ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Телекоммуникациялық желілер және жүйелер **кафедрасы**

«Қорғауға жіберілді»
Кафедра меңгерушісі
т.ғ.к., профессор Байкенов А.С.
(аты-жөні, ғылыми дәрежесі, атағы)

_____ «____» _____20___ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: IP желілеріндегі виртуалды қосылымдарды пұрсатылатын ІМЕТ-ны ұйымдастыру жобасы

5В071900–Радиотехника,электроника және телекоммуникациялар **мамандығы бойынша**

Орындаған Елмесаева К.Б РЭТ(ИНТ)к-14-1
(аты - жөні) (тобы)

Жетекші аға оқытушы Абиров Д.А
(аты-жөні, ғылыми дәрежесі, атағы, қолы)

Кеңесшілер:

Экономикалық бөлім бойынша:
аға оқытушы Касеева Р.Т
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «16» наурыз 20 18ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
аға оқытушы Бекмуратова Н.С
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «16» наурыз 20___ж.
(қолы)

Есептеу техникасын қолдану бойынша:
аға оқытушы Абиров Д.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «15» 05 20 18ж.
(қолы)

Мөлшер бақылаушы: аға оқытушы Абиров Д.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «15» 05 20 18ж.
(қолы)

Пікір жазушы: „Motorola ТМБх" компаниясының өкілі Букашов Б.Т.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «29» наурыз 20 18ж.
(қолы)

Алматы 2018

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Ғарыштық инженерия және телекоммуникациялар институты
Радиотехника, электроника және телекоммуникациялар мамандығы
Телекоммуникациялық желілер және жүйелер кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Смаилова Куралай Болатқызы
(аты - жөні)

Жоба тақырыбы IP желілеріндегі виртуалды қосылулардың рұқсатталған шектеуді реттеу

ректордың «23» 10. 2017 №155 бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «15» шілде 2018 ж.

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

N=30 тораптар (маршрутизаторлар) саны
n=1,2,...,N
p_1=0,6 Эрл түйінге кешегі нүктеге шақтау
p_2=0,7 Эрл
p_3=0,8 Эрл
μ = 90 c^{-1} пакет қорытқы көрсетудің орташа уақыты
m=1,06 пуск коэффициент

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

Кіріспе
1. IP желісі сипаттамалары
2. IP желілеріндегі рұқсатталған шектеу
3 Есептеу бөлімі
4 Өмір тіршілік қауіпсіздігі
5 Бизнес жоспар
Қорытынды
Қосымшалар тізбесі
Әдебиеттер тізімі

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі:

Виртуалды желіаралықтарды теориялық-қолданылу бөлігі
IP-дестелер түбегі
IP-дестелерді классификациялау
Дестелердің пішіні
Деректер фрагментациясы
IP sec түнелінің қарапайым мысалы
IP sec транспорттық режимінің мысалы
IP sec транспорттық режимінің сызбасы
p=0,6; 0,7; 0,8 әрі белгілерде V1(N) және V2(N) шамдарының N арасындағы тәуелділік графигі

Негізгі ұсынылатын әдебиеттер

1. Олифер В.Г, Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов - СПб.: Питер, 2010
2. Andrew Mason. IPsec Overview. - Cisco Press, 2002
3. Andrew Mason. IPsec Overview, 2002, How IPsec works
4. СанПиН 2.2.2/2.4.1340-03 Общие требования к организации рабочих мест пользователей ПЭВМ
5. Бахтиев К.Б, Алибаева С.А, Нурмаганбетова Е.С. Бітіруші шығарылымы жоғарылығының бойынша ақпараттық-коммуникациялық технологиялар мамандығының студенттеріне арналған АЖБК, 2009.

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
экономика	Косан Р.Т	16.05.2018	
ОЕСТР факультеті	Бекмуратова Н.С	16.05.2018	
Негізгі бөлім	Абдуалиев Д.Н.	15.05.2018	
Мойынша бөлім	Абдуалиев Д.Н.	15.05.2018	
Есептеу-қолдау	Абдуалиев Д.Н.	15.05.2018.	

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Кіріспе	30.01.18	орындалды
2	ІР желісі сипаттамалары	30.01.18	орындалды
3	ІР желі сапасына әсер етуші факторлар	30.01.18	орындалды
4	ІР желілеріндегі рұқсатсыз шектеу	6.02.18	орындалды
5	ІР желілердегі вирусқа қарсы жұмыстар	6.02.18	орындалды
6	Әсерлер болжамы	15.02.18	орындалды
7	Вирусқа қарсы жұмыстарды рұқсатсыз шектеуді тарсорма қатынасы	15.02.18	орындалды
8	Вирусқа қарсы жұмыстардың теория-комплексті үлгісі	15.02.18	орындалды
9	ІР желі хатжасқыдағы тұнжыру эффектінің математикалық үлгісі	1.03.18	орындалды
10.	ІР желі хатжасқыдағы тұрақсыз деректер құрылымы	15.03.18	орындалды
11	ІР желі транспорттық режимде деректің болуы	26.03.18	орындалды
12	Өсіп тұрған жаңылыстың болжамы	25.04.18	орындалды
13	Бизнес жоспар	25.04.18	орындалды
14	Қорытынды	30.04.18	орындалды

Тапсырманың берілген уақыты «12» қаңтар 2018 ж.

Кафедра меңгерушісі _____ т.ғ.к., профессор Байкенов А.С.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

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

Орындалатын тапсырманы қабылдаған студент _____ Ешкеева К.Б
(қолы) (аты -жөні)

Аңдатпа

Берілген дипломдық жобада виртуалды қосылулар жағдайы негізінде IP - желілердегі рұқсаттылықты шектеуді зерттеу қарастырылды. IPsec хаттамасындағы тунельдеу эффектінің математикалық моделі құрылып, IPsec хаттамасымен таратылатын дестелер тобының ұзындығын анықтадық.

Сондай-ақ, өмір тіршілік қауіпсіздік бөлімінде жұмыс бөлмесіндегі радиацияның оптималды деңгейі қарастырылып, экономикалық бөлімде бизнес жоспарға қатысты есептеулер жүргізілді.

Аннотация

В данном дипломном проекте рассматривается исследование ограничения разрешений виртуальной коммутации в IP сетях. Создана математическая модель эффекта тунелирование в протоколе IPsec, а также определили длину группы пакетов, который распространяется по IPsec.

В разделе безопасности жизнедеятельности рассматривается оптимальный уровень радиции в рабочем кабинете, в экономической части произведены расчеты относительно бизнес-плана.

Abstract

This thesis project examines the research of the restriction of virtual switching access in IP networks. A mathematical model of the tunneling effect in The IPSec Protocol is created, and determine the length of the group of packages which is distributed by IPsec.

The optimal level of radiation in the study is considered in the section of life safety, in the economic part of the calculations made with respect to the business plan.

Мазмұны

Кіріспе 7
1 IP желісі сипаттамалары 8
1.1 IP хаттамасы 8
1.2 H.323 хаттамасы 9
1.3 TCP/IP хаттамасындағы шлюздің қызметі 11
1.4 Абоненттердің өзара байланысуы 17
1.5 IP -желі сапасына әсер етуші факторлар 21
1.6 IP-желілердегі адрестеу және маршруттау 32
2 IP- желілердегі рұқсаттылықты шектеу 43
2.1 IP желілеріндегі виртуалды жалғастырулар 43
2.2 Виртуалды байланыс IP-желі қосымшаларының өзара ақпараттық әрекеттесуін сипаттау әдісі ретінде. 48
2.3 IP – желілердегі рұқсаттылықты шектеудің мәселерелін шешудің қолайлы жолдары. 50
3 Есептеу бөлімі 57
3.1 Витруалды жалғастырулардағы рұқсаттылықты шектеуде тапсырма қойылуы 57
3.2 Витруалды жалғастырудың теориялы-көпмүшелі үлгісі 57
3.3 IPsec хаттамасындағы тунельдеу эффектінің математикалық моделі 61
3.4 IPsec хаттамасымен таратылатын дестелер тобының ұзындығын анықтау 63
3.5 IPsec тунельдік режимде дестенің болуы 64
3.6 IPsec транспорттық режимінде дестенің болуы 65
4 Өмір тіршілік қауіпсіздігі бөлімі 68
4.1 Еңбек шартын талдау 68
4.2 Радиацияның өлшем бірліктері 68
4.3 Радиацияны өлшейтін құрылғы 69
4.4 Радиацияның нормалары 72
4.5 Радиация және адам денсаулығы 72
4.6 Радиациядан қорғану 74
4.7 Роутерден сәулеленудің негізгі парамерлері 75
4.8 Компьютерге қойылатын негізгі параметрлер 75
5 Бизнес жоспар 77
5.1 Түйін 77
5.2 Маркетинг жоспары 77
5.3 Ұйымдастыру жоспары 77
5.4 Қаржылық жоспар 77
5.5 Интеллектуалды еңбек бағасы 84
Қорытынды 87
Қысқартулар тізбесі 88
Әдебиеттер тізімі 89

Кіріспе

Интернет технологиясын жасаушылар мынадай екі түсінікті негізге алды: барлық пайдаланушылардың барлық қажеттіліктерін қамтамасыз ететін бірыңғай желі құру мүмкін емес; пайдаланушыларға бір-бірімен байланысу үшін әмбебап әдіс керек.

Белгілі бір физикалық желі шеңберінде қосылған компьютерлер дискреттеу немесе басқа технологияны пайдалану керек (Ethernet, Token Ring, FDDI, ISDN, нүкте-нүкте қосылу типі, соңғы кездері бұл тізімге ATM желісі, Wi-Fi, WiMAX).

Физикалық желілердің мәліметтеріне тәуелді коммуникация механизмдері мен қолданбалы жүйелер арасына әртүрлі физикалық желілердің бір-бірімен байланысын қамтамасыз ететін бағдарламалық қамсыздандыру орнатылады және мұндай жағдайда бұл қосылыстың деталдары пайдаланушылардан жасырын болады және оларға бір үлкен желіде жұмыс жасау мүмкіндігі беріледі. Физикалық желілердің жиынын бұлай қосу әдісі интернет технологиясы деген атауға ие болды. Осының негізінде интернет желісі пайда болды. Интернет желісін құрайтын негізгі хаттама интернет хаттамасы немесе IP хаттама деп аталады. Екі немесе одан да көп желілерді интернет желісінде қосу үшін маршрутизаторлар қолданылады. Маршрутизатор – желілерді бір-бірімен физикалық түрде жалғайтын және арнайы бағдарламалық қамсыздандырудың көмегімен дестелерді бір желіден бір желіге беретін құрылғы.

Интернет технологиясы желіаралық қосылыстарды белгілі бір топологиямен ғана байланыстырмайды.

Интернет желісіне жаңа желінің қосылуы қандай да бір орталық коммутация нүктесіне оның жалғануын немесе интернет желісіне кіруші барлық желілермен тікелей физикалық байланыс орнатуды тудырмайды.

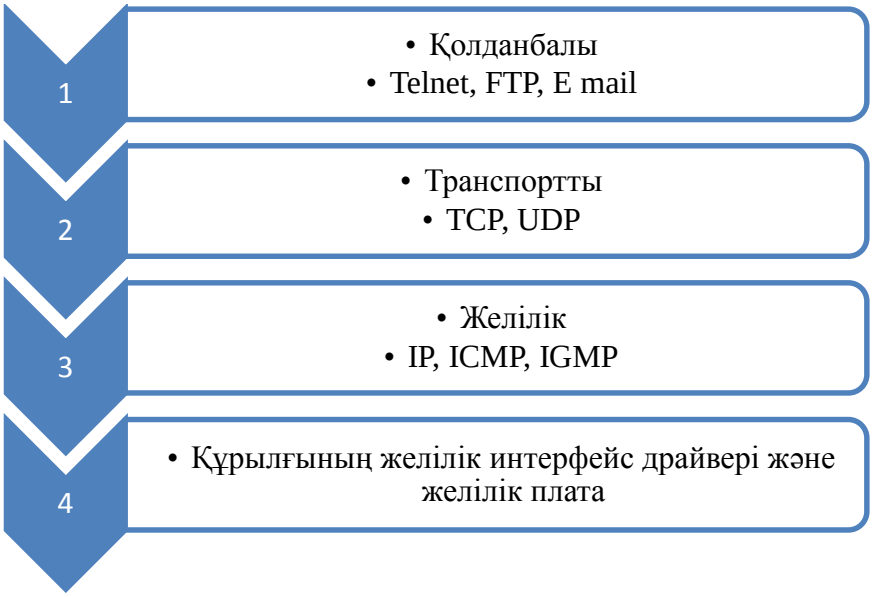
Маршрутизатор өзі байланыстыратын желілер аумағында интернет желісінің топологиясын біледі, осылайша, дестені сол немесе басқа маршрутпен жібереді. Интернет желісінде желіге қосылған компьютерлердің (адрестер) әмбебап идентификаторлары қолданылады, сондықтан кез келген екі машина өзара жұмыс жасай алады. Интернет желісінде сондай-ақ пайдаланушы интерфейсінің желіден тәуелсіз болу принципі жасалуы керек, яғни байланыс орнатудың және деректерді берудің барлық желілік технологиялар үшін бірдей көптеген тәсілдері болуы керек.

Қосылған барлық физикалық желілердің тең дәрежелілігі интернет желісінің негізгі принципі болып табылады. Кез келген коммуникация жүйесі параметрлеріне берілетін дестелердің өлшеміне және географиялық масштабына қарамастан интернеттің компоненті ретінде қарастырылады.

1 IP-желісі сипаттамалары

1.1 IP хаттамасы

Әмбебап интернет желісі TCP/IP хаттамаларының негізінде құрылады және төрт коммуникация деңгейі хаттамаларынан тұрады (1.1-сурет).



1.1 – сурет. TCP/IP хаттамасы түйісінің төрт деңгейі

Желілік интерфейс деңгейі интернет желісі нақты бір физикалық желінің компонентінде байланыс орнату қызметін атқарады. Бұл деңгейде операциялық жүйедегі құрылғы драйвері және осыған сәйкес компьютердің желілік платасы жұмыс істейді.

Желілік деңгей TCP/IP хаттамаларының негізі болып табылады. Бұл деңгейде желі аралық байланыс принципі жасалады, сонымен қатар интернет желісі бойынша дестелерді маршрутизациялау да осы деңгейде жүзеге асады. IP хаттамасы – осы деңгейдің желі аралық байланыс орнататын негізгі хаттамасы болып табылады. Транспорттық деңгейдің TCP және UDP хаттамалары да IP хаттамасын пайдаланады. IP хаттамасы TCP/IP желісімен өтіп жатқан барлық ақпараттардың форматын көрсете отырып, интернет желісінде мәліметтер берудің базалық өлшемі IP дейтограмманы анықтайды. IP желісінің бағдарламалық қамсыздандыруы физикалық желілердің қосылыстары бойынша мәліметтердің жолын таңдай отырып, маршрутизациялау қызметін атқарады. Маршрутты анықтау үшін арнайы кесте болады, таңдау компьютер-адресат қосылған желі адресі негізінде жасалады. IP хаттамасы деректердің әр дестесі үшін бөлек маршрут тағайындайды, бірақ қажетті ретпен сенімді түрде жеткізілуіне кепіл болмайды. Деректерді төменгі орналасқан физикалық деңгейге береді, осылайша дестелерді жеткізудің жоғары эффективті деңгейін жүзеге асырады.

Желілік деңгейде IP хаттамасы жүйелер арасында байланыс орнатпастан желімен дестелерді сенімсіз жеткізу қызметін атқарады. Яғни, дестелерді жеткізу үшін барлық амалдар жасалады, бірақ дестелердің дұрыс жетуіне кепілдік бермейді. Дестелер жоғалуы қате ретпен беріліп немесе қайталануы мүмкін және т.с.с. IP хаттамасы коммуникация сенімділігін қамтамасыз етпейді. Деректер өрісіне тексеру болмайды, тек тақырып үшін бақылау сомасы болады. Деректерді сенімді түрде беруді келесі транспорттық деңгей жүзеге асырады. Транспорттық деңгейдің негізгі хаттамалары TCP және UDP машина-жіберуші мен машина-адресат арасында байланыс орнатады.

Қолданбалы деңгей – төменгі деңгейлердің хаттамаларынан тұратын клиент-сервер типті қосымша. Басқа үш деңгейдің хаттамаларынан айырмашылығы – қолданбалы деңгейдің хаттамалары нақты қосымшаның деталдарымен айналысады, желімен деректерді беру әдістеріне қатыспайды. TCP/IP-дің негізгі қосымшаларының арасында оның әр жұмысына қатысатындары: терминал эмуляциясы хаттамасы TELNET, файлдарды беру хаттамасы FTP, электрондық пошта хаттамасы SMTP, World Wide Web (WWW) жүйесінде қолданатын желіні басқару хаттамасы SNMP, гипертекстті беру хаттамасы HTTP және басқалар.

Ақырғы жүйелер арасында бірнеше ондаған маршрутизаторлар және көптеген әр типті аралық физикалық желілер болуы мүмкін, бірақ қосымша бұл конгломератты бір физикалық желі ретінде қабылдайды. Бұл IP хаттамасы мен Интернет технологиясының негізгі күші мен тартымдылығын көрсетеді.[1]

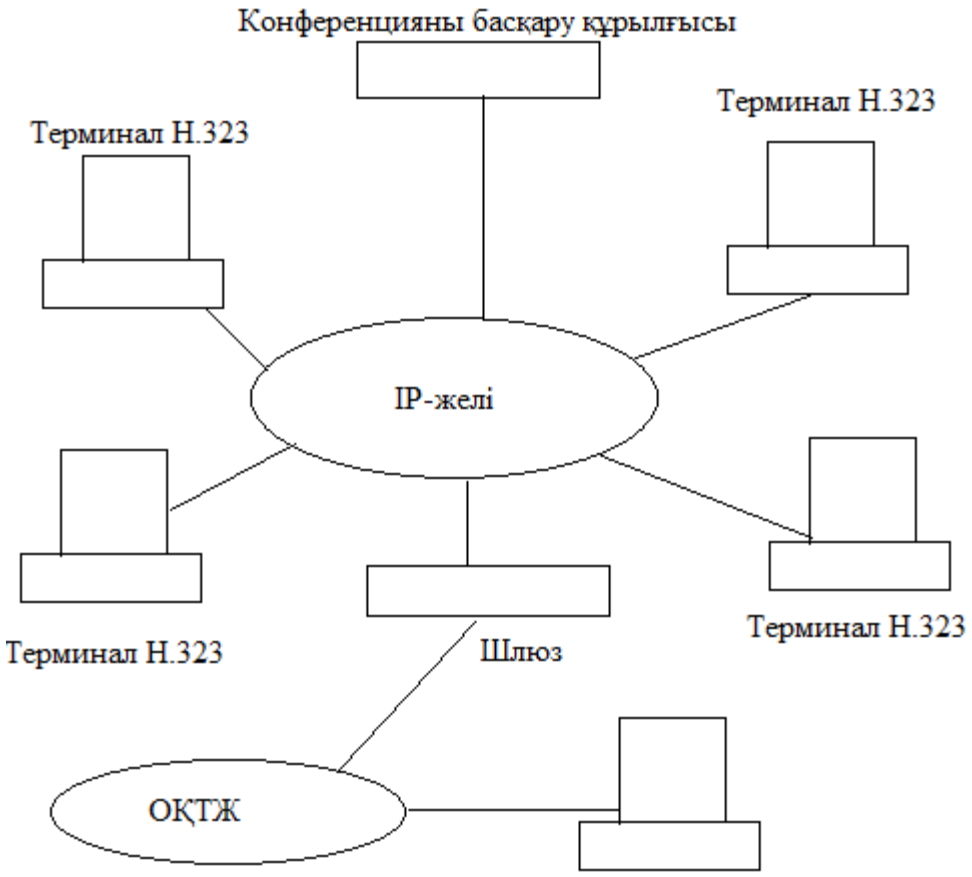
1.2 H.323 хаттамасы

Тарихта стандартты негізде H.323 рекомендациясымен IP-желі желілерін құруға Халықаралық Электрбайланыс Одағы (ITU) бірінші болып қадам жасады. H.323 хаттамасына негізделген желілер телефондық желілерді интегралдауға бағытталған және олар деректерді беру желісіне салынған ISDN желісі сияқты қарастырылады. H.323 рекомендациясы дестелері коммутациялы IP желісімен дауыстық ақпараттарды ғана жіберуге арналмаған хаттамалар жинағын алдын-ала қарастырады. Оның мақсаты желіде мультимедиялық қосымшалардың жұмысын қамтамасыз ету. Дауыстық трафик бейне ақпарат және деректермен қатар H.323-тің қосымшаларының бірі.

