биіктігі 74 – 78 см ;

– жұмыс орнында аяққа арналған тіреуді қарастыру керек, бұл әсіресе ұзақ отырып істелетін жұмыстарға ұсынылады.

Жұмыс нәтижесінде жалпы залдардағы жұмыс орындарының орналасу кеңістігіндегі адамның қорғануы үшін дербес кеңістік пен өзарақатынас сипаттамасы және сыртқы жағдайларға байланысты қолайлы арақашықтықтың қажеттілігін есепке алу қажет.

Арақашықтығы 215 – 400 см болатын жұмыс орындарын орналастыру ұсынылады (ұзағы фазалық әлеуметтік арақашықтық). Осы арақашықтықтарға басқа беттің қатысуына байланысты жақын орналасқан арақашықтықтарды жатқыза алмаймыз. Осы кезде адам жұмыс жасауын жалғастыра алады және басқа адам қатыса алады.

Жүйелік одақтар жұмысшы орында – жинақтағыштарға қол жетерліктің иілгіш магниттіктерді тегеріштерде және ыңғайлы рұқсаттың және басқару органдарына сырт жақтарында орналастырады. Жүйелік одақ жақын маңда жиі

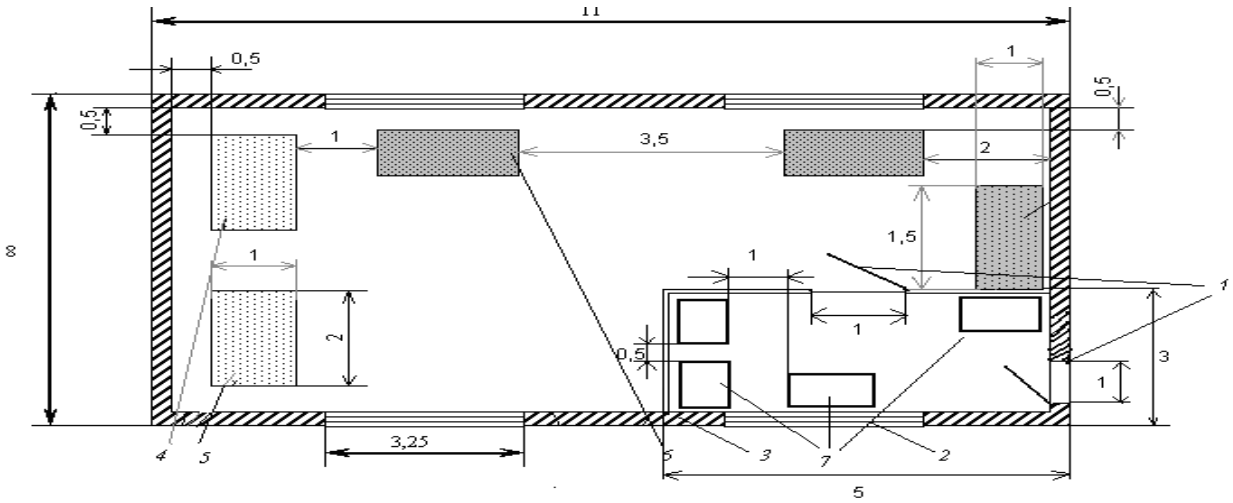
қолданылатын дискеталарға тиісті электромагниттен қорғалған ұйымда сақталу қажет. Принтер болса ережеге сәйкес, пайдаланушыдан оң жағында орналастырады. Басылатын мәтін операторға тиісті белгілі болу оның табу жанында ең басты жұмысшы дене тұрысына. Принтерден жақын маңда орналасқан таза қағаз және басқа қажетті бұйымдар арнайы бөліктерде сақталады.

Құрастырылған сымдар арнайы арналарда салынады. Сондай арналардың құрылғысы бар болуы тиіс, құрастырылмағандар үшін сымдардың шығаруына кедергі болды .

Бүкіл зал аппараттық және операторлық залдарға бөлінеді.Бұл бөлменің өлшемдері: ұзындығы 11м, ені 8м, биіктігі 3,5м. Ауданы 88м^2.

Бөлменің төбесі жарық, қабырғалары ашық түсті және терезелеріне еш нәрсе ілінбеген. Көрермендік жұмыс разряды – III. Нормаланған жарықтылық – 300 лк.Операторлық зал қауіпсіздігі төмен бөлмелерге жатады, себебі: жоғары қауіпсіздікті тудыратындай ешқандай белгілері көрсетілмеген. Ол белгілерге дымқылдық, токөткізуші шаң, токөткізуші едендер, жоғарғы температура жатады.

Синхронизация жүйелерінің құрылғысын алдын алу жылына бір реттен кем болмауды талап етеді және операторлық зал сәуле шығарушы құрылғыдан қорғалған. Құрылғымен екі оператор және бір инженер жұмыс істейді. Жұмыс кестесі қалыпты күніне 8 сағатты құрайды, сонымен қатар жыл сайынғы жалақысы сақталған еңбектік демалыстары бар. Құрылғылардың тораптық – құрылғылар бөлмесінде орналасу сұлбасы 4.1 суретте көрсетілген.



4.1 Сурет – Автозал жоспары

1– есік; 2 – терезе; 3 – қабырға; 4 – маршрутизатор, шлюз; 5 – коммутатор, 6 – үстел; 7 – компьютерлер.

Суретте көрсетілгендей аппараттық залды қауіпсіздігі жоғары бөлмелерге жатқызуға болады, себебі: оған тән бір белгі бар, ол адамның біруақытта жермен қосылған металл конструкциялы ғимаратқа, технологиялық аппараттар мен механизмдерге жанасу мүмкіндігін айтады

4.2. Электр қауіпсіздігіне баға беру

Бөлмеде біз келесідей телекоммуникациялық құрылғыларды орналастыруды ұсынамыз:

– медиа – шлюзі RNG-120;

– телефондық рет қақпа ;

– Cisco 7505 маршрутизаторлары;

– Cisco Catalyst 3500 коммутаторлары;

– персональді компьютерлер.

Құрылғылардың барлығы куәлікке ие болғандықтан, профессионалдық тәуекел класын минималды деп анықтаймыз.

Қауіпсіздік өлшеміне қатысты электрқұрылғылар жұмыс кернеуі 1 кВ дейінгі құрылғыларға жатады.

Электрлік тоқпен жеңіліс қауіптілігінің дәрежесі бойынша,бөлмені қауіпсізділігі төмен кластарға жатқызамыз, бұл келесідей талаптарға сай келеді:

-құрғақ;

-нормаланған температуралы;

-изоляцияланған едендермен;

-шаңсыз;

-жерленбеген заттар бар;

Дегенмен, қызметкөрсетуші персоналдың тұрақты жиіліктегі тоқтан ұтылу ықтималдылығы болады. Құрылғыдағы қоректендіру блоктарын, коммутация блоктарын ауыстырған кезде, қорек кернеуі (48–ден 60В дейінгі) астындағы изоляцияланбаған электрлік бөлшектерге кездейсоқ жұғысып қалады. Бұл кернеу өмір үшін қауіпті. Сондықтан берілген құрылғыны жерлеу қажет. Төменде жерлеуге есептеулер жүргізіледі. Қоршаған орта сипаттамасы бойынша бөлмені "нормальді құрғақ" классына жатқызуға болады, қатысты ауа ылғалдылығы 60% асырмайды. Рұқсат дәрежесі бойынша, оны электротехникалық санатқа жатқызамыз, яғни құрылғыға рұқсат тек электротехникалы персоналдармен ғана жүзеге асырылады. Барлық жоғарғыжиілікті құралдар мынандай түрде жобаланған, жұмысшыларға әсер етуші сәулелену деңгейлері нормативті мәндерден аспайды.

4.3 Бөлме желдетуінің есептелуі

Аппараттық зал бөлмесінде ескі ВК – 1 маркалы кондиционер орнына фирмасының қазіргі кездегі ауалы кондиционерлері орнатылған, олар жылдың барлық мезгілінде нормаланған жұмысқа қажетті құрылғы темпера-турасын қадағалайды және де олар шаңнан және зиянды заттардан тазартылған таза ауаның берілуін қамтамасыз етеді. Вентиляция әдістемелік нұсқауы мен СНиП РК 4.02.42 – 2006.Отопление, вентиляция и кондиционирование воздуха.» тарабымен байланысты орындалып, бөлмеде жоғары микроклимат пен құралдардың дұрыс жұмыс істеуін қамтамасыз етеді. Желдеткіштің техникалық сипаттамасы 4.1 кестеде.