IP-желінің H.323 рекомендациясымен желі құру нұсқасы қала аралық және халықаралық байланыс орнатуды көздеген операторларға ыңғайлы. 1.2-суретте H.323 рекомендациялы желінің архитектурасы көрсетілген. Желінің негізгі құрылғылары: терминал, шлюз, аймақ контроллері (қақпақшы) және конференцияларды басқару құрылғысы.

H.323 терминалы нақты уақыт мезетінде желінің басқа терминалмен, шлюзімен немесе көп нүктелі конференцияны басқару құрылғысымен өзара

байланыса отырып, тарату, қабылдау мүмкіндігі бар желінің ақырғы нүктесі болып табылады.



1.2 – сурет. Н.323 желісінің архитектурасы

Бұл функцияларды атқару үшін терминалдың:

– аудио элементтері (микрофон, акустикалық жүйелер, акустикалық жаңғырық басу жүйелері);

– бейне элементтері (монитор, бейнекамера);

– желілік интерфейс элементтері;

– пайдаланушы интерфейсі болуы керек.

IP желісімен дауыс беру технологиясы арналары коммутацияланған классикалық желі орнына шлюздерді қондыру конфигурациясын қарастырады. Шлюз ақпаратты (дауыс) сығып, оларды IP-дестелерге айналдырады және IP-желіге жібереді. Қарсы жақтағы қабылдаған шлюз керісінше амалдарды орындайды: шақыру дестелерін қайта ашады (расшифровка) және қайтадан түзіп (расформирование) шығады. Нәтижесінде қарапайым телефон аппараттары бұл шақыруларды еш қиындықсыз қабылдайды.

Ақпаратты мұндай түрлендіру тәсілі бастапқы дауыстық ақпаратты бұрмаламауы тиіс, ал тарату режимі нақты уақыт масштабында ақпарат алмасуды сақтау қажет.[3]

1.3 TCP/IP хаттамасындағы шлюздің қызметі

Шлюздің негізгі қызметтері:

– телефондық желі мен IP желі арасында физикалық интерфейсті ұйымдастыру;

– абоненттік сигнализация сигналдарын детектірлеу және генерациялау;

– абоненттік сигнализация сигналдарын дестелерге түрлендіру және керісінше орындау;

– абоненттерді жалғау;

– сигнализациялық және дауыстық дестелерді желімен тарату;

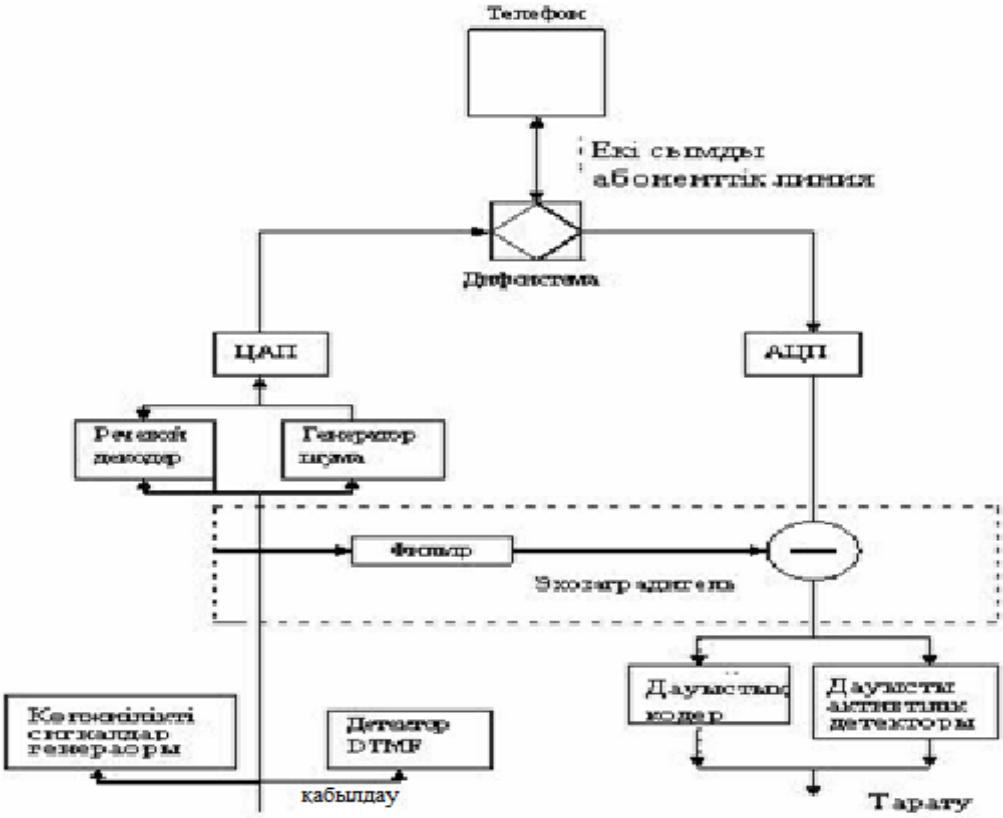
– байланысты ажырату.

TCP/IP архитектурасы шеңберіндегі шлюздің қызметінің көп бөлігі қолданбалы деңгейдегі процестерде ұйымдастырылады. Аналогтық екі сымдық телефондық арна қосылғанда шлюзде сигналдардың өңделуі 1.3-суретте келтірілген. Телефондық сигнал екі сымдық абоненттік желіден арнаның қабылдаушы және таратушы бөлігін айырып тұратын дифференциалдық сұлбаға келіп түседі. Әрі қарай таратылған сигнал қабылдау сигналының сіңген бөлігімен бірге аналогтық-сандық түрлендіргішке (АЦТ) беріледі де, 12-разрядты стандартты сигналға айналады. Соңғы өңдеу жағдайында сәйкес экспандер болуы керек. Жаңғырықты компенсациялау (эхокомпенсация) құрылғысында тарату сигналынан қабылданған сигналдың қалдықтары өшіріледі (жойылады). Жаңғырықты компенсациялау құрылғысы (эхокомпен-сатор) бұл сүзгінің қызметін атқарады. Ішкі жолақтық көп жиілікті телефондық сигнализация сигналдарын (MF сигналдары), жиіліктік (DTMF) немесе импульстік сигналдар жиынын табу және анықтау үшін сәйкес детекторлар типі қолданылады. Кіріс сигналын әрі қарай өңдеу дауыстық кодерде жүзеге асады. Кодердің анализаторында сигнал белгілі бір ұзындықтағы фрагменттерге сегменттеледі (кодтау әдісіне байланысты) және әр кіріс блогына сәйкес ұзындықтағы ақпараттық кадр қойылып шығады.

Кодер анализаторында есептелген параметрлер бөлігі дауыстық белсенділікті анықтау блогында қолданылады. Дауыстық белсенділікті анықтау блогы зерттелініп жатқан сигнал дауыс па, әлде үзіліс екендігін анықтайды.

Үзіліс болған жағдайда ақпараттық кадр виртуалды арна қызметіне жіберілмей қалуы мүмкін. Сеанстық деңгейге әр бесінші үзілістік ақпараттық кадр ғана жіберіледі. Дауыс жоқ болған жағдайда ағымдағы спектрлік параметрлерді кодтау үшін ең қысқа ақпараттық кадр қолданылады. Виртуалды арнаның қабылдаушы жағында логикалық амал орындаушыға ақпараттық кадр немесе үзілісті білдіретін жалауша келіп түседі. Үзілістік

кадрларда дауыстық интезатор орнына үзілістік сигналдың спектралдық құрамын қалпына келтіретін комфорттық шу генераторы қосылады. Үзілістік ақпараттық кадр алынғанда сигналдың параметрлері жаңаланады. Ақпараттық кадрдың болуы шығысында дауыстық сигнал түзетін дауыстық декодерді іске қосады. Эхокомпенсатор үшін қашықтағы абоненттің сигналы болып табылады, бұл сигналдың сүзгіленуі таратылатын сигналдағы электрлік жаңғырықтың құраушысын береді. Сандық-аналогтық түрлендіру түріне байланысты сигнал қосымша кодтауға ұшырауы мүмкін.



1.3 – сурет. Шлюзде сигнал өңдеу сұлбасы

Сигналдардың шлюзде сандық өңделуінің мынадай қиындықтарын атауға болады: екі сымдық абоненттік желілерді қолданғанда негізгі жұмыс болып эхокомпенсация болып қала береді, өйткені оның ерекшелігі мұнда сигналдардың екі класын – дауыс сигналдарын және телефондық сигнализация сигналдарын компенсациялау қажет. Телефондық сигнализация сигналдарын тауып, детектирлеу өте маңызды жұмыс болып табылады. Оның қиындығы: қызметтік сигналдар дауыс сигналдарымен араласып кетуі.

Аймақтың контроллерінде (қақпақшада) IP-желінің барлық интеллекті шоғырланған. H.323 рекомендациясы бойынша құрылған желінің зоналық архитектурасы бар. Аймақтың контроллері IP-желі желісінің бір аймағын басқару функциясын орындайды, мұндай аймаққа терминалдар, шлюздер, бір аймақ контроллеріне тіркелген конференцияларды басқару құрылғысы кіреді.

Н.323 желісі аймағының бөлек фрагменттері территориямен бөлінген және олар маршрутизаторлар арқылы бір-бірімен байланыса алады.

Аймақ контроллерінің маңызды қызметтері:

– ақырғы және басқа құрылғылардың тіркелуі;

– пайдаланушылардың RAS сигнализациясының көмегімен IP-желі қызметтеріне кіріп қосылуын бақылау;

– шақырылған пайдаланушының alias адресін IP дестелерді

– маршрутизациялау (IP адрес – TCP порты номері) желісінің транспорттық адресіне түрлендіру (абоненттің жарияланған есімін, телефондық номерді, электрондық пошта адресін және т.б.);

– желінің өткізу жолағын резервтеу, басқару және бақылау;

– терминалдар арасында Н.323 сигналдық хабарларын ретрансляциялау.

IP-желінің бір желісінде ITU Н.323 талаптарына жауап беретін өзара RAS хаттамасы арқылы байланысатын бірнеше аймақ контроллерлері болуы мүмкін.

Конференцияларды басқару құрылғысы (MCU) үш немесе одан да көп қатысушылар арасында байланыс ұйымдастыруды қамтамасыз етеді. Н.323 рекомендациясы конференцияның үш түрін қарастырады: орталықтандырылған (яғни MCU арқылы басқарылатын, әр қатысушы нүкте-нүкте режімінде қосылған), орталықсыздандырылғын (әр қатысушы қалған басқа қатысушылар мен нүкте-нүктелер тобы режімінде қосылған) және аралас. Конференцияны басқару құрылғысы конференцияның бір міндетті элементі конференция контроллерінен (MC) тұрады және бір немесе бірнеше ақпаратты өңдеу процессорынан (MP) тұруы мүмкін. MC аймақ контроллерімен, шлюзбен, конференцияны басқару құрылғысымен бірігуі мүмкін.

Н.323 желісінің прокси-сервер деген тағы бір элементі, яғни сервер-делдал (посредник). Бұл сервер қолданбалы деңгейде жұмыс істейді және екі қосымша арасында алмасатын ақпаратты дестелерді бақылай алады. Прокси-сервер шақыру қай қосымшамен қосылғандығын анықтап, қажетті қосылысты жалғайды.

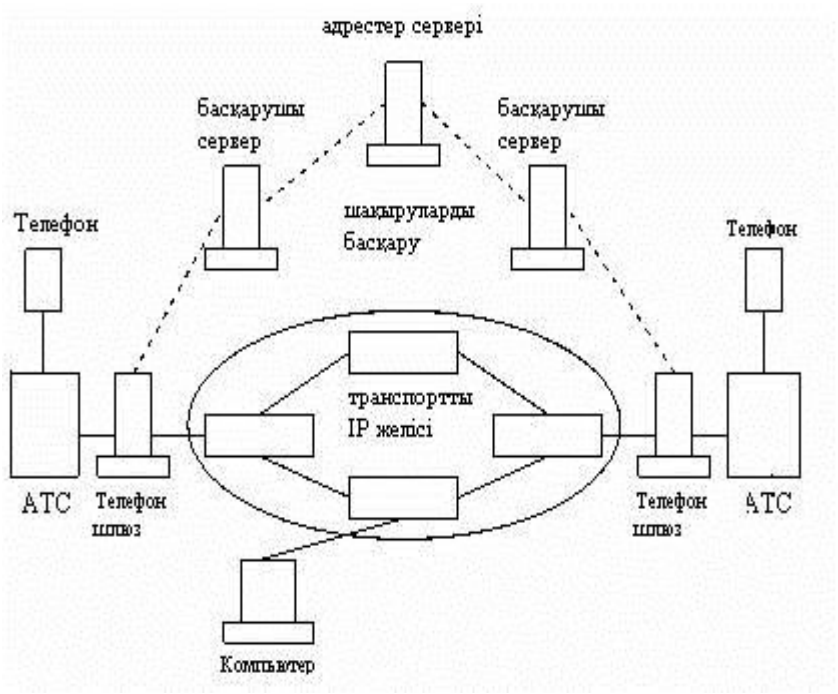
Н.323 хаттамалар тобының негізгі үш хаттамасы бар: ақырғы құрылғының RAS қақпақшасымен өзара байланысу хаттамасы, Н.225 қосылыстарын басқару хаттамасы және Н.245 логикалық арналарын басқару хаттамасы.

Халықаралық Электрбайланыс Одағы Н.225.0 хаттамасында Н.323 желісі компоненттерінің өзара әрекеттесу хаттамасын анықтады: ақырғы құрылғының (терминалдар, шлюздер, конференцияны басқару құрылғысы) қақпақшамен. Бұл хаттама RAS деп аталды (Registration, Admission and Status)[5].

Дәстүрлі желіда шақырушы, қолданушы керекті абоненттің номерін тереді, ал телефондық желіні шақырудың маршруты ретінде қолданады. Шақыруды басқару үрдісі үш кезеңге (фазаға) бөлінеді: байланысты

ұйымдастыру, дауысты беру және ажырату. Сигнализация жүйесінің хабары бұл фазаларды ұйымдастырады, ал стандартты бақылау сигналдары және жазылған дауыстық хабарлар абонентті өз шақыруының өту сипаттамалары туралы хабардар етіп отырады.

IP-желі жүйелерінде шақыруларды басқару үрдісі сигнализация хаттамалармен орындалады.



1.4 – сурет. IP-желіде шақыруларды басқару

IP-желідағы маңызды сұрақ – жүйеге қатынауды бақылау. Жалпы қолданыстағы телекоммуникация желілеріндегі абонент белгіленген жергілікті шлейф арқылы АТС-қа қосылады, сондықтан телефондық аппаратты анықтау өте оңай. IP-желі желісінде барлығы күрделі, себебі оған қатынаудың көптеген түрлері бар:

– ортақ қолданыстағы телекоммуникация желілері (СТОП) арқылы жай телефонмен;

– модемдік байланыс арқылы қашықтықтағы нүктенің сервері арқылы жалғастыру;

– ЛЕЖ (LBC) арқылы және территориялды бөлінген желі арқылы.

Жалпы жағдайда шақырушы және шақырылушы абоненттер арасындағы байланысты ұйымдастыруда IP-желі шлюзі мынадай болуы керек:

– ақырғы құрылғы тіркелуі мүмкін аймақ контроллерін табу;

– аймақ контроллерінде өз мнемоникалық адресін тіркеу;

– керекті өткізу жолағын көрсету;

– жалғауды ұйымдастыру;

– шақыру процесі кезінде жалғау параметрлерін басқару;

– жалғауды ажырату.

Жалғаудың ұйымдастыру, ұстап тұру және бұзу алгоритмдері.

Жалпы жағдайда жалғауды ұйымдастыру, ұстап тұру және бұзу алгоритмдері H.323 бойынша өзіне келесі фазаларды біріктіреді[4]:

– A фазасы. Жалғауды ұйымдастыру;

– B фазасы. Жүргізуші құрылғыны анықтау және функционалды мүмкіндіктер туралы деректермен алмасу;

– C фазасы. Шақырушы және шақырылушы абоненттер арасында аудиовизуалды байланысты ұйымдастыру;

– D фазасы. Өткізу жолағын өзгерту, құрылғының осы сәттегі жағдайы туралы хабар алу, конференцияны ұйымдастыру және қосымша қызметтерге бет бұру.

Аймақ контроллерінің қатысуы арқылы базалық жалғауды ұйымдастыру жүргізіледі: шақырушы құрылғы alias адресті ARQ хабарын шақырылушы абонентке береді, жауап ретінде аймақ контроллері ACF хабарын қайтарады. Келген хабарда аймақ контроллері сигналдық хабарды өзі басқаратыны туралы және өзінің сигналды каналының транспортты адресін көрсетеді. Ары қарай шақырушы құрылғы осы транспорттық адреске Setup (жалғауды) жалғау туралы сұрау жібереді. Аймақ контроллері Setup хабарын шақырушы абонентке қайта жібереді және шақырылушы абонентке Call Proceeding хабарын, яғни алынған мәлімет келген шақыруға қызмет етуге жететіндігі туралы хабарын береді.

Шақырылған абонент Setup–қа Call Proceeding хабарымен жауап береді. Егер құрылға шақыруды қабылдауға мүмкіндігі болса, ARQ желісінің ресурстарына жіберу туралы сұрау жібереді. Бұл сұрауға аймақ контроллері ACF бекітуімен жауап беруі мүмкін немесе ARQ желісінің ресурстарына жібермеуі туралы хабар береді. Бірінші жағдайда шақырылатын құрылғы Alerting (дайындыққа келу) хабарын жібереді және аймақ контроллері оны шақырушы құрылғыға маршуруттайды. Шақырылатын құрылғыға кіруші шақырыс ретінде визуалды немесе акустикалық сигнал беріледі, ал шакырушыға шақырылып жатқан құрылғының бос екендігі туралы белгі ретінде шақырушы сигнал беріледі. Желі ресурстарына қатынауға болмайтын кезде шақырушы құрылғы өзінің сигналды арнасын аймақ контроллеріне Release Complete (босату) хабарын береді.

Шақырылған қолданушы кіріс шақыруды қабылдаған соң, аймақ контроллеріне шақырылатын құрылғының басқарушы H.245 каналының транспорттық адресімен Connect хабары беріледі. Контроллер бұл адресті өзінің басқарушы H.245 арнасының транспорттық адресімен алмастырады және Connect хабары шақырушы құрылғыға береді, осыдан соң басқарушы H.245 арнасы ашылады[5].

Сөйлесу сессиясын жылдамдату үшін басқарушы арна шақырылушы құрылғымен ашылуы мүмкін. Бұл тек шақырушы құрылғы немесе аймақ контроллерінің басқарушы H.245 арнасының транспорттық адресімен

берілетін Setup хабарын алған соң болады немесе шақырушы қолданушымен аймақ контроллерінің немесе шақырылушы қолданушының басқарушы H.245 каналының транспорттық адресіне ие Call Proceeding немесе Alerting хабарымен іске асады.