4.1К е с т е - Желдеткіштің техникалық сипаттамасы

Желдеткіш үлгісі	С-65-СВН-С
Суыту қуаты	15,3
Қыздыру қуаты	12
Толық жүктеме тоғы	25
Номиналды ауалы ағын, (м3/сағ)	14350
Жұмыс режимі	Үздіксіз

Кестеде сонымен қатар жеке бөлмелерде ауаны таратын жеке реттеушінің мүмкіншілігі қарастырылады.Бөлмеден жою керек кездегі ауа санының жылу шығынын анықтайтын формула:

$$Lb = \frac{Q_{шы}}{C_b \Delta t \gamma_b} \qquad (4.1)$$

мұндағы,Qшығ – шығындық жылу, ккал/сағ;Са – құрғақ ауаның жылу сыйымдылығы, (0,24 ккал/кг С); ∆ t=tшығ – tкір – бөлмеден шығатын және келіп түсетін ауаның айырымы, С;γb=1,206 кг/м3 – ауаның меншікті массасы. ∆ t өлшемі есептеу кезінде ауаның жылу кернеулігінің тәуелділігінен таңдалады.

$$Qн=Qшығ/Vп \qquad (4.2)$$

Егер ауаның жылу кернеулігі Qн<20 ккал/м болса, онда Δ t= 6С деп алынады, ал Qн>20 кезінде Δ t=8С. Шығындық жылу келесі формулада:

$$Q_{шығ}=Q_{құр}+Q_{жар}+Q_{адам}+Q_{күн}-Q_{ж.беру} \quad (4.3)$$

мұндағы, Qқұр – өндірістік құрылғымен бөлінетін жылу, ккал/сағ; Qжар – бөлменің жасанды жарықтылық жүйесінен бөлінетін жылу, ккал/сағ;Qадам – адамдармен бөлінетін жылу, ккал/маг; Qкүн – күнмен бөлмеге келіп түсетін жылу, ккал/сағ; Qж.беру – жасанды жылумен жылу беру, ккал/сағ;

Qқұр – өндірістік құрылғымен бөлінетін жылуды мына формуладан көруге болады (4.4)формулада:

$$Q_{құр}=860P_{құр} \times n \quad (4.4)$$

мұндағы, 860 – 1 кВт/сағ жылулық эквиваленті; Рқұр – құрылғының қолданатын қуаты, кВт/сағ (Рқұр=40 кВт/сағ); n – бөлмеге өтетін жылу мөлшері, оны n= 0,95 деп аламыз:

$Q_{құр}=860 \times 40 \times 0,95=32680$ккал/сағ

Жарықтандырғыш құрылғылармен бөлінетін жылуы:

$$Q_{жар}= 860 \ P_{жар} \times \alpha \times \beta \times \cos\varphi \quad (4.5)$$

мұндағы, $P_{жар}$ – жарықтандырғыш құрылғының қуаты ($P_{жар}$=0,018 кВт);α – электрлік энергияның жылулыққа айналуындағы ПӘК (қыздыру шамы үшін 0,92÷0,97); β – бөлмедегі аппаратура жұмысының біркелкілігінің ПӘК – і (егер барлық аппаратура жұмыс істесе β=1);cosφ = 0,75 – коэффициент;Qжар= 860x0,018x0,94x1x0,75= 10,91 ккал/сағ. Аппараттық зал үшін жылу мәні ретінде адамдармен бөлінетін Qад–ды (Qад=0) деп қарастыруға болады. Аппараттық залда қосымша шарттар болмағандықтан, шығындары көп болатын бөлмелер үшін, бөлме конструкциясы арқылы берілетін табиғи жылуберу жолы шамамен біз ескермеген Qкүн= Qж.беру күн радияциясы арқылы терезеден бөлмеге келіп түсетін жылу санына тең деп есептейміз. Жылдың жыл мезгілі үшін есептеулер кезінде Qж.беру=0 деп аламыз. Нәтижесінде жылу шығыны, жарықтандырғыш қондырғылар мен құрылғылармен бөлінетін жылу есебінен пайда болады:

$$Q_{шығ}= Q_{құр}+ Q_{жар}= 32680+10,91= 32690,91 \text{ ккал/сағ} \quad (4.6)$$

Осыдан, бөлмедегі жойылатын қажетті ауа саны:

$$Lb = \frac{32680}{0{,}24 \times 8 \times 1{,}206} = 14116.6 \text{ м3/сағ}$$

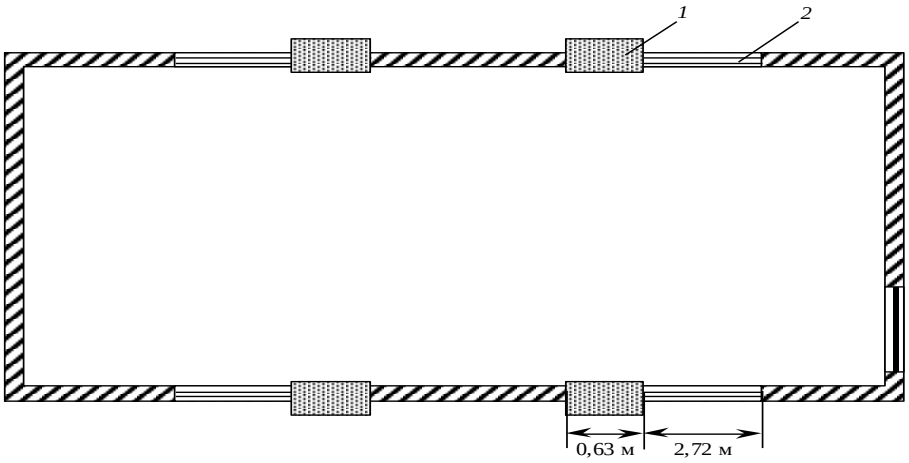
Желдеткіш жүйесі сұранылатын ауа алмасу қысқалығын қамтамасыз етуі қажет. Ауа алмасу қысқалығы n – 1 сағатта бөлмеге келіп түсетін ауа санының, бөлме көлеміне Vп (аппараттық залда стандарт В – 210 м^3) қатынасын айтады.Осыдан қорытындылағанда, ауа алмасуының қысқалығын табамыз:

$$n = LB/VЛ \qquad (4.7)$$

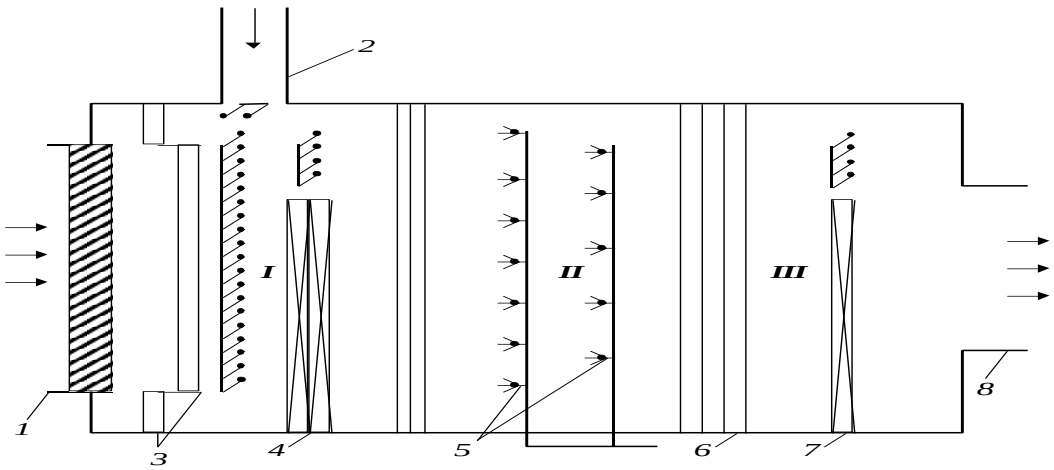
мұндағы, LB – бөлмеге келіп түсетін, ауа саны, м^3/сағ;$V_п$ – бөлме көлемі, м^3;Мәндерді орнына қойғанда, алатынымыз:

$$n = \frac{14116{,}6}{210} = 67.22$$

Сондықтан, В стандартты станцияның аппараттық залының бөлмелерінде, бөлінетін жылу шығынын жою үшін, 67,22 ауа алмасу қысқалығы қамтамасыз етіледі. Есептеуге сәйкес, моделі С – 65 – СВН – С АРАС фирмасының желдеткішін таңдаймыз. Бөлмедегі кондиционерлердің орналасуы және кондиционер сұлбасы төмендегі суреттерде:



4.2 Сурет – Бөлмедегі кондиционерлердің орналасуы:
1 – кондиционер; 2 – терезе



4.3 Сурет – Кондиционер сұлбасы бөлмедегі кондиционерлердің орналасуы және кондиционерсұлбасы көрсетілген

I – ауа ығысуының камерасы; II – шаю камера; III –екіншілік жылыту камерасы; 1 – сыртқы ауаның ауа алмасуы; 2 – рециркуляциялы ауаның ауа алмасуы; 3 – сүзгі; 4 , 7 – калориферлер; 5 – форсунка; 6 – тамшы бөлгіш; 8 – нақтылы ауа

4.4 Шешімі

Байланыс желілерінде жұмыс істеу кезіндегі еңбекті қорғау және экологиялық қауіпсіздік бөлімінде IP телефондама мәліметтерінің тарату желісін тұрғызу мүмкіншілігі қарастырылды. Оператордың жұмыс орны отырып жұмыс істеу үшін талаптарға сәйкес болуы керек.