Басқарушы H.245 каналының ашылуынан кейін құрылғының функционалды мүмкіндіктері туралы деректермен алмасады. Біздің жағдайда бір ақырғы құрылғыдан екіншісіне берілетін басқарушы хабарлар аймақ контроллерімен маршрутталады. Терминал Terminal Capability Set (қабілеттіліктерді терминалды теру) хабарларымен алмасады, оларда қабылданатын информацияның декодалануының мүмкін болатын алгоритмдері көрсетіледі. Terminal Capability Set хабары басқарылушы арнамен берілетін хабарлардың біріншісі болуы керек. Басқа бір құрылғыдан Terminal Capability Set хабарын қабылдаған құрылғы, бұл хабарды алғаны туралы растау ретінде Terminal Capability Set Ack хабарын жібереді.

Сонан соң жетекші/жетектегі құрылғыларды анықтау процедурасы ұйымдастырылады. Бұл конференция кезінде екі құрылғы арасында болатын келіспеушілікті шешуге қажетті. Олар конференцияның активті контроллерлері болуы мүмкін немесе бір уақытта екі бағытты логикалық арналар ашуға тырысады. Процедура барысында құрылғылар master Slave Determination (бастыны анықтау) хабарларымен алмасады. Алынған хабарларға (mSD) жауап ретінде екі құрылғыда mSDAck хабарларын, яғни қай құрылғы жетекші немесе жетектегі екенін білдіретін хабарлар жібереді. mSD хабарын беріп, mSDAck хабарын алған құрылғы mSDAck хабарын таратады. Функционалды мүмкіндіктері туралы деректермен алмасып және жетекші немесе жетектегі құрылғыны анықтаған соң, бір бағыттағы логикалық арналар процедурасы орындалуы мүмкін. Open LogicalChannel арнасын ашу талабында құрылғы осы арна бойынша таратылатын ақпарат түрін және кодтау алгоритмін көрсетеді. Логикалық арна дауысты тасу үшін қолданылады, сондықтан Open Logical Channel хабарында RTCP арнасының транспорттық адресі көрсетілетін media Control Channel параметрі қосылады. Оның көмегімен RTP дестелерді бақылайды. Open Logical Channel хабарына жауап ретінде құрылғының транспорттық адресі көрсетілетін OpenLogicalChannelAck дейтін растау жібереді. Оған таратушы жақтан RTP дестесі, сонымен қатар RTPC арнасының транспорттық адресін жіберуі керек.

Әрі қарай сөйлесу сессиясы ашылады. Шақырушы қолданушының құрылғысы RTP/UDP/IP дестелері түріндегі дауыстық мәліметтерді шақырылған қолданушының құрылғысына RTP арнасының транспорттық адресіне береді. Ал шақырылған қолданушы дестеленген дауыстық мәліметтерді шақырылған қолданушы құрылғысының RTP арнасының транспорттық адресіне жібереді. RTCP арнасының көмегімен RTP арналары бойынша мәліметтерді тарату бақыланады.

Сөйлесу фазасы аяқталған соң байланысты бұзу фазасы басталады. Тұтынушы құрылғысы дауыстық мәліметтерді беруі тоқтатуы керек, логикалық арналарды жабу және басқарушы H.245 арнасына тұтынушы

байланысты аяқтағысы келетіні туралы end Session Command (сессияның аяқталуы туралы команда) хабарын береді. Сонан соң қарсы құрылғыдан end Session Command хабарын күтеді, оны қабылдаған соң басқарушы H.245 арнасы жойылады. Бұдан әрі, егер сигналды арна ашық болса, онда Release Complete хабары беріледі.

Үзуді ынталанған қолданушы жіберген end Session Command бұйрығын алған қолданушы дауыстық мәліметтерді тоқтатуы, логикалық арнаны жабуы және end Session Command хабарын беру керек. Ары қарай, егер сигналды арна ашық болса, Release Complete хабары беріледі және сигналды арна жабылады.

Бұл әрекеттердің барлығы аяқталған соң ақырғы құрылғы аймақ контроллеріне иеленген өткізу жолағының босағандығы туралы хабарлайды. Осы мақсатпен әрбір байланысқа қатысушы RAS арнасы бойынша DRQ байланысынан шығу туралы сұрау жібереді. Бұған аймақ контроллері DCF растауымен жауап беруі керек, бұдан соң шақыруға қызмет көрсетілу аяқталды деп есептеледі[3].

1.4 Абоненттердің өзара байланысуы

IP жүйесіндегі екі абонентті қарапайым түрде жалғау үшін әрбір ақырғы бөлікте біруақытта тарату функциясы әрі қабылдау функциясы ұйымдастырылады. IP желі деп ғаламдық IP желіні немесе деректерді таратудың корпоративтік желісі ретінде түсінуге болады.

А және Б абоненттері бір-бірімен сөйлесуі үшін интернетке немесе басқа бір желіде IP хаттамасымен шығуы керек. Осы абоненттер арасындағы байланысты ұйымдастыру алгоритмін қарастырайық:

– А абонентінің құрамында H.323 хаттамасы бар өзінің IP-желі қосымшасын жібереді;

– Б абоненті H.323 хаттамасы бар IP-желі қосымшасын бұрынырақ жібереді;

– А абоненті Б абонентінің домендік атын біледі, әрі осы атты өздерінің IP-желі қосымшасындағы “кімге соғу” бөліміне енгізеді және Return түймесін басады;

– IP-желі қосымшасы Б абонентінің домендік атын IP адресіне айналдыру үшін DNS серверге жүгінеді;

– DNS сервері Б абонентінің IP адресін қайтарады;

– А абонентінің қосымшасы Б абонентінің IP-желі адресін алады және оған H.225 Setup хабарын жібереді;

– H.225 Setup хабарын алған уақытта Б абоненті оған кіріс шақыру туралы сигнал береді.

– Б абоненті шақыруды қабылдайды және IP-желі қосымшасы H.225 Connect жауаптық хабарын жібереді;

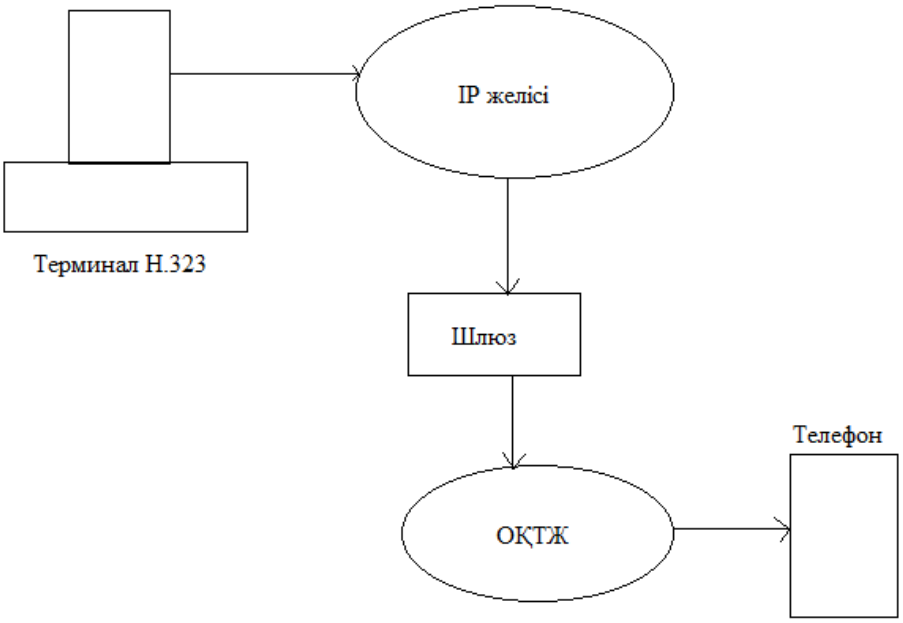
– А абонентінің IP қосымшасы H.245 рекомендациясына сәйкес Б абонентінің қосымшасымен өзара әрекеттеседі;

– Н.245 хаттамасы бойынша өзара әрекеттер аяқталған соң және логикалық арналардың ашылуынан соң А және Б абоненттері IP желісі арқылы сөйлесе алады[7].

«Компьютер-телефон» сценариі мәлімет – ақпараттық сүйеу қызметтерінің әр түрлерінде қолданыс тапты. Бұл IP-желі модификациясының екі сценариін қарайды:

– компьютерден (IP желіні қолданушы) телефонға (ОҚТЖ абонентіне), жекелей түрде, IP желісін қолданушыларға телефондық қызмет көрсету, оның ішінде мәлімет – ақпараттық қызметтерге және интеллектуалды желі қызметтеріне;

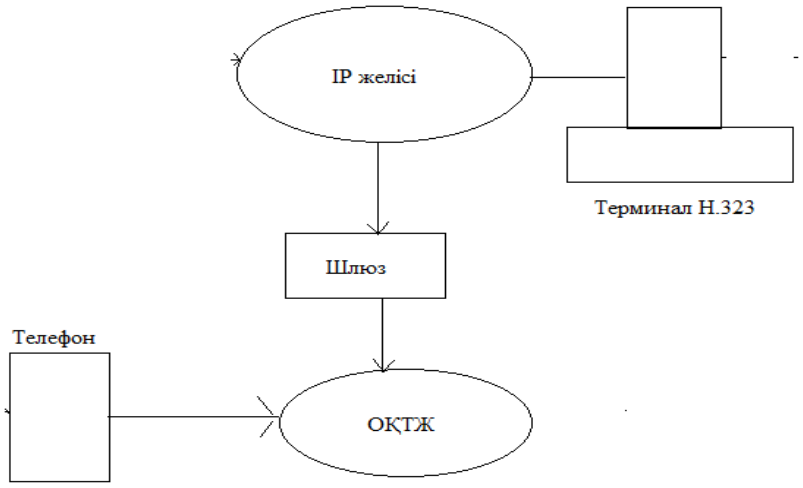
– ОҚТЖ абонентінен IP желісінің қолданушысына, яғни шақырылатын жақтың екі нөмірлік Е.164 немесе IP адресациялары негізіндегі идентификациясымен. Бірінші модифифкацияда «компьютер – телефон» сценариінде IP желісін қолданушы мен коммутация арналары жүйесінің қолданушысы арасында ұйымдастырылады (1.5-сурет).



1.5 – сурет. ОҚТЖ абонентінің IP желісін қолданушыға шақыруы

Байланысты ұйымдастыруға IP желісін қолданушы ынталы деп есептейік. ОҚТЖ (СТОП) және IP желілерінің өзара әрекеттесуі үшін керекті шлюз жеке құрылғыда жасалуы немесе ОҚТЖ (СТОП) және IP желісі құрылғыларында интеграцияланған.

«Телефон - компьютер» сценариі бойынша жасалған IP-желі жүйесі құрылымының қарапайымдатылған мысалын толық түрде қарастырып көрейік.

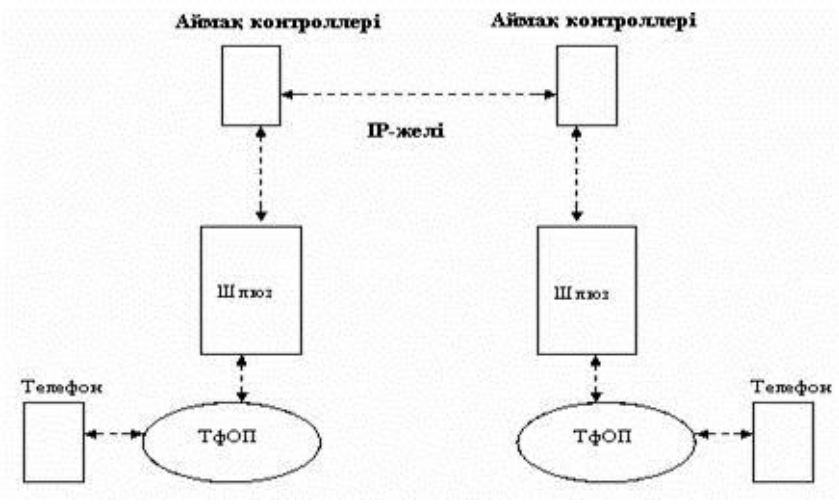


1.6 – сурет. IP желісін қоданушы ОҚТЖ абонентін шақыруы

Алғашқы фазада мәліметті-ақпараттық қызметті шақыру әрекеті кезінде дестелі желі немесе қарапайым телефон қызметтерін қолдана отырып, А абоненті IP-желінің жақын жердегі шлюзін шақырады. Шлюзден А абонентіне шақырылуы керек абоненттің нөмірін теру туралы сұрау түседі. Сонымен қатар аутентификация үшін керек идентификациялық нөмір (PIN) және бұл қызмет шақыруға шақырушы абонентпен ақы төленетін болса, онда төлеудің келесі есептеулері келеді. Шлюз шақырылатын номерге негізделе отырып берілген қызметке ең қолайлы жолды анықтайды. Бұдан басқа, шлюз өзінің дауысты кодтау және дестелеу функцияларын активизациялайды, шақырылуға қызмет көрсету процесіне мониторинг жүргізеді және бұл процес (үзу шақырысы посылкасының бос еместігі) туралы мәліметтерді шығушы жақтан басқару және сигнализациялау хаттамалары арқылы қабылдайды. Кез келген жақтан үзілу сигнализация хаттамасы бойынша қарсы жаққа беріледі, орнатылған байланыстарды аяқтауды шақырады және келесі шақыруға қызмет көрсету үшін шлюздің ресурстарын босатады.

Келесі «телефон - телефон» сценариі IP-желінің басқа сценарилерінен айрықшаланады, себебі оның мақсаты қарапайым ОҚТЖ (СТОП) абоненттеріне қалааралық және халықаралық телефон байланысының альтернативтік мүмкіндіктерін беру болып табылады. Бұл режімде IP-желінің қазіргі технологиясы IP қатынау арқылы виртуалдық телефондық линияны пайдалануға береді.

IP-желінің мұндай сценариі бойынша шақыруларға қызмет көрсету келесі түрде жүреді. IP-желі қызметін жеткізуші өз шлюзін коммутациялық торапқа немесе ОҚТЖ (СТОП) станциясына қосады, интернет желісі бойынша немесе бөлінген арна арқылы басқа бір қалада немесе елде орналасқан ұқсас шлюзбен жалғанады (1.7-сурет).



1.7 – сурет. ОҚТЖ (СТОП) абонентінің транзитті
IP желісі арқылы жалғануы

IP желі қызметін жеткізушілер «телефон-телефон» қызметін беруді IP желі шлюздерін IP желінің кірісіне және шығысына орнату арқылы жүзеге асырады. Абоненттер арнайы қатынау нөмерін тере отырып ОҚТЖ арқылы жеткізушінің шлюзіне қосылады. Абонент дербес идентификациялық номерін (PIN) немесе шақырушы абонент нөмерінің идентификация қызметін қолдана отырып шлюзге рұқсат алады. Бұдан соң шлюз шақырылатын абоненттің телефон нөмерін енгізуді сұрайды, оны талдап және шлюздердің қайсысы телефонға ең тиімді қатынай алатынын анықтайды. Кіріс және шығыс шлюздердің арасында байланыс орнатылысымен, ары қарай шақырылатын абонентке байланысты шығыс шлюздің жергілікті желісі арқылы орындалады[11].

IP желісі арқылы байланысты орнату үшін А абоненті IP-желі қызметін жеткізуші шлюздің жергілікті телефон нөмерін тереді. А абонентіне станцияның екінші жауап сигналы беріледі және шақырылатын абоненттің нөмерін теруін сұрайды. Әрі қарай Б абоненті жағынан байланыс орнатылады. IP-желінің «компьютер – компьютер» және «компьютер – телефон» сценариін қолдануының негізгі стимаулы болып дауысты және деректерді берудің тиімділігі болып табылады.

Дәстүрлі телефондық жүйелері электр сигналдарын дауыстық спектр сигналдарын беруге жетерліктей кепілдік беретін өткізу жолағымен жалғайды. Берілетін сигналдың бекітілген өткізу қабілеті үшін уақыт бірлігінің шамасы шақыру нүктесінің және жауап беру орнының алыстығына және орналасуына байланысты.

Дестелерді жалғау желісі кепілдік етілген өткізу жолағын қамтамасыз етпейді, себебі байланыс нүктелері арасындағы кепілдік етілген жолды қамтамасыз ете алмайды.

Дестелердің келу интервалы мен реті маңызды емес қосымшаларда (электрондық пошта) жеке дестелер арасындағы кідіру уақыты шешуші

мағынаға ие емес. IP-желі деректерді тарату аумақтарының бірі болып табылады, онда қазіргі әдістермен кодтау және мәліметтерді таратуды қамтамасыз ететін сигналдарды беру динамикасы маңызды, сонымен қатар арналардың өткізу қабілетінің ұлғайуы да.

1.5 IP -желі сапасына әсер етуші факторлар

IP-желінің сапасының негізгі құраушылары болып дауыс және сигнализация сапасы болып табылады. Дауыс сапасы келесілерді біріктіреді:

– диалог немесе қолданушының реалды уақытта және толық дуплексті режімде бір-бірімен байланысуы және сөйлесуі;

– дауыстың айқындылығы, тазалығы және тоналдығы;

– меншікті дауыстың жаңғырықпен естілуі;

– дауыстың деңгейі немесе дауыстылығы.

Сигнализация сапасы келесілерді біріктіреді:

– шақыруды орнату немесе табысты қатынау жылдамдығы және жалғауды орнату уақыты;

– шақырыстың аяқталуы немесе бас тарту уақыты және үзу жылдамдығы;

– көпжиілікті нөмір теру сигналдарының анықталуы немесе DTMF сигналдарды бекіту.

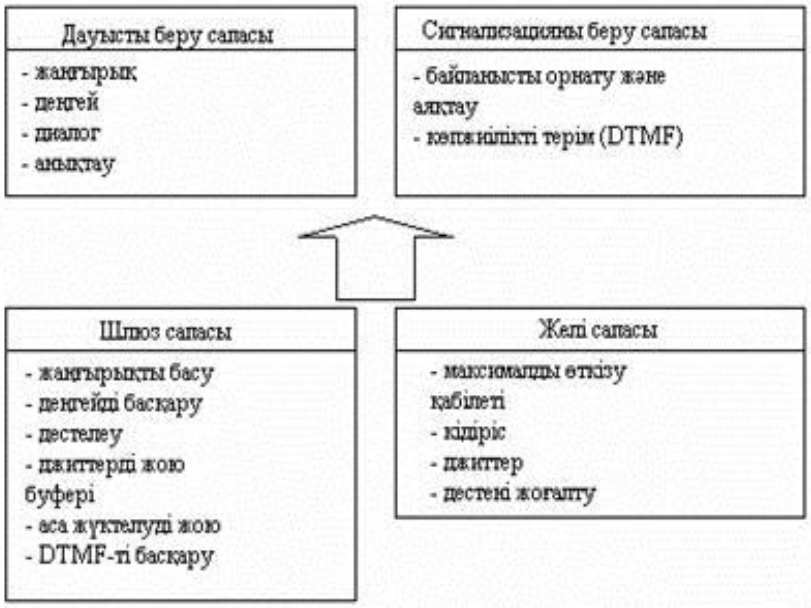
IP-желі сапасына әсер етуші факторлар екі категорияға бөлінуі мүмкін:

– максималды өткізу қабілеті немесе берілетін деректердің пайдалы және артық максималды саны;

– желі арқылы дестелерді беруге қажетті кідіру немесе уақыт аралығы;

– тізбектелген екі десте арасындағы джиттер немесе кідіріс;

– желі арқылы таратуда жоғалған дестелер немесе дестелер жоғалуы.