ҚОРЫТЫНДЫ

Бүгінгі қоғам үшін телекоммуникацияның, жалпы алғанда, компьютерлікжеліліер мен телефонияның маңызы өте зор. Соңғы уақытта әр түрлі желілердің бір-біріне тоғысу (жақындау) тенденциясы байқалуда: жаһанды және локальдікомпьютерлік желілер, телекоммуникациялық желілердің түрлерінің тоғысуы: телефондық, телевизиялық, радиожелілер. Технологиялық тоғысудың себептері ақпарат алмасуда сандық форматқа көшумен тікелей байланысты.

VoIP технологиясын пайдалану жаһанды роумингті қолжетімді етеді, интернет желісі арқылы абонентті әлемнің кез келген нүктесімен байланыстыра алады. VoIP – қарқынды даму үстіндегі өзекті технология, өндірістің, бизнестің дамуына кеңінен жол ашатын, болашақта дәстүрлі телефонияны толығымен алмастыратын озық технология. Жобада Asterisk бағдарламасын қолдана отырып, фирмада корпоративті VoIP желісі орнатылды. VoIP желісін пайдалану арқылы фирма халықаралық телефон байланысына кететін шығынды төмендетуге қол жеткізе алады.

Есептеу бөлімінде байланыс арнасының есебі, қоңыраулардың маршрутизациясы мен VoIP желілеріне FdoS шабуылдары қарастырылып, жоба нәтижелерін қанағаттандыратындай мәндер алынды. Соған сәйкес, Zfone бағдарламасында есептеулер жүргізілді.

Жобаның экономикалық бөлімінде өзін ақтау уақыты есептеліп, уақыты 1.5 жыл болды. Жобаның пайдасы үнемділікте болуы алғы шарты болғандықтан, жобаның келешегі әбден мүмкін және сенімділігі мол.

Өміртіршілік қауіпсіздігі бөлімінде байланыс желілерінде жұмыс істеу кезіндегі еңбек шарттарының талабы, электр қауіпсіздігіне баға беріліп, бөлме желдетуі есептелді. Шешіміне сәйкес, жұмыс орны барлық талаптарға сәйкес болды.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1.Олифер В.Г., Олифер Н.А.Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2006 - 958 с.
2.Кульгин М. Компьютерные сети. Практика построения.СПб.:Питер, 2003,464 с.
3.Дэвидсон Д. и др. Основы передачи голосовых данных по сетям IP. CiscoPress.М.:Вильямс, 2007 – 400с.
4.Меггелен Д., Мадсен Л., Смит Д. Asterisk: будущее телефонии. Символ, 2009 – 656с.
5. Д. Шобар, К. Галекович. «ENGINE – решение для коммуникации речью, данными и мультимедиа». Журнал Revija, том 14–й № 1-2. Загреб, 2002 год.
6. РекомендацияITU – TQ.1901.
7. JanVanGeel. “Bearer Independent Call Control Opens Up New Technological Solutions”.
8. Вестник Связи № 12`03 – «Живой разговор о «NGN» – Глава 1.1.
9. Б.С. Гольдштейн – «IP – телефония». Москва, Радио и Связь, 2003 г
10. А.Г. Барсков – «Сети и системы связи». №9 (73), 2001 г. 86
11. РД 45.129 – 2000 «Телематические службы».
12. РД 45.046 – 99 «Аппаратура связи, реализующая функции передачи речевой информации по сетям передачи данных с протоколом IP».
13. Б. С. Гольдштейн – «Сигнализация в сетях связи». Москва, Радио и Связь, 2001 г.
14. Электронный ресурс, посвященный телекоммуникационному оборудованию – URL: http://www.protei.ru/products/xsm/features/.
15. http://www.uzmzcge.by/_files/news/infogigtrd/04062011.pdf
16. А.Г.Дашковский, М.Э.Гусельников – «Безопасность жизнедеятельности»
17. СанПиН № 1.01.004.01 санитарлық нормалары және ережелері
18. ҚР еңбек қорғау бойынша нұсқамалары
19. Доспаев М., Жандаулетова Ф.Р. Еңбекті қорғау және өміртіршілік қауіпсіздігі негіздері. Алматы, 2008
20. Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д.. Охрана труда на предприятиях связи иохрана окружающей среды. – М.: Радио и связь, 2001
21. Охрана труда и техники безопасности в практической деятельности субъектов Республики Казахстан/Сост. В.И.Скала. – Алматы, 2002
22. Закон РК «О труде в Республике Казахстан». – Алматы, ЛЕМ,2004
23. Чаадаев В.К. Бизнес-процесы в компаниях связи. Эко – Тренз. – М.:2004
24. С.А. Алибаева, К.Б. Базылов. Оқу құралы, Алматы, 2012
25.http://www.bcot.ru/aktualnost_i_osobjennost_ip_tjeljefonii.html
26. http://www.iptelefon.su/
27.http://ippbx.kz/
28.http://www.rgc.kiev.ua/main.php?css=sscc0hr81td0bd0ne0qq

29.http://www.lwcom.ru/solutions/doc.php?do=read&doc=47
30.http://www.cisco.com/web/RU/products/sw/custcosw/callmanager/index.html
31.http://macrotelecom.ru/?p=33
32.http://www.lwcom.ru/solutions/doc.php?do=read&doc=47

А ҚОСЫМШАСЫ

А қосымшасы – IBM System x3250 – негізгі сипаттамалары

Типі	сервер / базалық шығарушы
Корпусы	1U бағанында орнатылған шкаф
Кірілген құрылғылары	USB панелі
Процессоры	1 x Intel Xeon E3120 (макс. 1) - socket 775 - 3.16 ГГц - жүйелікшина: 1333 МГц - Wolfdale (2 ядра) кэшжады: - деңгей 1 • 64 кБ - деңгей 2, бірге қолданылған • 6 МБ Архитектурасының артықшылықтары: - Enhanced Halt State - Execute Disable Bit - Stop Grant state - Streaming SIMD (SSE) - Streaming SIMD Extensions 2 (SSE2) - Streaming SIMD Extensions 3 (SSE3) - Streaming SIMD Extensions 4.1 (SSE4.1) - Virtualization Technology - 64-разрядты жадтың адресациясының технологиясы (EM64T) - MMX технологиясы - SpeedStep жақсартылған технологиясы
Аналық плата	• Intel 3010 • 333 МГц (FSB)
Оперативтіжады	PC6400 DDR2 SDRAM • 2 ГБ (макс. 8 ГБ) • 4 x 240-конт. DIMM (2 бос) • 800 МГц
Сақтау құрылғысының контроллері	RAID контроллері • тұрғызылған ұсынылған интерфейс: Serial Attached SCSI / Serial ATA • 2 канал деңгейі RAID: 0, 1
Қатты дисктер	2 Serial ATA 250 Гб
Оптикалық сақтау құрылғысы	DVD/CD-RW

	• орнату тәсілі: ішкі • интерфейсі: Serial ATA 1.0
Видео	ішкі • ATI ES1000 • PCI • 1024 x 768 • 16 МБ (макс. 16 МБ) DDR SDRAM
Желі	• желілік адаптер • тұрғызылған 2 портты Желі түрі: - Ethernet • (10 Мбит/сек.) - Fast Ethernet • (100 Мбит/сек.) - GigabitEthernet • (1000 Мбит/сек.)
Кеңейтілу анығы	2 x 3.5" (hot-swap) (2 бос) 1 (доступ алдынан) (бос емес)
Слоттар	1 x PCI Express x8 1 x PCI Express x4
Интерфейстер	1 x жалғастырылған • DB-9M (негізгі құрылғы) 1 x VGA • HD-15F (негізгі құрылғы) 2 xEthernet 10/100/1000BaseT • RJ-45 (негізгі құрылғы) 2 xUSB 2.0 • Атипі (артқыпанель) 2 xUSB 2.0 • А типі (алдыңғыпанель)
Ұсталатын желілік стандарттары	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet) - IEEE 802.3z (GigabitEthernet)
Электрқорегі	1 x қоректену блогы • тұрғызылған • 700 Вт • 100 / 240 В (айнымалы тоқ) (макс. 1)
Өлшемі, салмағы	44 x 4.3 x 55.9 см, 12.7 кг

Сервердің шамамен алғандағы бағасы 400000 теңге.