1.8 – сурет. IP-желі сапасына әсер етуші факторлар

Шлюз сапасының факторлары:

– қажетті өткізу жолағы немесе әртүрлі кодерлер, әртүрлі жолақты керек етеді;

– дауыстық сигналдарды өңдеу үшін сандық процессорға немесе басқа құрылғыларға керекті кідіріс немесе уақыт;

– барлық дестелер алынып болғанша деректер дестелерін сақтау немесе джиттер буфері және джиттерді минимизациялау үшін керекті тізбекті беруге болады;

– дестелердің жоғалуы немесе IP-желі құрылғысында дестелерді беру немесе қысу кезіндегі дестелердің жоғалуы;

– желі бойынша тарату кезінде пайда болатын жаңғырықты басу немесе жаңғырықты басушы механизм;

– деңгейді басқару немесе дауыс қаттылығын бақылау мүмкінділігі.

Кідіріс диалогты енгізгенде қолайсыздықтар туғызады, сөйлесулердің бірін-бірі жабуы және жаңғырықтың пайда болуы. Шағылған дауыстық сигнал сигналмен бірге алыстағы соңынан сөйлеушіге қайта оралуы жаңғырықтың пайда болуына әкеледі. Тарату бөлігіндегі кідіріс 50 мс-тан көп болғанда, жаңғырық қиын проблемаға айналады.

Бір бағыттағы кідіріс 250 мс-тан асып кеткенде, диалогтың қиындауы және сөйлесулердің бірін-бірі жабуы сапаның маңызды сұрағына айналады.

Бір соңынан екінші соңына дауысты беру кезінде кідіріс көздерінің келесі түрлерін көрсетуге болады:

– жиналу кідірісі (алгоритмтік кідіріс): бұл кідіріс дауыстық кодерде орындалатын дауыстық кадр санақтарын жинау қажеттілігімен шартталған;

– өңдеу кідірісі: анықталған кідірістерді кодтау процесінде және дестелік желі арқылы тарату үшін кодталған санақтардың дестеге жиналуында пайда болады.

1.9 – сурет. IP-желі желісіндегі кідірістердің құраушылары

Желілік кідіріс: кідіріс физикалық орта және хаттамалармен шартталған, сонымен қатар қабылдау соңындағы джиттерді жою үшін қоданылатын буферлермен. Желілік кідіріс желі сыйымдылығына және желідегі процестерге тәуелді.

Кідіру уақытын үш деңгейдің біреуіне жатқызуға болады:

– бірінші деңгей 200 мс-қа дейін байланыстың өте жақсы сапасы. Салыстыру үшін, ОҚТЖ-ға рұқсат етілетін кідіріс 150, 200 мс;

– екінші деңгей 400 мс-қа дейін байланыстың жақсы сапасы. Бірақ ОҚТЖ-мен салыстырғанда айырымы елеулі;

– үшінші деңгей 700 мс-қа дейін маңызды емес сөйлесуге жарайтын байланыс сапасы. Мұндай байланыс сапасы жерсеріктік байланыста да болуы мүмкін.

Деректерді IP желісі арқылы таратуда өте жиі дестелейді, дестелер жиі әртүрлі уақыттарда және әртүрлі реттерде келіп түседі. Бұл дестелерді (джиттерлерді) жеткізудің уақытты таралуын пайда қылады. Джиттер дауысты тарату кезінде сатыр-сұтырлар және шертулер түрінде естілетін бұзылуларға әкеледі. Джиттердің үш түрін ажыратуға болады:

– деректерге тәуелді джиттері өткізу жолағы шектелгенде немесе желі бұзылғанда пайда болады;

– жұмыс циклының бұрамалануы төменнен жоғарыға және жоғарыдан төменге беру арасындағы таралулар кідірісімен шартталған;

– кездейсоқ джиттер жылулық шудың нәтижесі болып табылады.

IP-желідегі жоғалған дестелер дауысты бұзады және темір бұрмалануын пайда қылады. Барлық дауыстық кадрлар деректер ретінде өңделеді, сондықтан дауыстық кадрлар шыңдық жүктемелерде басқа да деректер кадрлары сияқты алынып тасталады. Деректер кадрлары уақытпен байланысты емес, және тасталған кадрлар қайталану жолымен табысты түрде берілуі мүмкін, ал дауыстық дестелердің жоғалуы мәліметтің толық емес жоғалуына әкеледі. 5%-ке дейінгі шығындар білінбестей, ал 10-15%-тен жоғары рұқсат етілмейтін болып есептеледі. Трафиктің жоғарылауымен арнада кідірістер мен жоғалулар өсуі мүмкін деп ұйғаруға болады.

IP-желіде сапалы дауыстық сигналдарды беруді қамтамасыз ету үшін келесідей өңдеулер қажет:

а) кіріс аудиосигналдан барлық жағымсыз компоненттерді алып тастау. Дауысты цифрлаған соң микрофон динамигінен жаңғырықты, бөлмелік жаңғырықты және фондық шуылды, сонымен қатар дауыстық спектрдегі төменгі жиіліктегі айнымалы тоқтағы шуылдарды сүзгілеу. Бұл функциялар дербес компьютердің аудиокомпоненттерімен жүзеге асырылады, сондықтан IP-желі жүйесі мұндайды иеленбеуі мүмкін;

б) дауыстағы кідіруді (паузаны) басу; қалдықты фондық шуылды (сыртқы шуылдарды) айқындау және ең алыс ақырғы бөлікте қалпына келтіру үшін кодтау. Жақын ақырғы бөліктегі үзілістерді толығымен жойған дұрыс. Алыстағы соңғы бөлікте қалпына келтіру үшін DTMF сигналдарын және

басқа да сигналдарды қысқа кодтарға айырбастау керек. Дауыс қаттылығы анықталған табалдырықтан төмен кезде үзілістерді басу функциясы активтелгені әсерінен кейбір жүйелер сөздің басын немесе аяғын кесіп тастайды (энергияның жоғарылауы немесе төмендеу периоды кезінде);

в) дауыстық деректерді сығу. Цифрленген дауысты әртүрлі әдістермен сығуға болады. IP-желіда қолданылатын шешімдер жылдам болуы керек, дауыс сапасын сақтау және шығысты деректердің үлкен емес массивтерін беруі керек;

г) сығылған дауыстық деректерді нөмірлеу тәртібі бойынша ұзындығына тең қысқа сегменттерге бөлу, дестелердің тақырыптарын қосу және тарту;

д) шығындарды немесе дестелер кідіруін интеллектуалды өңдеуді қамтамасыз ету үшін адаптивті ресинхронизация буферінде реттеу және қабылдау. Басты мақсат болып дестелер арасындағы айнымалы кідірістердің әсер етуінен құтылу табылады. Бұл проблеманың шешуі болып келіп түсетін дестелердің жеткілікті шамасын буферизациялау, себебі дестелердің түсу уақыты әртүрлі болса да дауыс үзіліссіз болуы керек.

IP арнаның өткізу қабілетін қолданудың басты мақсаттарының бірі болып кодектің дауыстық мәліметті тиімді кодтау/декодтау алгоритмін таңдау болып табылады.

Барлық дауыстық кодерлерді әрекет ету принципі бойынша үш топқа бөлуге болады:

– 50-жылдары пайда болған және қазіргі уақытта дәстүрлі телефондық жүйелерде қолданылатын ИКМ кодегімен және адаптивті дифференциалды ИКМ (АДИКМ). Көпшілік жағдайларда олар АЦТ/ЦАТ қосындысын бейнелейді;

– дауыстық сигналды вокодерлік түрлендіруі бар кодектер жылжымалы байланыс жүйелерінде радиотрактінің өткізу қабілетіне талаптарды төмендету үшін пайда болды. Бұл кодектердің тобы мәліметтердің фонемалардың вокалды құраушылары негізінде сигналдың гармоникалық синтезін қолданады. Әдетте мұндай құрылғылар аналогты құрылғылар негізінде жасалған;

– аралас (гибридті) кодектер өздеріне дауысты вокодерлік түрлендіру/талдау технологиясын біріктіреді, бірақ специализацияланған процессорлар арқылы цифрлық сигнал көмегімен операция жасайды. Бұл типтегі кодектер өзіне ИКМ немесе АДИКМ кодекті және цифрлық әдіспен жасалған вокодерді біріктіреді.

IP-желінің дауыстық шлюздерінде кодек түсінігі тек қана кодтау/декодтау алгоритмдерін ғана емес, сонымен қатар олардың аппараттық орындауын да. IP-желіда қолданылатын кодектердің көпшілігі H.323 стандартының «G» тобы рекомендациясымен сипатталған (1.10-сурет).

ХЭБ-ның (МСЭ) 1984 жылы бекіткен G.711 рекомендациясы, аналогты сигналды 8 кГц дәлдікпен ИКМ түрлендіруді және сигнал амплитудасын

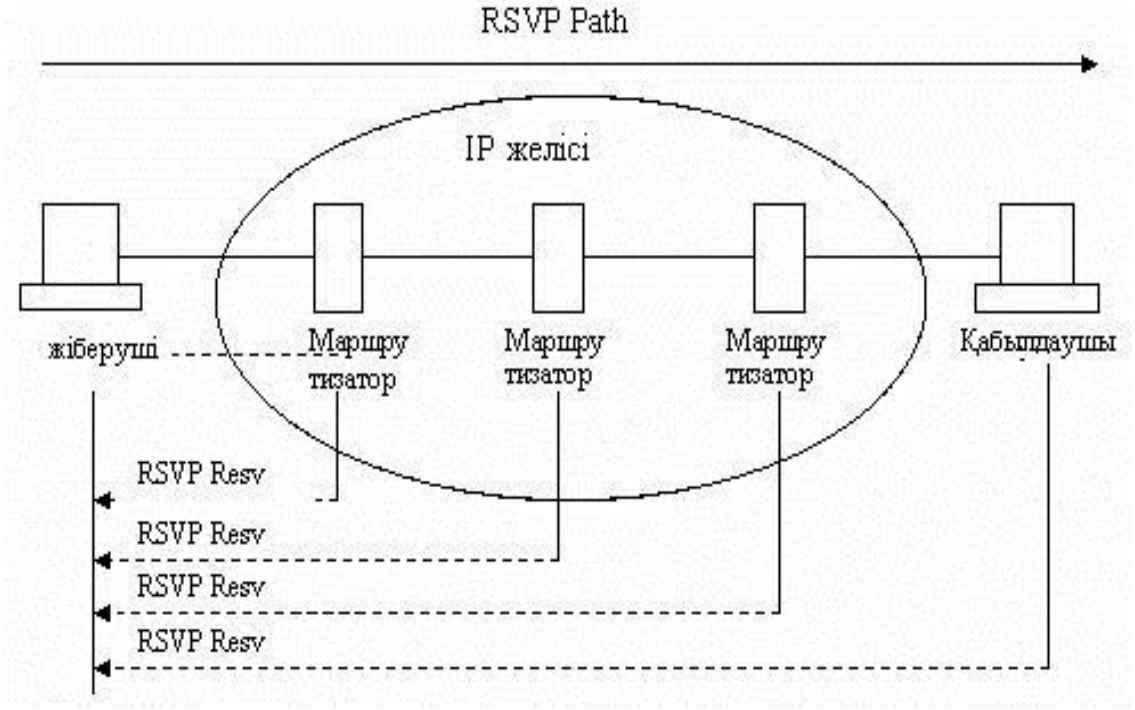
қарапайым компрессиялауды қолданатын кодекті сипаттайды. Түрлендіргіштің шығысындағы деректер ағынының жылдамдығы 64 кбит/с (8 бит х 8 кГц) құрайды. Кодтау кезінде үлкен емес амплитудалы сигналдарды түрлендіруді жақсарту және кванттау шуын төмендету үшін деңгей бойынша сызықсыз кванттау қолданылады. G.711 кодегі дәстүрлі желі жүйелерінде кең таралған. G.711 рекомендациясы H.323 стандартында негізгі және біріншілік болғанымен IP-желі шлюздерінде сирек қолданылады, себебі өткізу жолағына жоғары талаптары және тарату арнасындағы кідірістерге байланысты. G.711-дің IP-желі жүйелерінде қолданылуы тек, біруақыттағы аз санды сөйлесулер кезінде дауыстық мәліметті кодтаудың максималды сапасын қамтамасыз ету жағдайларына ғана негізделген. Дауысты сығу алгоритмдерінің ең ескілерінің бірі АДИКМ адаптивті дифференциалды ИКМ (G.726 стандарты 1984 жылы қабылданған) болып табылады.

1.10 – сурет. Дауыстық сигналдарды кодтау үшін стандарттар

Бұл алгоритм практика жүзінде ИКМ сияқты дауыс шығарудың сапасын береді, алайда оны қолдану кезінде тек 16, 32 кбит/с жолағы керек етіледі.Әдіс аналогты сигналдағы берілуші сөзде интенсивтіліктің күрт секіруінің мүмкін еместігіне негізделген. Сондықтан, егер сигналдың амплитудасын емес оның алдыңғы мәнімен салыстырғандағы өзгеруін кодтаса, онда разрядтардың аз санымен амалдауға болады. Кодек видеоконференция жүйелерінде қолданылуға арналған. G.723.1 рекомендациясы дауыстық мәліметті кодтау технологиясын MP MLQ (MultyPulse Multy Level Quantization көп импульстік, көпдеңгейлі кванттау) қолданатын гибридтік кодектерді сипаттайды, бұл кодектерді АЦТ/ЦАТ немесе вокодер комбинациясы ретінде сипаттауға

болады. G.723.1 кодегі аналогты сигналды деректер ағынына 64 кбит/с жылдамдықпен (ИКМ) түрлендіруді жүзеге асырады, сонан соң көпжолақты цифрлық сүзгі/вокодер көмегімен жиіліктік фонемаларды бөліп, оларды талдап және IP арнасы бойынша дауыстық сигналдағы фонемалардың ағымдағы жағдайы туралы мәліметтерді ғана береді. Берілген алгоритм дауыс сапасының нашарлауын білдіртпей жылдамдықты 5,3-6,3 кбит/с дейін азайтуға мүмкіндік береді. Түрлендіру процесі 37 мс кідірісті енгізеді. G.723.1 кодегі IP-желінің дауыстық шлюздарында және басқа да құрылғыларында кең қолданылады. Кодек сапасы бойынша G.729 кодтауына жол бергенімен, процессор қорларына және арнаның өткізу қабілетіне онша қатал емес. G.729 кодектерін қысқартылған түрде CSACELP (Conjugate Structure Algebraic Code Excited Linear Prediction – басқарылатын алгебралық коды бар кездесетін құрылым). Дауыстық сигналды кодтау жылдамдығы 8 кбит/с. Бұл кодек VoIP құрылғыларында жетерліктей жоғары компрессиясымен дауыстық мәліметті кодтаудың өте жақсы сапасын қамтамасыз ете отырып алдыңғы орынды алады.

1992 жылғы G.728 рекомендациясында сипатталған гибриді кодек LDCELP Lowe DelayCode Excited Linear Prediction санатына (категория) жатады, ол кодек алдын ала сызықты айтуы бар басқарылатын кодегіне ие. Кодек 16 кбит/с түрлендіру жылдамдықты қамтамасыз етеді, 35 мс-пен кодтау кезінде кідірістерді енгізеді және ұйымдастыру үшін тез әрекеттігі 40 MIPS көп процессор қажетті. Кодек видеоконференция жүйелерінде қолданылуға арналған. Берілген кодек IP-желі құрылғыларында айтарлықтай сирек қолданылады.



1.12 – сурет. RSVP хаттамасын қолдану

IP-желі сапасын қамтасыз ететін құралдардың бірі IETF комитетімен ұсынылған қорларды сақтау хаттамаларын қолдану болып табылады. RSVP көмегімен мультимедиа бағдарламалары желілік IP, әрі UDP хаттамасының кез келгені арқылы арнайы қызмет ету сапасын (QoS) талап етуі мүмкін, себебі видео және аудиосигналдарды сапалы түрде қамтамасыз ету үшін RSVP хаттамасы әрбір компьютер немесе торап арқылы кепілденген QoS-ты қарастырады, деректердің белгілі шамасы берілуі мүмкін. RSVP хаттамасы өткізу қабілетінің бөлігін резервтеу үшін ғана арналған. Жіберуші RSVP-ны қолдана отырып RSVP Path хабары арқылы алушыны қорлардың бос шамасы туралы периодты түрде хабардар етіп отырады Транзитті маршрутизаторлар да осы хабардың өтуі өлшемінде олардағы бос ресурстар шамасын талдайды және кері бағытта берілетін RSVP Resv сәйкес хабарымен нақтылайды. Егер ресурстар жеткілікті болса, онда жіберуші мәлімет таратуды бастайды. Егер ресурстар жетпесе, онда алушы талаптарды төмендетеді немесе мәлімет беруді тоқтатады.

RSVP сұралған QoS деңгейіне кепілдік бере алмаған кезде, оның өз сыйысушылық шегіне тәуелділігінде, барлық тізбектелген сұраныстар еленбейді және жойылады. Бір тораптың сұрауға жауап беру кезінде бас тартуы RSVP жүйесі бөліктерге бөлінеді. Ондағы QoS-ты беру туралы сұрауларға қызмет ету үшін маршрутизатордың қандай параметрлерді қолданатынын администратордың анықтай алу мүмкіндігі бар кезде RSVP корпоративтік деңгейде айтарлықтай жақсы болашаққа ие. Ғаламдық желілердегі маршрутизаторлар осындай юрисдикцияның астында болуы міндетті емес, сұрауларды шығаратын хосттар немесе қосымшалар кепілденген QoS-ты қиындатады. Джиттер мәнін және желілік деңгейдегі кідірістерді азайту үшін қолданушыға берілген деңгейдің сапасына кепілдік етуге RSVP, MPLS, ATM, басқа да механизмдері қолданылады. Олар желімен көрсетілетін қызмет сапасын жақсартады, бірақ желілік құрылғылардағы кезектердің түзілуін толықтай жоя алмайды, ізінше джиттерді де алып тастамайды.

Төменде IP-желінің бағдарламалық құралдары мен жабдықтарын жасауда озық нәтижеге жеткен компаниялардың тізімі келтірілген: VocalTec, Dialogic, Cisco, Ascend, 3Com, Nortel, Lucent, IBM, Motorola, RAD, Rock-well, Digitcom және т.б.

Nortel Networks концепциясының тәжірибелік жүзеге асуы Ресейлік ВСС үшін сертификациядан өткен MMCS (MultiMedia Carrier Switch) платформасы болып табылады. DPN (хаттама X.25, FR) сериялы дестелік коммутаторлар тобы Magellan және Passport 7000/6000 сериялы мультихаттамалық маршрутизаторлар, Passport Voice Gateway шекаралық құрылғылары, телефондық түйіндесуші желілер және ATM желілері, сондай-ақ Passport 15000 жоғарыжылдамдықты ATM-коммутаторлары мысал бола алады. Аталған барлық құрылғылар дауысты, факсимильдік хабарларды, бейнеақпараттарды, IP, FR, SNA, X.25, HDLC хаттамалары бойынша деректерді интегралдайды және бар қорларды (мысалы, дауысты беру кезінде

дестелерді айнымалы жылдамдықпен беру технологиясы қолданылады) пайдалануын оптималдай отырып, мультимедиялық қызметпен қаматамасыз етеді.

IP-желінің тағы да бір мысалы ретінде жапондық NEC корпорациясының гамма өнімдеріне кіретін IP45/951 әмбебап маршрутизаторы мысал бола алады. Бұл маршрутизатордың дауыстық және мультимедиялық хабар беру функциялары бар. 1P45/951 маршрутизаторы шлюз және қақпақша қызметін іске асырады. Бұл маршрутизатор дауысты кодтаудың көптеген алгоритмдерінде жұмыс жасайды, мысалы, ITU-T G.729, G.729a, G.729b, G.729ab, G.723.1, G.729.1a, G.711, G.711VAD, G.728 және G.728VAD. Бұл IP45/951 маршрутизаторына H.323 хаттамасында жұмыс істейтін барлық шлюздермен қосылуға мүмкіндік береді. IP45/951 маршрутизаторы мынадай ерекшеліктеріне байланысты дауысты беру сапасы жақсы болады: қазіргі заманғы кодтау алгоритмдерін қолдану; жаңғырықты басу (64 мс); джиттерді тегістеу; сөйлесулердегі паузаларды басу; комфорттық шуды генерациялау; RSVP хаттамасын қолдау; IP/UDP/RTP тақырыптарын сығу; әртүрлі трафиктер түрі үшін приориттерді қолдау[3].

Соңғы кездері осы барлық сценарийлер үшін IP-желі жабдықтарының келесідей түрлері пайда болды:

– IP-желінің цифрлық және аналогтық интерфейстер арқылы АТС-ға қосылатын және дауыс сигналдарын алдын ала өңдейтін, компрестейтін, IP-дестеге айналдыратын және оларды желімен жіберетін автономды шлюздер;

– мекемелік АТС-ларды корпоративті IP-желіге қосуға арналған интерфейсті 10/100BaseT (ЛВС Ethernet) магистралдық дауыстық платалар. АТС-на осындай платаны қондырғаннан соң дауыстық трафик IP-дестелер түрінде АТС-нан телефондық желіге жіберілгені сияқты жергілікті немесе ғаламдық желіге жіберіледі;

– дауыстық ақпаратты IP-дестелерге түрлендіруші және телефондық желіге емес тікелей ЛЕЖ Ethernet-ке қосылатын телефондық аппараттар (IP-телефондар). Ережеге сай, Dynamic Host Configuration Protocol (DHCP) динамикалық конфигурация хаттамасын қолдана отырып, мұндай аппараттар желілік администратордан минималдық баптауларды қажет етеді;

– IP хаттамасы негізіндегі дәстүрлі АТС-дың қызметін атқаруға арналған дауыстық дестелердің мамандандырылған коммутаторлары. Әдебиеттерде мұндай құрылғылар IP-АТС деп аталады, бірақ бұл жағдайда арналардың емес, дестелердің коммутациясы жүргізілетіндіктен бұл атау онша сәйкес келмейді.

Бұрынғы модельдерде сигналды цифрлық өңдеу бағдарламалық құралдармен жүргізілді. Содан соң бағдарламалық өңдеуді аппараттық өңдеу алмастырды, негізгі қызметті DSP (Digital Signal Processing) платалары орындай бастады, бұл негізгі процессор мен оперативті жадының жұмысын жеңілдетті, құрылғының порттар санын көбейтіп, дауыстық ақпараттың кідіріс уақытын азайтты.

Texas Instrument, Dialogic (DM3 IP Link) және Natural MicroSystems (Quad E1) фирмаларының DSP платалары көпке танымал.

Арналары коммутациялы желілер мен дестелері коммутациялы желілер арасын байланыстыратын шлюздер IP-желіны енгізудің онша маңызды емес себебі болып табылады.

Қазіргі кезде бірнеше ондаған компаниялар осы сияқты жабдықтарды шығыруда, олардың қатарында: Cisco Systems, VocalTec, Lucent Technologies және т.б. Оның үстіне, осы шлюздердің негізінде әр телекоммуникациялық компаниялардың алдыруға арыз берген немесе алған IP-желілық құрылғылары бар. IP-дестелерді маршрутизациялау технологиялары негізінде құрылған АТС-лар ұсынылады. Cisco компаниясы Catalyst 5500 коммутаторлы интегралданған AS5300 қосылу серверін жасап шығарды. Ascend Communications Inc. компаниясы коммутацияланатын TNT арналарына арналған модемді гигабиттік GRF маршрутизаторымен біріктірді. 3Com компаниясы өзінің Total Control Hub концентраторына IP-мен дауыс беру мен факсты қосты.

Бірыңғай телефон желісіне IP-дестелерді маршрутизациялау желілерімен дауыстық ақпараттарды беру технологиясын енгізген кезде жоғарыда қарастырылғаннан басқа мынадай спецификалық қиындықтар туындайды:

– IP-желі жабдықтарын екісымды аналогтық абоненттік желілермен ортақ қолданыстағы телефон желісі АТС-на қосқан кезде бұл желілерде сигналдардың тез өшуі кедергі болады;

– IP-желі жабдықтарын ОҚТЖ коммутациялық жабдығына қосқанда станцияаралық жалғау желілеріндегі байланыс декадты-қадамдық және координаттық АТС-ларының спецификалық сигнализация жүйелері әсерінен нашарлайды.

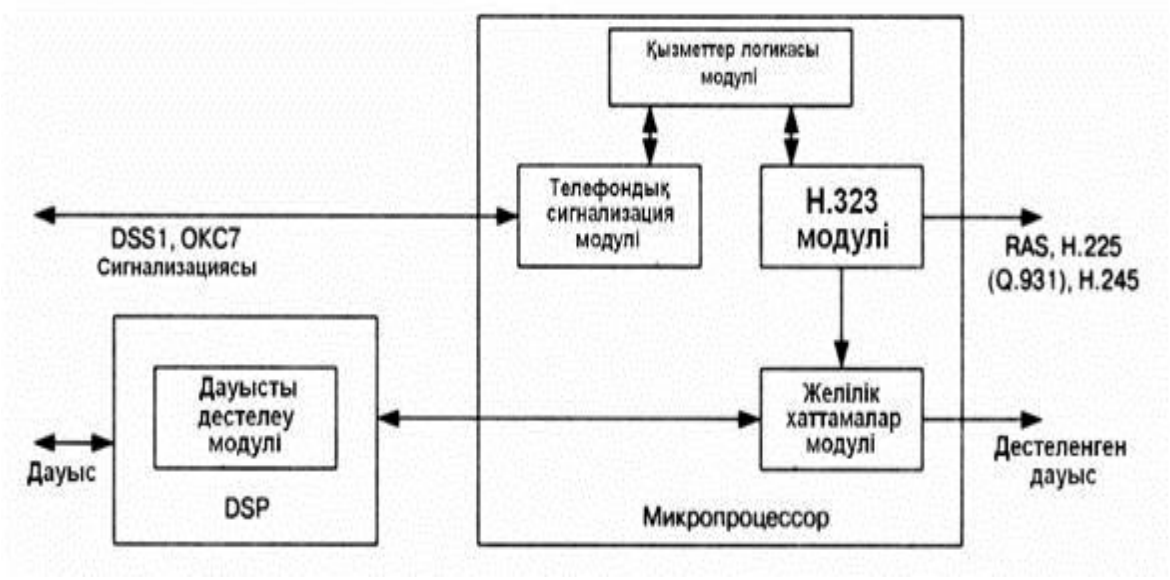
Қазақстандық шарттарда Протей-ITG жабдығымен IP-желісін құруды қарастырамыз. IP-желінің Протей-ITG шлюзі 2-нұсқалы H.323 хаттамасымен дестелерді маршрутизациялау желісімен дауыстық трафикті және факсимильдік ақпараттарды беруді жүзеге асырады. Шлюздің негізгі функционалдық жұмысы ОҚТЖ-дан тұрақты жылдамдықпен келетін дауыстық ақпараттарды IP-дестелерді маршрутизациялау желілерімен жіберуге дайын түрге түрлендіру. Яғни, кодтау және дауыстық ақпараттарды RTP/U DP/IP дестелеріне түрлендіру, сондай-ақ кері түрлендіру. Одан басқа, шлюз E-DSS1 және ОКС7 сигнализация жүйелерінің сигналдық хабарларын H.323 сигналдық хабарларына айналдырады және ITU H.246 рекомендациясы бойынша кері түрлендіру жасайды.

Протей-ITG шлюзі ОҚТЖ-ға цифрлық желілерге ISUP-R жүйесінің сигнализациясын, E-DSS1 абоненттік сигнализациясын, сондай-ақ бөлінген екі сигналдық «R1.5» арналары сигнализациясын қолдана отырып 2048 Кбит/с беру жылдамдығымен қосылады, ал IP-дестелерін маршрутизациялау желілеріне 10/100Базе-Т интерфейсінің көмегімен қосылады.

1.13-суретте IP-желінің Протей-ITG шлюзінің жалпылама құрылымдық сұлбасы көрсетілген. ОҚТЖ-дан келетін дауыс сигналдарын кодтау және дестелеу цифрлық сигналдарды өңдеуге арналған арнайы Digital Signal Processors (DSP) процессорларына негізделген Протей-ITG шлюзі арқылы іске асатынын айта кету керек. Қалған функциялар әмбебап процессорды пайдаланатын бағдарламалық қамсыздандыру арқылы орындалады.

Телефондық сигнализацияны өңдеу модулі DSS1 и ОКС7 жүйелерінің сигналдарын жүйе ішілік примитивтерге түрлендіре отырып, телефондық жабдықпен өзара байланысады. Примитивтер процессордың шақыруға қызмет көрсету (қосылу, ажырау т.с.с.)жағдайын көрсетеді және шлюздің СТОП пен IP-желі арасына байланыс орнату қызметі логикасының модулі ретінде қолданылады.

H.323 сигнализациясының модулі H.225.0 (Q.931) және H.245 хаттамаларының сигналдық ақпараттарын өңдейді. Процессордың IP-желісіндегі шақыруға қызмет көрсету (қосылу, ажырау т.с.с.)жағдайы туралы мәлімет шлюздің қызметі логикасының модуліне беріледі.

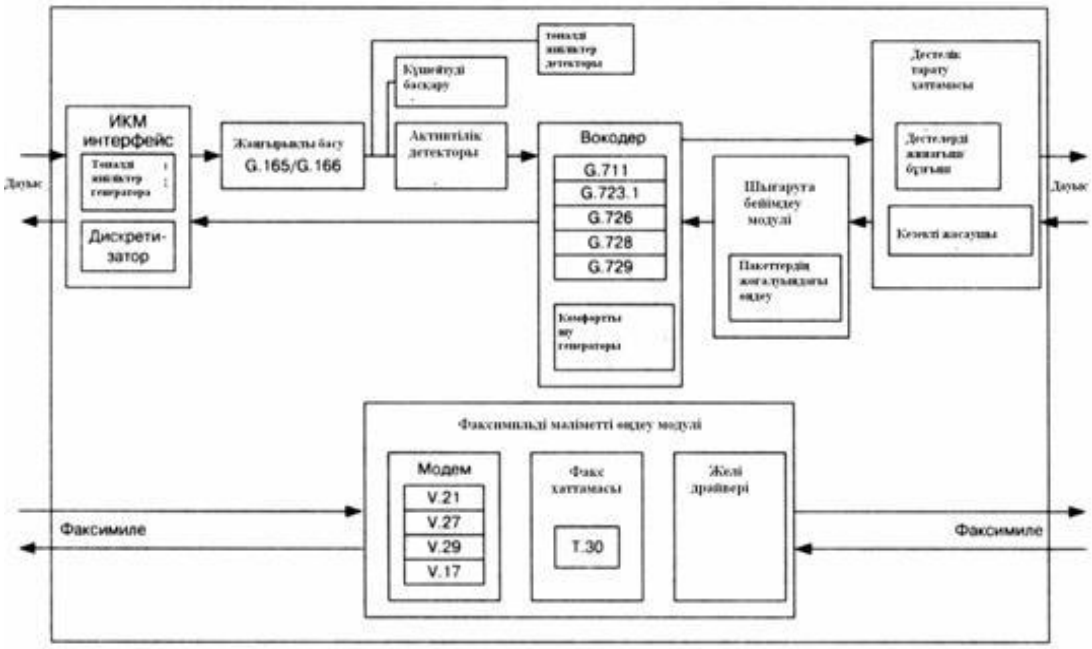


1.13 – сурет. Протей-ITG шлюзінің құрылымдық сұлбасы

Шлюздің қызметі логикасының модулі ОҚТЖ-дан IP-желіге келген шақыруларды маршрутизациялауға жауап береді. Қосылуды бақылау және шақырылатын абоненттің нөмірін анықтау сияқты қызметтер жүргізіледі. IP-желі желісінде қақпақша (привратник) болған жағдайда көптеген функциялар соған аударылады.

Дауысты дестелеу модулі ОҚТЖ-дан тұрақты жылдамдықта келіп түскен дауыстық сигналдарды ары қарай IP-дестелерді маршрутизациялау желілерімен жіберуге дайындау қызметін атқарады. Модульдің негізгі қызметтері: дауыстық сигналдарды импульсты-кодтық модуляция әдісімен түрлендіру, эхокомпенсация, дауыстық сигналды кодтау, сөйлеудегі активті

периодтар мен паузаларды табу және қайта шығаруды бейімдеу (адаптация воспроизведения).



1.14 – сурет. Дауысты дестелеу модулі

Одан басқа, модуль DTMF сигналдарын генерациялауға және детектирлеуге жауап береді, факсимильдік және модемдік сигналдарды өңдеуге жауап береді. Дауысты дестелеу модулінің құрылымы 1.14-суретте көрсетілген.

Сөйлеудегі активті периодтарды табу механизмі ОҚТЖ-дан алынған сигналдарды дауыстық ақпараттың бар-жоқтығына тексереді. Егер белгілі бір уақыт ішінде дауыстық ақпарат табылмаса, дауыстық дестелерді IP-желіге жіберу тоқтатылады.

IP-желінің барлық интеллектісі қақпақшада шоғырланған. Ол құрамына терминалдар, шлюздер және осы қақпақшада тіркелген конференцияларды басқару құрылғысы кіретін IP-желі аймағын басқару қызметін атқарады[2].

Басқарылатын аймақтың жақсы жұмысын қамтамасыз ету үшін қақпақшаның маңызды қызметтерінің қатарына мыналар кіреді:

– ақырғы және басқа құрылғылардың тіркелуі;

– пайдаланушылардың RAS (ITU H.225.0 рекомендациясы) сигнализациясының көмегімен IP-желі қызметтеріне кіріп қосылуын бақылау;

– шақырылған пайдаланушының a/yas адресін IP дестелерді маршрутизациялау (IP адрес – TCP порты номірі) желісінің транспорттық адресіне түрлендіру (абоненттің жарияланған есімін, телефондық номерді, электрондық пошта адресін және т.б.);

– желінің өткізу жолағын резервтеу,басқару және бақылау;

– терминалдар арасында H.225.0 және H.245 сигналдық хабарларын ретрансляциялау.

Соңғы жағдайда қақпақша ақырғы пайдаланушылардың күй-жағдайын кез келген уақытта біле алады және байланыстарды қайта қосу, переадресация, күтуге қою (ожидание), шақыруды ұстап қалу, т.с.с. сияқты қосымша қызметтер ұсына алады.

Протей платформалы IP-желі жабдықтарын қолдану арқылы байланыс орнатудың екі нұсқасы бар. Бірінші нұсқада IP-желінің Протей-ITG шлюзі мен Протей-GK қақпақшасы IP-желінің бұрынғы желісіне қосылады.

1.6 IP-желілердегі адрестеу және маршруттау

IP-желілердегі адрестеу принциптерімен таныстыру.

IP-желілердегі түйіндерді адрестеу тәсілі аз деңгейде осы технологияның масштабталуымен сәйкес келеді.Осыдан, ол миллиондаған желілік интерфестерді идентификациялай алады (мысал ретінде, миллиардтаған Интернет қолданушыларды алайық). Бірақ TCP/IP технологиясында мұндай мүмкіндікті жасау үшін арнайы механизмдер мен хаттамаларды қосуға тура келді.

TCP/IP стегінде адрестердің үш типі қолданылады:

– ішкі желі аумағындағы түйіндерді адрестеуде қолданылатын жергілікті, немесе аппараттық адрестер;

– барлық құрама желі аумағында түйіндердің бір мәнді идентификациясы үшін қолданылатын желілік, немесе IP-адрестер;

– домендік атаулар – пайдаланушылар жиі хабарласатын түйіннің символдық идентификаторлар.

Жалпы жағдайда желілік интерфейстің бір мезгілде бір немесе бірнеше жергілікті адресі немесе бір немесе бірнеше желілік адресі, сондай-ақ бір немесе бірнеше домендік атаулары болуы мүмкін.

Сонымен, аппараттық (жергілікті) адрес түйінді ішкі желі аумағында анықтап береді. Егер ішкі желі мына: LAN – Ethernet, FDDI, Token Ring базалық технологиялардың бірін пайдаланса, – онда деректерді осындай ішкі желінің кез келген түйініне жеткізу үшін MAC-адресті көрсету жеткілікті. Осылайша, бұл жағдайда MAC-адрес ақпараттық адрес болып табылады.

TCP/IP технологиясының құраушы желісіне күрделі технологиялар негізінде, мысалы, IPX/SPX сияқты күрделі технологиялар негізінде құрылған ішкі желілер кіреді. Бұл желінің өзі ішкі желілерге бөлінеді және IP-желісі сияқты өзінің түйіндерін аппараттық және желілік IPX-адрестермен анықтайды. Бірақ, IPX/SPX құраушы желісі TCP/IP құраушы желісі үшін қарапайым ішкі желі болғандықтан осы ішкі желі түйіндерінің аппараттық адресі ретінде дәл осы ішкі желінің түйіндерін анықтайтын адрестер алынады, ал бұл адрестер – IPX-адрестер. Осыған орай, егер құрашы желіге X.25 желісі қосылған болса, онда сәйкесінше IP хаттамасы үшін жергілікті адрестер X.25 адрестер болып табылады.

IP-адрестер негізгі адрестер болып саналады. Осы адрестердің негізінде желілік деңгей желілер арасында дестелер жібереді. Бұл адрестер 4 байттан тұрады, мысалы 109.26.17.100. IP-адресті компьютерді немесе маршрутизаторларды конфигурациялап жатқан кезде администратор енгізеді.IP-адрес екі бөлімнен тұрады: желі нөмірлері және түйін нөмілері. Желі нөмірін администратор өзі таңдайды немесе желі интернеттің құраушы бөлігі сияқты жұмыс жасау керек болса, интернеттің (InternetNetworkInformationCenter, InterNIC) бір бөлімшесінің ұсынысы бойынша таңдалады. Әдетте интернет қызметшілері InterNIC бөлімшелерден адрестер диапазонын алады да, оны өз абоненттері арасында бөліп алады. IP хаттамасындағы түйіндер нөмірі түйіннің жергілікті адресіне қатыссыз тағайындалады. Маршрутизатор анықталуына қарай бірден бірнеше желіге кіреді, сондықтан маршрутизатордың әр портының меншікті IP-адресі болады.

Ақырғы түйін де бірден бірнеше IP желіге кіре алады. Бұл жағдайда желілік байланыстар санына байланысты компьютердің бірнеше IP-адресі болуы керек. Осылайша, IP-адрес бөлек компьютерді немесе маршрутизаторды емес, түгелдей желілік байланысты білдіреді.

IP-желіде символдық атаулар домендік деп аталады және иерархиялық белгілері бойынша құралады.IP-желінің толық символдық атауларының құраушылары нүктемен ажыратылады да, мынадай ретпен саналады: бірінші жәй хосттың аты, сосын түйіндер тобының аты (мысалы, ұйымның аты), содан соң одан үлкенірек топтың аты (поддомена) және осылайша, ең жоғарғы домен атына дейін жалғаса береді (мысалы, ұйымдарды географиялық принциптеріне қарай біріктіретін домен: RU — Ресей, UK – Ұлыбритания, SU – АҚШ. Сондықтан домендік атауларды DNS-атаулар деп те атайды.

IP-адрестің ұзындығы 4 байт (32 бит) және екі логикалық бөліктен тұрады – желі нөмірі және желідегі түйін нөмірі.

IP-адрестің жазу түрінің ең көп қолданылатын түрі әр байттың мәнін ондық санау жүйесінде бейнелеп, нүкте арқылы бөлінентін төрт сан ретінде жазу түрі, мысалы:126.10.2.30.

Бұл адрес екілік форматта: 10000000 00001010 00000010 00011110.

Сондай-ақ он алтылық форматта:80.0A.02.1D.

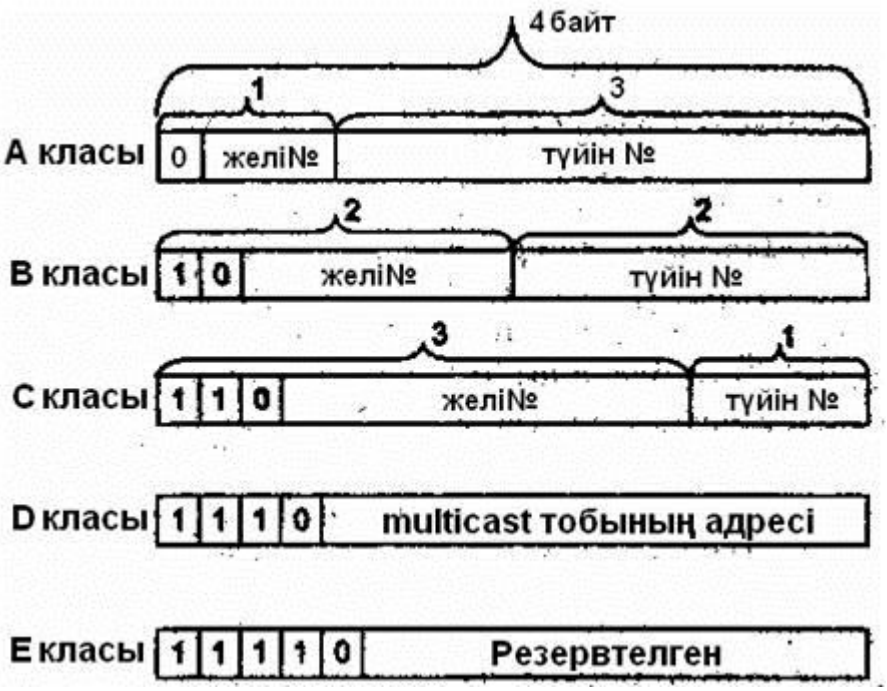
Адрестің жазылуы желі нөмірі мен түйін нөмірі арасындағы арнайы шектеуші таңбаны ескермейтінін байқаймыз. Қарапайым жолы адрестің 32-биттік өрісі алдын ала екі бөлікке бөлінеді, тең болуы міндетті емес, бірақ бекітілген ұзындықта болуы керек, біреуіне үнемі желі нөмірі, екіншісіне түйін нөмірі жазылады. Түйін нөмірін сақтауға арналған өрістің бекітілген ұзындығы болғандықтан, барлық желілердің максималды саны бірдей болады. Егер, мысалы, желі нөмірі орнына бір бірінші байтты жазса, онда бүкіл адрестік кеңістік үлкен өлшемді (2^{24} түйінді) желі сандарына бөлініп кетеді. Егер шекараны оңға жылжыта берсе, желілер саны артады, бірақ олар бәрібір бірдей өлшемде болады. Мұндай қатаң қадам жеке ұйымдар мен кәсіпорындардың қажеттіліктерін өтеуге мүмкіндік бермейді. Сондықтан адрес құрудың дәл осы тәсілі ғана қолданыс таппады.

Екінші, маска қолдануға негізделгендіктен ғана желі нөмірі мен түйін нөмірі арасындағы шекараны ыңғайлы етіп қоюға жол берді. Бұл жағдайда *маска* –IP-адреспен бірге жұптап қолданатын сан; масканың екілік форматтағы жазылуы IP-адресте желі нөмірі ретінде түсіндірілетін разрядтағы бірліктер тізбегінен тұрады. Желі нөмірі адрестің тұтас бөлігі болғандықтан, маскадағы бірліктер үздіксіз тізбек болуы қажет. Маскадағы бірліктер тізбегі мен нөлдіктер тізбегі арасындағы шекара IP-адрестегі желі нөмірі мен түйін нөмірі арасындағы шекараға сәйкес келеді. Мұндай жағдайда адрестік кеңістік әртүрлі өлшемдегі желілер жиынтығы болып табылады.

Желілердің бірнеше класы бар және олардың әрқайсысының өлшемі анықталған.

IP-адресін желі нөмірі мен түйін нөміріне бөлу дәстүрлі әдісі адрестің алғашқы бірнеше биттері мәнімен анықталатын класс түсінігіне негізделген. Міне, адрестің бірінші байты 185.23.44.206 128-191диапазонына жататындықтан, бұл адрес В класына тиісті деп айта аламыз, яғни желі нөмірі екі нөлдік байтпен толтырылған IP-адрестің алғашқы екі байты болып табылады – 185.23,0.0, ал түйін нөмірі әуелі екі нөлдік байтпен толтырылған екі кіші байт – 0.0.44.206 болып табылады.

IP-адрестің қай класқа жататындығы адрестің алғашқы биттерінің мәнімен анықталады. 1.15-суретте әртүрлі кластардың IP-адрестердің құрылымы көрсетілген.



1.15 – сурет. IP-адрестер құрылымы

Егер адрес 0-ден басталса, онда бұл адрес желі нөміріне бір байт қосылып, қалған үш байт желі түйіні нөмірі ретінде түсіндірілетін А класына жатады. 1 (00000001) -мен 126 (01111110) диапазонында жататын нөмірлі

желілер А класының желілері деп аталады. (0 нөмірі қолданылмайды, ал 127 нөмірі төменде баяндалатын арнайы мақсаттарға арналған.) А класына жататын желілер аз, бірақ олардың түйіндерінің саны 2^{24}-не жетеді, яғни 16777216 түйін.
Егер алғашқы екі байты 10 тең болса, онда адрес В класына тиесілі. В класының адрестерінде желі нөмірі мен түйін нөміріне екі байттан енгізіледі. Нөмірі 128.0 (1000000000000000) бен 191.255 (1011111111111111) диапазонындағы желілер, В класының желілері деп аталады. Осылайша, В класының желілері А класының желілерінен көп болып шығады, бірақ өлшемдері кіші, түйіндер санының максимумы 2^{16} (65536).

Егер адрес 110 биттерінің тізбегінен басталса, онда бұл С класының адрестері. Бұл жағдайда желі нөміріне 24 бит енгізіледі, ал түйін нөміріне – 8 бит. С класының желілері көбірек таралған, бірақ түйіндері саны 2^8 (256)-мен шектелген.

Тағы да D және Е кластары адрестерінің желіге тікелей қатысы жоқ.

Егер адрес 1110 биттерінің тізбегінен басталса, онда бұлD класының адрестері және бұл ерекше, топтық адрес (multicast). Топтық адрес жалпы жағдайда әр желіге тиісті түйіндер тобын(желілік интерфейстер) анықтайды. Топқа кіретін интерфейс әдеттегі жеке IP-адреспен қатар тағы бір топтық адрес алады. Егер дестені жіберу кезінде тағайындалған адрес ретінде Dкласының адресі көрсетілсе, онда бұл десте осы топқа кіретін барлық түйіндерге жекізілу керек.

Егер адрес 11110 биттерінің тізбегінен басталса, онда бұл Е класының адрестері. Бұл кластың адрестері алдағы жұмыстар үшін резервтелген.

1.1-кестеде желі нөмірлерінің диапазондары және әр желі класына сәйкес келетін максимал түйіндер саны келтірілген.

1.1− кесте. Әртүрлі кластар адрестерінің сипаттамалары

Класс	Алғашқы биттер	Желінің ең кіші нөмірі	Желінің ең үлкен нөмірі	Желідегі максимал түйіндер саны
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Резервтелген

Үлкен желілер А класының адрестерін алады, орташалары – В класын, ал кішіректері – С класын:

– егер IP-адресінің барлық екілік разрядтары 1-ге тең болса, онда мұндай адресті десте осы желідегі барлық түйіндерге таратылуы тиіс. Мұндай таратылма шектеулі кеңтаралушы хабарлар(limited broad cast)деп аталады (ограниченным широковещательным сообщением). Бұл жағдайдағы шектеулік десте ешқандай жағдайда маршрутизатор шегінен аспайтындығын білдіреді;

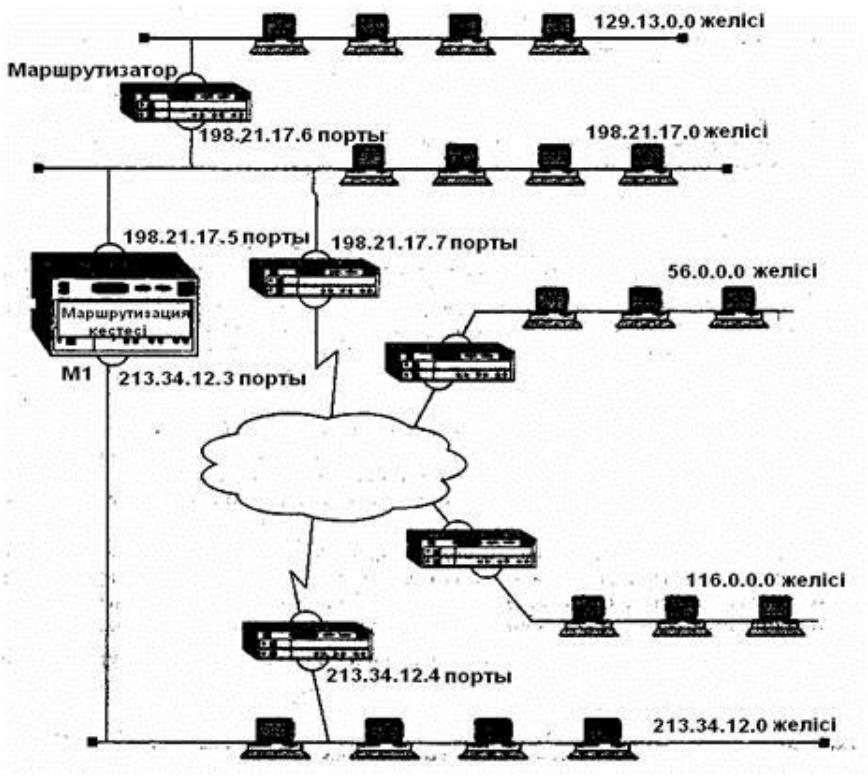
– егер тағайындалған түйін нөмірі, өрісі тек бірліктерден құралса, онда мұндай адресі бар десте желі нөмірі берілген барлық желілерге таратылады.

Мысалы, 192.190.21.255 нөмірлі адресті десте 192.190.21 желісінің барлық түйіндеріне жеткізіледі. Мұндай таратылма шектеулі кеңтаралушы хабарлар (limitedbroadcast)деп аталады)[1].

Нөлдіктердің тізбегінен тұратын арнайы адрестер тек жіберушінің адресі ретінде ғана қолданылады, ал бірліктердің тізбегінен тұратын адрестер тек алушының адресі ретінде ғана қолданылады. TCP/IP стегі құрылымы жоғарыда қарастырылған құру принциптеріне сәйкес келеді. Бірақ, IP-маршрутизациясы кестесінің түрі TCP/IP стегінің нақты жүзеге асуына байланысты. M1 маршрутизаторы 1.16-суретте келтірілген желіде жұмыс жасай алатын маршрутизация кестесінің үш түрін мысалға келтіреміз.

Маршрутизация кестесі өрістерінің қызметі. Сыртқы айырмашылықтарына қарамастан, барлық үш кестеде маршрутизация концепцияларын қарастырған кезде талданған және маршрутизатор жұмысына қажетті барлық кілттік параметрлер бар.

Мұндай параметрлерге, біріншіден, тағайындалған желі адрестері жатады (NetBuilder маршрутизаторларындағы «Destination» бағандары және MPR маршрутизаторларындағы «NetworkAddress» немесе UNIX). Кейбір жағдайларда, мысалы желі түйіндерінің бірінің маршруты осы желінің басқа түйіндерінің маршрутынан басқа болса, онда бұл бағанда нақты тағайындалған түйіннің адресі көрсетілетінін байқаймыз.



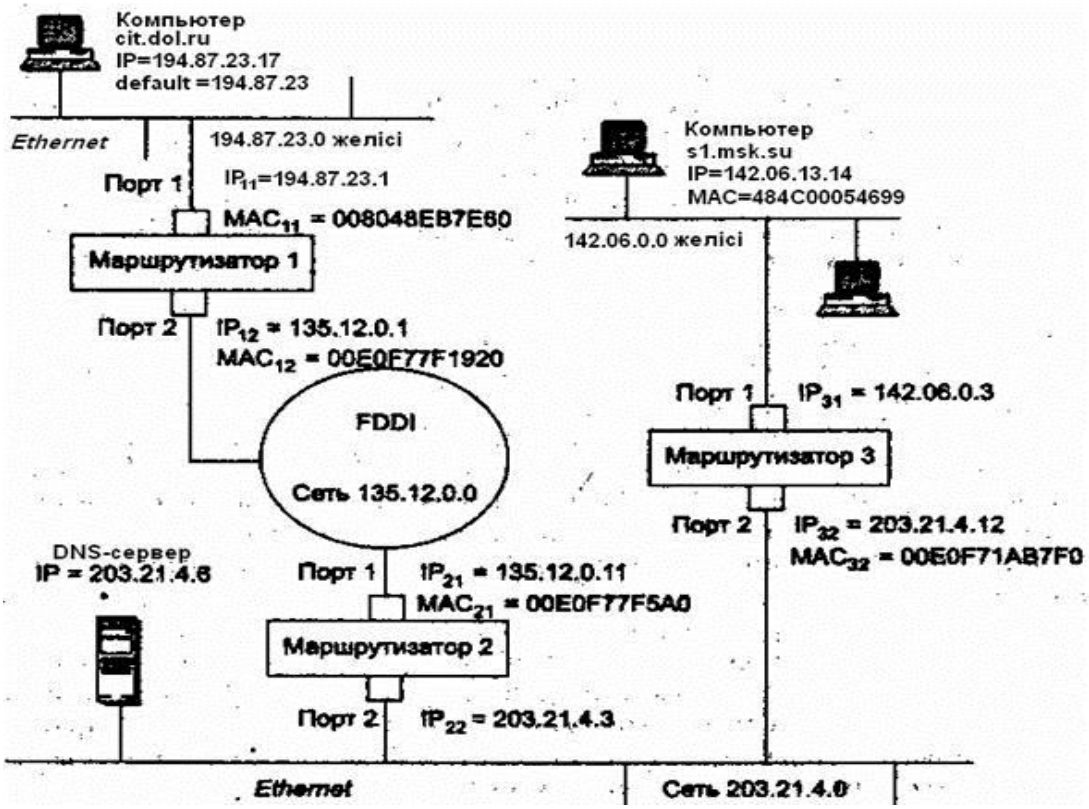
1.16 – сурет. Маршрутизацияланатын желінің мысалы

Маршрутизация кестесінің екінші міндетті өрісі келесі маршрутизатор адресі болып табылады (NetBuilder маршрутизаторларындағы «Gateway» бағандары NetBuilder және MPR маршрутизаторларындағы «GatewayAddress» немесе UNIX).

Үшінші кілттік параметр – десте бағытталатын порт, кейбір кестелерде тікелей (WindowsNT кестесінде «Interface» өрісінде), ал кейбірінде — жанамалы түрде көрсетіледі. UNIX-маршрутизаторының кестесінде 198.21.17.5 адресті порты үшін порт адресі орнына оның шартты атауы – le0 беріледі, ал 213.34.12.3 адресті порты үшін — le1 және 127.0.0.1 адресті порты үшін — lo0 атауы беріледі.

NetBuilder маршрутизаторында шығыс портын білдіретін II өріс тіпті жоқ. Бұл шығыс портының адресін келесі маршрутизатордың адресіне жанама түрде анықтауға болатындығын білдіреді.

Кестеде маска өрісінің болуы немес болмауы бұл маршрутизатор қаншалықты қазіргі заманға сай екендігін білдіреді. MPRWindowsNT (поле «Netmask») және NetBuilder (поле «Mask») маршрутизаторлары кестесінде жасалғандай, маска өрісін кестенің әр жазбасында қолдану стандарты шешім болып табылады. Маршрутизаторлармен шешім қабылдағанда маскаларды өңдеуді төменде қарастырамыз. Маска өрісінің болмауы маршрутизатор үш стандарты адрестер класымен ғана жұмыс істеуге арналғандығын немесе ол барлық жазбалар үшін сол бір ғана масканы қолданатындығын білдіреді. Бұл маршрутизацияның ыңғайлылығын төмендетеді.



1.17 – сурет - Компьютерлердің желі арқылы өзара байланысу мысалы

10.1.2 маскаларды қолданбай маршрутизациялау. IP-желісі мысалында желілік деңгейдің құралдарының құраушы желімен кестелерді жылжыту жұмысының алгоритмін қарастырамыз (1.17-сурет). Мысалда қарастырылатын желінің барлық түйіндерінің адрестері кластарға негізделген, маскалар қолданбайды деп есептейміз. IP хаттамасы мен ARP және DNS адреске рұқсат беру хаттамаларымен байланысуына ерекше назар аударылған.

Ethernet желісінде отырған және 194.87.23.17 IP-адресі (С класының адресі) бар cit.dol.ru компьютерінің пайдаланушысы FTP хаттамасы бойынша басқа Ethernet желісінде отырған және 142.06.13.14IP-адресі (В класының адресі) бар s1.msk.su компьютеріне хабарласады: ftps1.msk.su.

FTP модулі өзінің хабарын өзінің сегментін IP хаттамасының дестесіне қоятын TCP транспорттық хаттамасының сегментіне айналдырады. IP-дестенің тақырыбында тағайындалған түйіннің IP-адресі көрсетілуі тиіс. cit.dol.ru компьютерінің пайдаланушысы s1.msk.sukомпьютерінің символдық атауын көрсеткендіктен TCP/IP стегі де тағайындалған түйіннің IP-адресін өздігінен анықтау керек.

FTP модулі өзінің хабарын транспорттық TCP хаттамасының сегментіне айналдырады (буады). Ал TCP хаттамасы өз кезегінде өзінің сегментін IP хаттамасының дестелеріне орнатады. IP дестесінің тақырыбында тағайындалған түйіннің IP адресі көрсетілуі тиіс. cit.dol.ru компьтерінің қолданушысы s1.msk.su компьтерінің символды атын көрсетеді, онда TCP/IP стегі тағайындалған түйіннің IP адресін өз бетінше анықтауы керек.

Осылайша, атқа рұқсат ету жергілікті түрде орындалады, және IP хаттамасы s1.msk.su компьютерлерімен өзара әсерлесу үшін тағайындалған адреспен 142,06,13.14 IP дестелерді жасай алады.

cit.dol.ru компьтерінің IP модулі дестелерді 142.06.13.14 адресімен маршруттау керектігін тексереді. Тағайындалған желі адресі (142.06.0.0) компьтер-жіберушіге тиісті желі адресімен (194.87.23.0) сәйкес келмесе, онда маршруттау қажетті.

cit.dol.ru компьютері IP адресі 194.87.23.1 белгілі маршрутизаторға дестені үнсіз жіберу үшін Ethernet кадрын жасауға кіріседі, бірақ кадрдың жергілікті желі бойынша жылжуына керекті MAC адрес белгісіз. Маршрутизатордың MAC адресін анықтау үшін ARP-кестесін қарастыратын ARP хаттамасына жүгінеді. Егер cit.dol.ru компьютері қандай да бір желі аралық алмасулар орындап жатса, онда маршрутизатордың IP және MAC адрестері арасындағы сәйкестілікті ұстаушы барлық ізделіп отырған жазулар, ARP хаттамасының кэш-кестесінен үнсіздік бойынша табылады. Берілген жағдайда керекті жазу кэш-кестеден табылған болсын:

194.87.23.1 008048EB7E60.

Табылған MAC адресті 008048EB7E60 маршрутизатор нөміріне сәйкес белгілейік және оның порттарын MAC_{11} арқылы.

Нәтижесінде cit.dol.ru компьютері Ethernet кадрына буылған дестені локальды желі арқылы жібереді.

Кадр 1 маршрутизатордың 1 порты арқылы Ethernet хаттамасына сәйкес қабылданады, себебі бұл порттың MAC түйіні өзінің MAC_{11} адресін таниды. Ethernet хаттамасы бұл кадрдан IP дестені шығарып алады және IP хаттаманы жүзеге асыратын маршрутизатордың бағдарламалық қамтамасыз етуіне жібереді. IP хаттамасы дестеден тағайындалған адресті 142.06.13.14 шығарып алады және өзінің маршрутизация кестесінен жазылуын қарайды. 1 маршрутизатор өз маршрутизация кестесінде келесі жазуларға ие:142.06.0.0135.12.0.11 2.

Бұл жазу 142.06.0.0 желісінің дестелерін 135.12.0.11 желісінде орналасқан, 1 маршрутизатордың 2 портына қосылған маршрутизаторға беру керектігін білдіреді.

1 маршрутизатор 2 портының параметрлерін қарайды және оған FDDI желісі қосылғанын табады. FDDI желісі Ethernet желісіне қарағанда MTU мәніне көбірек ие, онда IP дестесінің фрагментациясы талап етілмейді.

Сондықтан 1 маршрутизтор FDDI форматының кадрын жасайды. Осы сатыда IP модулі келесі маршрутизтордың MAC адресін белгілі IP адресі 135.12.0.11 бойынша анықтайды. Бұл үшін ол ARP хаттамасына жүгінеді. Кэш кестесінде керекті жазу табылмаса, онда FDDI желісіне құрамында келесі мәліметтері бар кеңінен хабарлаушы ARP сұрауы жіберіледі.

2 маршрутизатордың 1 порты өзінің IP адресін таниды және ARP-жауабын сұраған түйіннің адресіне жібереді; енді 1 маршрутизатор келесі маршрутизатордың MAC адресін 00E0F77F51A0 біле отырып, FDDI кадрын 2 маршрутизатор бағыты бойынша жібереді. Ол FDDI кадрын алып, кадрдың тақырыбын алып тастайды, ал IP тақырыбынан тағайындалған IP адресін шығарады және өзінің маршрутизация кестесін қарайды. Кестеден тағайындалған нақты желінің жазуын табуы мүмкін:142.06.0.0 203.21.4.12 216.

Мұндай жазу болмағанда маршрутизатор туралы жазу үнсіз келісім бойынша қолданылады: default203.21.4.12 2.

Келесі маршрутизатордың IP адресін 203.21.4.12 анықтаған IP модулі, Ethernet желісімен 3 маршрутизаторға дестені беру үшін Ethernet кадрын жасайды. Ол АКР хаттамасының көмегімен осы маршрутизатордың MAC адресін табады және оны кадр тақырыбына енгізеді. Тағайындалған түйіннің IP адресі өзгеріссіз қалады.

Тағайындалған желінің маршрутизаторына (3 маршрутизатор) десте келіп түскен соң, бұл дестені тағайындалған компьютерге жіберу мүмкіндігі туады. 3 маршрутизатор өзінің бірінші портына тікелей қосылған желіге 142.06.0.0 беру керектігін анықтайды. Сондықтан ол Ethernet желісі бойынша s1.msk.su компьютерінің IP адресімен ARP сұрауын жібереді. ARP жауабында ақырғы түйіннің MAC адресі болады. Ол адресті IP модулі Ethernet кадрын жасау үшін арналық хаттамаға береді.

s1.msk.su компьютерінің желілік адаптері Ethernet кадрын ұстап, тақырыпта болатын MAC адреспен өзінің адресін салыстырады және оны IP модуліне жібереді. IP тақырыбы өрісін талдаған соң дестеден деректерді шығарып алады, бұл деректерде жоғары тұрған хаттаманың хабарлары

болады. Берілген мысалда транспортты TCP хаттамасы ретінде қолданылатын FTP хаттамасы бойынша деректер алмасуын қарастырғандықтан, IP дестенің деректер өрісінде TCP сегмент орналасады. TCP тақырыптан порт нөмірін анықтаған IP модулі сегментті сәйкес кезекке бағыттайды. Берілген сегмент бұл кезектен FTP-серверінің бағдарламалық модуліне түседі.

Маршрутизация хаттамалары желілік деңгей дестелерінің жылжуы өтетін маршрутизация кестесін автоматты түрде құруға арналған. IP және IPX сияқты маршрутизация хаттамаларының желілік хаттамалардан айырмашылығы міндетті болып табылмайды, себебі маршрутизация кестесі желі администраторы арқылы қолмен құрылуы мүмкін. Алайда күрделі топологиялы және көптеген балама маршруттары бар ірі желілерде маршрутизация хаттамалары өте маңызды және пайдалы жұмысты орындайды, яғни маршрутизация кестесінің құрылуын автоматтау, жұмысшы маршруттардың ағымдағы жинағын желі жағдайына динамикалық түрде өзгерте отырып және оның жұмыс өнімділігін арттырады.

Құрылымдық желілердегі дестелердің жылжуы маршрутизация кестелері негізінде жүзеге асырылады. Маршрутизация кестелеріндегі ортақ нәрсе болып, маршрутизаторға түсетін кез келген дестенің жылжуы үшін шешім қабылдауы туралы жеткілікті мәлімет сақталады. Ереже бойынша, мұндай кестенің әрбір жазуы белгіленген желі адресімен адресті немесе осы адреспен десте берілетін шығыс интерфейстің нөмірімен байланыстырады. Әрбір желі маршрутизаторы дестенің желімен жылжуы кезіндегі көп қадамды процесінің бір қадамын анықтайтын өзінің меншікті маршрутизация кестесін иеленеді.

Әрбір маршрутизатордағы дестенің желі көзінен белгіленген желіге жылжуы туралы тапсырмасы екі тапсырмаға бөлінеді:

– дестені маршрутизация кестесі көмегімен өңдеу;
– маршрутизация кестесін құру.

Маршрутизация хаттамаларының мақсаты екінші тапсырманы автоматты түрде шешуден тұрады. Бұл үшін желі маршрутизаторлары құрылымдық желінің топологиясы туралы арнайы қызметтік информациямен алмасады. Олардың негізінде әрбір маршрутизатор белгіленген тораптарға бағытталған маршруттарды таңдайды. Құрастырылатын маршрутизация кестелері желі арқылы дестелердің тиімді тізбектелуін қамтамасыз етеді, бұл кезде маршруттарды таңдау критерилері әртүрлі болуы мүмкін. Әдетте «ең қысқа» жол таңдалынады, ондағы қашықтық деп аралық маршрутизаторлардың саны немесе маршрутизаторлар арасындағы арнаның номиналды өткізу қабілетін көрсететін комплексті көрсеткіш, арналар сенімділігі немесе олармен енгізілетін кідірістер. Маршрутизация хаттамалары маршрутизаторларда бір-бірімен келістірілген маршрутизация кестелерін жасауы керек, яғни шығушы желіден белгіленген желіге деректердің соңғы қадамдар санымен жеткізілуін қамтамасыз ету. Қазіргі

кездегі маршрутизация хаттамалары кестелердің келістірілуін қамтамасыз етеді, алайда, олардың бұл қасиеттері желінің өзгеруінде абсолютті емес, мысалы арналардың немесе маршрутизаторлардың бас тартуы кезінде әртүрлі маршрутизаторлардың уақыттық келістірілмеген кестелері әсерінен желінің тұрақсыз жұмыс істеу периоды болады. Маршрутизация хаттамасына біраз уақыт кажет, себебі қызметтік мәліметпен алмасудың бірнеше итерациясынан кейін желінің барлық маршрутизаторлары өздерінің таблицаларына өзгерістер негізеді және нәтижесінде кестелер қайта келістіріледі.

Маршрутизация хаттамаларына өтуден бұрын, құрама желілердегі дестелердің жылжу туралы келесі әдістерді айту қажет, олар маршрутизаторлардағы кесте маршрутизациясын және маршрутизация хаттамаларын мүлде талап етпейді.

Желі бойынша деректерді тарату әдісінің ең қарапайым әдісі көшкінді маршрутизация деп аталады. Ондағы әрбір маршрутизатор өзінің тікелей көршілеріне дестелерді береді, тек өзі десте қабылдаған көршісіне бермейді. Бұл ең орында әдіс болып табылмайды, себебі желінің өткізу жолағы аса ысырап, бірақ ол жұмысқа қабілетті (осылайша локалды желілердің көпірлері мен коммутаторлары белгісіз адрестерге ие кадрларымен келіп түседі).

Кестесіз маршрутизациялаудың басқа бір нұсқасы – бұл оқиғалармен басқарылатын маршрутизация (Event Dependent Routing), ондағы десте белгілі тағайындалған желіге бұрынырақ табысқа әкелген маршрут (берілген тағайындалған адрес үшін) бойынша беріледі. Бұл жетерліктей тиімді маршрутизация әдісі, бірақ ол кері байланысты керек етеді, себебі жіберуші-маршрутизатор дестенің табыспен жеткізілу фактісін бекітуі керек. Оқиғалармен басқарылатын маршрутизация, маршрутизация кестесімен сыйысуы мүмкін. Мұндай кестеде әрбір тағайындалған желі үшін бірнеше мүмкін болатын көршілер көрсетіледі, оларға байланысты ұйымдастыруға мақсатты түрде сұрау жіберу. Бұған ұқсас жағдайлар телефондық желілерді қолданылады, оларда байланысты орнатуға керекті мүмкін болатын «бағыттарда» сұрау жіберу көрсетіледі. Алғашқыда бұл сұраулар көрсетілген бағыттардың біріншісімен беріледі, оның коммутациялық сыйымдылығы таусылған соң келесіге беріледі және тағы да сол сияқты.

Маршрутизация тағы бір түрі болып, маршрутизация кестесінің болуын керек етпейтін көзден шығу маршрутизация табылады (Source Routing). Бұл жағдайда жіберуші дестеге мәлімет енгізеді. Бұл мәлімет дестенің тағайындалған желіге берілуіне қандай аралық маршрутизаторлар қатысуы керек екендігін білдіреді. Осы мәлімет негізінде әрбір маршрутизатор келесі маршрутизатордың адресін салыстырып оқиды, егер ол оның тікелей көршісінің адресі болып табылса, дестені ары қарай өңдеу үшін оған береді. Желі арқылы десте сапарының дәл маршрутын жіберуші қалай анықтайды деген сұрақ ашық түрде қалады.

Маршрутты администратор қолмен немесе жіберуші торап автоматты түрде салуы мүмкін, бірақ бұл жағдайда оған торапқа желінің топологиясы және жағдайы туралы жеткізетін осы немесе басқа хаттаманы сүйемелдеу керек.

Маршрутизациялар кестелер негізінде жасалған жағдайларды, статикалық және адаптивтік маршрутизация деп айырады. Бірінші жағдайда желі администраторы арқылы қолмен кестелер құрылып және әр маршрутизатордың жадына енгізіледі, кестелердегі барлық жазулар олардың өмірінің шексіздігін білдіретін «статикалық» (static) статусқа ие. Қандай да бір элементтің жағдайын өзгерту кезінде желі администраторына маршрутизаторлардағы маршрутизация кестесіне міндетті түрде өзгерістер енгізуі керек. Мұндағы маршрутизаторлар үшін мұндай өзгертулер дестелер тізбегінің маршрутын өзгертуді талап етеді, бұлай етпесе желі қатемен жұмыс істейді және дестелер белгіленген желіге дейін жетуді тоқтатады немесе маршрут орынды болмайды. Осылайша, статикалық маршрутизация кезінде маршрутизация хаттамалары талап етілмеген болып табылады, себебі олардың барлық жұмыстарын бір немесе бірнеше администратор орындайды.Адаптивті маршрутизация желі құрылымы өзгергеннен кейін маршрутизация кестесін автоматты түрде жаңалауды қамтамасыз етеді. Кестелердің бейімделуі үшін маршрутизация хаттамалары керек. Бұл хаттамалар желідегі байланыс топологиясы туралы мәліметтерді барлық маршрутизаторларға жинауға мүмкіндік беретін әрі байланыс құрылымындағы өзгерістерді оперативті түрде өтейтін алгоритмдер негізінде жұмыс істейді. Адаптивті маршрутизация кезіндегі маршрутизация кестесінде әдетте берілген маршрут әрекеттегі болып қалатын уақыт интервалы туралы маршрутизация нақты болып қала береді. Бұл уақытты маршруттың өмір уақыты (Time To Live, TTL) деп атайды. Егер маршруттың өмір сүру уақыты маршрутизация хаттамаларымен расталмаса, онда ол жұмыс істемейтін болып саналады және онымен дестелер жіберілмейді.

Маршрутизация хаттамалары таратылған және орталықтандырылған болуы мүмкін. Таратылған жағдайда желіде топологиялық мәліметті жинайтын және талдап қорытатын қандай да бір бөлінген маршрутизаторлар болмайды: бұл жұмыс желідегі барлық маршрутизаторлар арасында таратылады. Әрбір маршрутизатор желінің қалған маршрутизаторларынан маршрутизация хаттамасы бойынша алынған деректер негізінде өзінің жеке маршрутизация кестесін құрады.

Орталықтанған жағдайда желіде бір маршрутизатор болады, ол басқа маршрутизаторлардан желінің жағдайы мен топологиясы туралы барлық мәліметтерді жинайды. Сонан соң бұл бөлінген маршрутизатор (кейде оны маршрут сервері деп атайды) жүргізудің бірнеше нұсқасын таңдайды. Ол желінің барлық маршрутизаторлары үшін маршрутизация кестесін құрады, кейін оларды желі бойынша таратады, себебі әрбір маршрутизатор келешекте әрбір дестенің жылжуы туралы шешімді өздігінше қабылдайды. Орталық маршрутизатор белгіленген маршруттар туралы тек ақырғы тораптарға (немесе шекаралық маршрутизаторларға) хабарлауы мүмкін, себебі олар желіге көзден маршрутизация техникасына сәйкес дестелерді беру үшін. Желіде бір емес, бірнеше маршрутизаторлар болуы мүмкін, олардың

әрқайсысы өздеріне тәуелді белгіленген маршрутизаторлар тобына қызмет көрсетеді.

Қазіргі уақытта есептеу желілерінде қолданылатын маршрутты мәліметпен алмасатын адаптивті хаттамалар, өз кезектерінде екі топқа бөлінеді, олардың әрқайсысы келесідегі алгоритмдердің бірімен байланысқан:

– қашықтықты-векторлық алгоритмдер (Distance Vector Algorithms, DVA);

– байланыс жағдайының алгоритмдері (Link State Algorithms, LSA)[7]

2 IP- желілердегі рұқсаттылықты шектеу

2.1 IP – желілердегі виртуалды жалғастырулар

«IP - желі» термині (мұнда IP –Internet Protocol, желі аралық хаттама) техникалық әдебиетте айтарлықтай кеңінен қолданыс тапқанымен, алайда оған бекітілген белгілі қатаң анықтамасын табу қиындық туғызды. Берілген жұмыста IP – желі ұғымында түйіндерден тұратын және осы желі қосымшалары IP – адресті кеңістік пен домендік есімдер иерархиясы жүйесінде TCP/IP хаттамасын қолдана отырып әрекеттесе алатын кең мағынадығы логикалық желіні қарастырамыз. Интернет IP – желінің дербес жағдайы болып табылады. Ол мақсаты, пішімі, архитектурасы, физикалық деңгей технологиялары мен бағдарламалы-аппаратты құралдары әр түрлі болып келетін метажелі.

IP – желілердің қарапайымдылығы мен әмбебептылығы олардың глобалды желілер сондай-ақ жеке шешімдерді (интранет) құруда кең қолданыс тапқанының себебі болып табылады. Алайда бұл шешімдердің екінші жағы болдып желі ресурстарының ақпараттық қауіпсіздігін қамтамасыз ету сұрақтары болып табылады. Осы метажеліні құру ерекшеліктеріне қарай содай-ақ TCP/IP хаттамасының осалдықтарына орай Интернетті қолданған кезде бұл сұрақтар ушығады. Осындай түрлі желілерді ұйымдастыру ерекшеліктеріне кеңінен тоқталып өтейік.

IP – желі ресурстары және функциялану принциптері.

Интернеттегі әрі IP – желілердің дербес жағдайындығы ақпаратты қорғау, қолданау және ұйымдастыру тұрғысынан қарағанда, келесі модельдер, механизмдер мен принциптер маңызды болып табылады:

– TCP/IP хаттамалар түйісі және эталонды моделі;

– дестелер коммутациясы принципі;

– басқаруды орталықсыздандыру.

Кез-келген IP – желі незізделетін өзекті түсініктер болып TCP/IP эталонды моделі және оны жүзеге асыратын хаттамалар түйісі болып табылады. OSI жеті деңгейлі эталонды моделіне қарағанда, TCP/IP моделі RFC-1122 сәйкес төрт деңгейден тұрады. Әр түрлі әдәби көздерде олардың әрқалай аталатынын айтып кету керек. Осыған сәйкес, модельдің әр деңгейіне

сәйкес келетін, TCP/IP хаттамасы түйісінің әр модель деңгейінің сәйкесінше келетін аты мен мақсаттырын атап көрсетейік.

Арналы деңгей локалды желінің кез келген түйіндері арасында кадрдың жеткізілуін қамтамасыз етеді (бұл деңгей берілген жұмыста қарастырылмайды).

Желіарадық деңгей IP – дестелерді хост-көзден хост-қабылдағышқа дейін құрама желі арқылы жеткізуге арналған. Дестенің желі бойынша жүруі қабылдаушының IP – адресі және желінің аралық түйіндерінің маршрутты ақпараты негізінде жүзеге асырылады. Желілік деңгей хаттамалары IP (4 және 6 ұсыным), сондай-ақ маршрутизаторлар арасындағы маршруттар жайындағы ақпататты таратуды қамтамасыз ететін динамикалық маршрутазация хаттамалар (мысалы, BGP, OSPF).

Транспорттық деңгей әр түрлі компьютерлерде, талап етілетін сенімділік дәрежесінде, жүзеге асырылап жатқан қосымшалар арасында ақпарат таратуды атқарады.Транспорттық деңгейдің ең кең таралған түрі болып TCP және UDP болып табылады. TCP хаттамасы ағындарды басқаруды қамтамасыз етеді әрі желілік қосымшалар арасында логикалық жалғастаруларды орнату және квитирлеу механизмі негізінде қолданбалы қосымшаларды сенімді түрде таратуды қамтамасыз етеді. UDP желілік тораптар арасында максималды жылдамдықпен логикалық байланыс құрмай деректерді таратуға мүмкіндік береді, алайда деректердің сенімді таратылуын қамтамасыз етпейді.

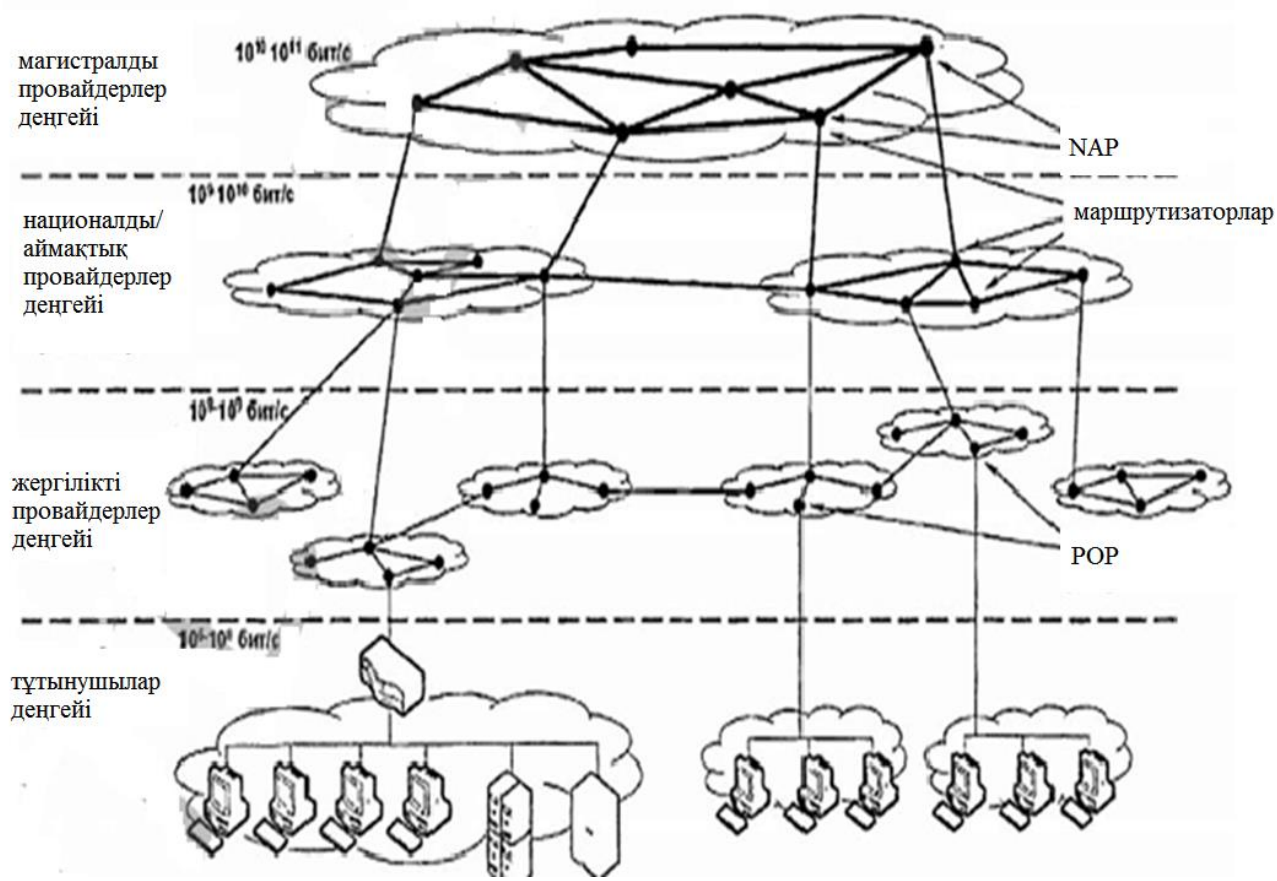
Қолданбалы деңгей тұтынушы олардың көмегімен ажыратылатын желі ресурстарына сондай - ақ сол желі ресурстарымен бірігіп жұмыс істейтін хаттамалар жиыны болып табылады. Бұл деңгейде электронды пошта (SMTP, POP3, IMAP хаттамасы), файлдарды тарату (FTP хаттамасы), бүкіләлемдік желі (HTTP хаттамасы), қашықтықтан басқару (Telnet, SSH хаттамалары), сондай-ақ заманауи операциондық жүйелермен қолданылатын басқа да хаттамалар.

Инернет, басқа да IP – желілері сияқты дестелер коммутациясы бар дестеде болып табылады. Ол таратылуы тиіс ақпарат белгілі пішімді блоктарға бөлініп, содан кейін басында белгісі бар IP -дестелерге инкапсуляцияланады да құрама IP – желі бойынша бір бірінен тәуелсіз түрде таратылады. Барлық таратылуға тиіс ақпараттың бағыты, яғни адресі IP - дестенің басында орналасады. Сондықтан, IP - желі барлық тораптары,соның ішінде ақпаратты қорғау құрылғылары, желі құрылғылары арасында деректерді таратуда қолданылатын кішкентай ақпаратты блоктарды құрайтын дестелерді өңдеуге негізделген.

Интернетте біртұтас басқару орталығы жоқ. Адресті қорлардың (IP - мекенжай, домен аттары) біртұтас техникалық саясатты, стандарттардың өндіруі және үлестірілу сәйкес келетін органдар бар. Жұмысқа қабілетті күйдегі желінің қолдауы әкімшілікпен және интернет кіретін (ұлт аралық, аймақтық, қалалық, жергілікті) жеке желілердің техникалық қызметтерімен қамтамасыз етіледі. Бұл желілер техникалық деңгейде біртұтас стандарттар

бойынша бір-бірімендерді әрекеттеседі, әкімшілік деңгейде тараптар арасында қабылданған экономикалық және саяси шарттармен сәйкес әректетеседі. Басқаруды орталықсыздандырудың қағидасы желілердің санының үлкеюіне оң ықпал етеді, алайда ақпараттық және есептеуіш қорлар салдар және желілер ол үшін ақпараттық қауіпсіздікті қамтамасыз ету мәселелері шешімінде теріс әсерін білдіреді. Іс жүзінде әрбір ұйымның қажеттілігінің басқаруын орталықсыздандыру салдары болып жеке ақпаратты қорғау жүйесінің қолдауға шамасының болуында болып табылады.

Интернеттің логикалық және физикалық құрылымын ажыратыды. Физикалық құрылым нақтылы түрінің (пассивті жабдық) байланыс канал бірлескен (белсенді жабдық) түйіндерінің жиыны болып табылады. Осындай иереархия мысалы 2.1-суретте келтірілген. Рұқсаттылық деңгейлері бір бірінен мақсаттылығы әсіресе қолданылатын құрылғылардың классымен және байланыс арнасының өткізу жолағымен ерекшеленеді.

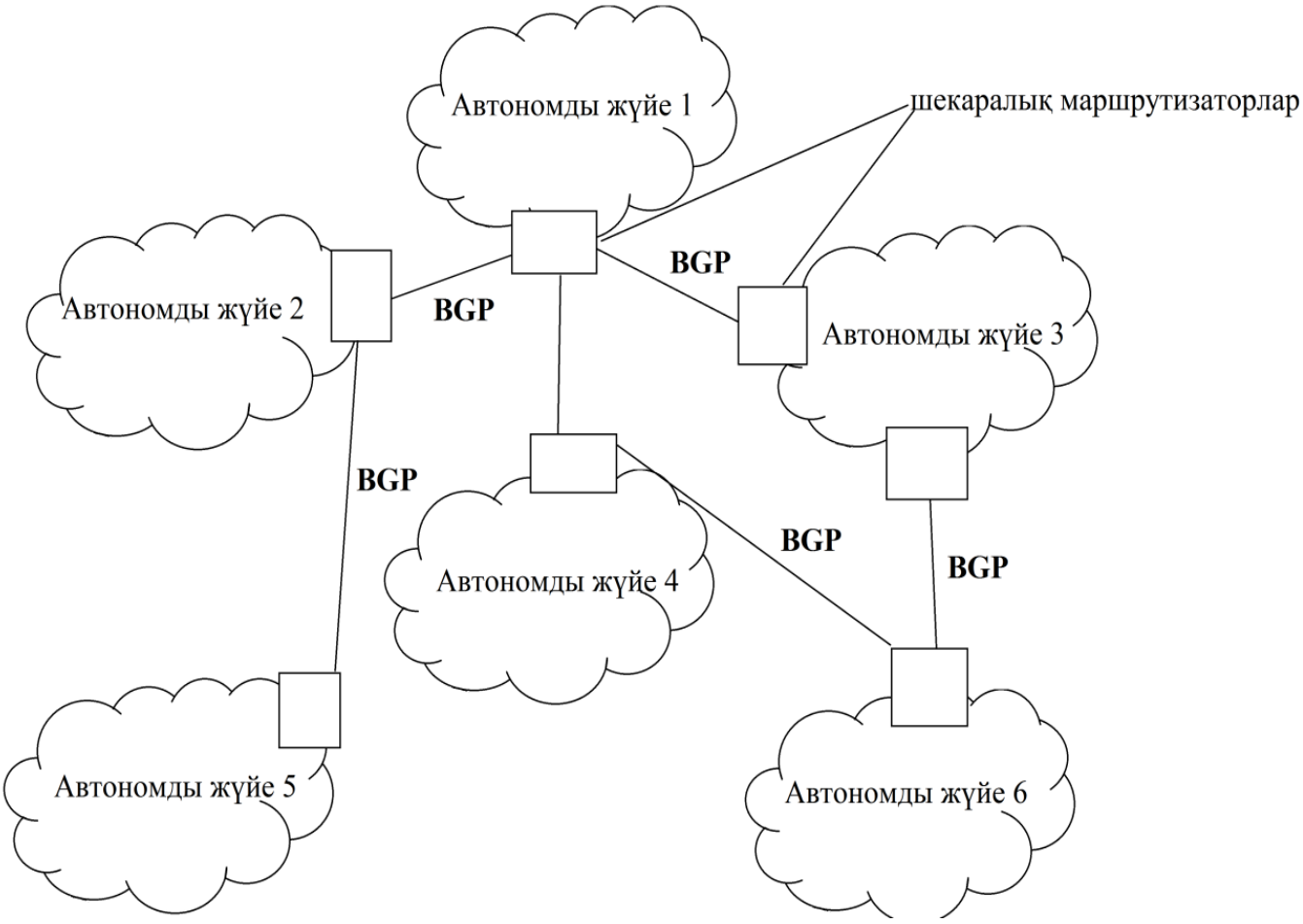


2.1 –сурет. Интернеттің физикалық құрылымындағы желі рұқсаттылығының деңгейлері иерархиясы

Деңгейлердің келтірілген иерархиясы интернеттің физикалық құрылымы туралы ортақ ұсыныстардың жүйелеуі үшін келтіріледі және желі қазіргі байланыстардың барлық күрделілік мен алуантүрлігін толық қамтып көрсетпейді. Бұған қарамастан, ақпараттық қауіпісіздік жүйесін жобалауда

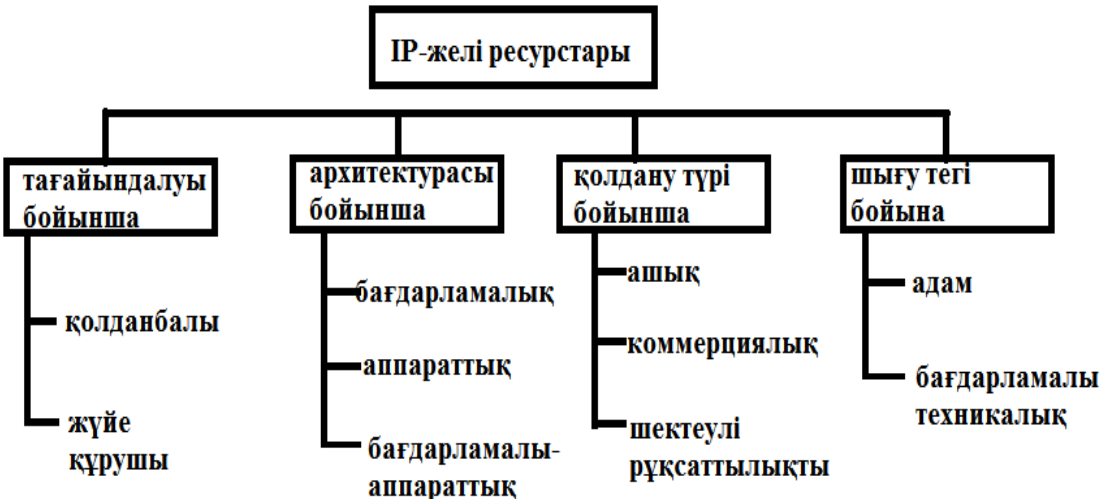
интернеттің физикалық ерекшелік құрылымын және, құрылымның иерархиясының деңгейінің IP-желісіне қосылатын ұйымның метажелісін есте сақтау керек. Әдетте бұл жергілікті және аумақтық провайдерлер деңгейі.

Интернетінің логикалық құрылымы үшін анықтайтын маршрутизацияның саясатына бәрімізге ортақ AS-ке кіретін жол көрсетуші қамтамасыз ететін біртұтас әкімшілік басқарумен желілерінің жиынтығы болатын автономды жүйе (Autonomous System, AS) ұғымы болып табылады. Маршрутизация саясаты деп IP-дестелердің жүру маршруттарының есептеуінде бұл процесстердегі саяси және экономикалық құраушыларды есепке алатын жолдарды атайды.



2.2 – сурет. Интернеттің логикалық құрылымының қарапайым сұлбасы

Мұндай жолға сәйкес және орталықсыздандырудың қағидасына негізделе отырып, интернеттің логикалық құрылымы кез келген түрінің өзара шекаралы маршрутизаторлар арқылы бірлескен автономды жүйелерінің бір деңгейлі (жазық) жиыны болып табылады. Көрші ASтердің шекаралы маршрутизаторлары маршрут мәліметін айырбас үшін BGP (Border Gateway Protocol, шекаралы шлюздар хаттамасы қолданады. Интернеттің қарапайым құрылымы 2.2 суретте келтірілген .



2.3 –сурет. IP-желілердің ресурастары классификациясы

BGP хаттамасы шешетін негізгі мәселе болып Инетрнеттегі логикалық байланысты қамтамасыз ету табылады. Бұл түсінік графта байланысы теориясына ұқсас болып табылады. Соған сәйкес граф байланысқан болып табылады, егер оның кез келген жұп төбелері арасында кем дегендет екі жол болатын болса.Бұл Интернет үшін желі қондырғысының жұмысын қамтамасыз ету болып табылады және осы орайда IP-десте құрама желінің бір белгілі компьютерінен басқа бір комьютерге таратылуын айтуға болады.

Сайып келгенде, орамдылық ұйымдар және тұлғалардың бөлінділерінің желісі бас себеп қосуда осыған болып табылған интернеттің қорларына рұқсаттың алуы үшін қажет. Интернеттерде өте қажетті қорлар ақпараттық қорлар болып табылады, бірақ олар қорлардың жалғыз түрлері болып табылмайды. 2.3 - суретте IP- желілердегі қорлардың классификациясы келесі белгілер бойынша классификацияланған: тағайындалуы, архитектурсы, қолдану әдісі және тегіне байланысты.

IP - желілер қорлары әр түрлі терминдерде сипаттала алатын желілік мәндердің арасындағы ақпараттық өзара әрекеттесуді мүмкіндік қамтамасыз етеді: клиент - аттас үлгімен сәйкесінше, рұқсаттылықтың логикалық шектеуінің үлгілерінің терминдеріндегі субъект-объект, желілік операциондық жүйелердегі процесс аралық әрекеттесуі және басқалары. Сипаттау әдісінен тәуелсіз түрде мұндай өзара әрекеттесу бір немесе екі жақа бағытталған IP-дестелер ағынын құраумен қатар жүргізіледі. Рұқсаттылықты шектеу мәселелерін қарастырған кезде IP-желілердегі осы ағындарға байланған түрде желіаралық экрандармен өңделетін IP-дестелерді қарастыру маңызды. Бұл рұқсаттылық субъектін тұтынушыға дейінгі дәлдікпен (тек қана IP-десте жеке қарастырылатын кездегі IP-адрес бойынша ғана емес), ал рұқсаттылық объектін рұқсаттылық семантикасына дейін қадағалауға мүмкіндік береді. Желілік қосымшалар арасындағы әрекеттесу сеансын белгідеу үшін «виртуалды байланыс» термині қолданылады. Және соны толығырақ қарастырайық[13].

2.2 Виртуалды байланыс IP-желі қосымшаларының өзара ақпараттық әрекеттесуін сипаттау әдісі ретінде

Қолданылатын виртуалды байланыс терминнің жан-жақты түсіну үшін түпдеректерге шолу жасайық, яғни стандарттар және басшылыққа алынатын құжаттарға. X25 желілеріндегі мәліметтің таратылу процедураларының регламент элементтерін белгілейтін ГОСТ26556-85, виртуалды байланысты дектерді таратудың дестелер коммутациясы негізіндегі қызметі ретінде және ондағы жалғастыруды орнату мен жалғастыруды аяқтау процедурасы абоненттік деректер таратылатын әрі байланыс уақыты соңғы деректер құралдарымен анықталатын, деркетер желіден желіге келген ретпен ғана жеткізілетін байланыс түрі ретінде анықтайды. Басқа анықтама оптоталшықты желілердегі асинхорнды тарату режимін сипаттайтын (Asynchronous Transfer Mode, ATM) РД 45.195-2001 салалық басқару документінде көрсетілген. Бұл құжат виртуалды байланысты виртуалды арна немесе тракт соңғы нүктелері арасындағы жұмыс істейтін логикалық жиын ретінде қарастырады. Көріп тұрғанымыздай, деректерді тарату технологиясының әр түрлілігіне байланысты (ATM немесе X25) втртуалды байланыстың анықтамасы пішімі және мазмұны бойынша ерекшеленетінін көріп тұрмыз. Кейбір авторлардың пікірі бойыша ол ақпараттық ірекеттесудің түрлі аспекттеріне байланысты.Алайда виртуалды байланыс терминімен анықталатын құбылысытың ATM және X25 желілері үшін ортақ жақтары айтарлықтай бар. Жалпы жағдайда аталған деректерді тарату технологияларында виртуалды байланыс деп жалғастыру басында құрылып және жалғастыру аяқталғаннан кейін жойылатын логикалық байланысты айтады. Осы жағдайда виртуалды байланысты орнату процессі деректерді таратудың соңғы және аралық қондырғылары арасындағы желілік ресурастарды (өткізу жолағы, оперативті жады, порттар номері, арналар) резервілеумен қатар жүреді.

IP-желілерге арналған виртуалды байланыс үшін нормативті құжаттарда негізделген аталмыш анықтаманы табу мүмкіндігі болмады. Алайда, IP-желілерлдегі құрылғылардың жұмысын және проктоколдар қызметін сипаттайтын көптеген әдебиеттерде зерттреліп отырған термин аталып өтіледі. Мысалы, желіаралық экранға заңсыз рұқсаттылықты сипаттайтын басқарк құжатында бір талаптарында «транспортты деңгейде виртуалды байланыстарды орнату фильтрациясы» талабын атап көрсетеді. Ал желіаралық экрандардың классификациясын келтіретін транспортты деңгейдегі дестелі сүзгілер арасында былай айтылады: «транспорты экрандау виртуалды байланыстарды бақылау мен олар бойынша ақпаратты тасымалдауға мүмкіндік береді». Және келесіде: «дестелі сүзгілермен салыстырғанда, транспортты экрандаудың ақпараты көп болып табылады, сондықтан желіаралық экран виртуалды байланыстарды дәлірек бақылауға мүмкіндігі бар(мысалы, ол таратылап отырған ақпаратты бақылап отырып,

ббелгіді шеккке жетккенде байланысты үзуге мүмкіндігі бар және ол осы жолмен ақпарат экспортының заңсыз рұқсаттылыққа кедергі бола алады)».

Сонымен, жоғарыда айтылған ақпараттарды ескере отырып келесідей қорытынды жасауға болады: виртуалды байланыс деп, берілген жұмыста, желі қосымшалары арасындағы, түрлі IP-желілері түйіндарі арасында жүзеге асырылатын, ақпараттық өзара әрекеттесуі процесін айтуға болады. Осы процедура төңірегінде жалпы жағдайда үш деңгейді ажыратуға болады.

Байланысты орнату өзара жұмыс істе қосымшалар орындалатын соңғы хосттар (егер бұл керек болса) сонымен бірге аралық шеткі орналасқан барлық аралық хосттар ақпараттық айырбастың жүзеге асыруы үшін қажетті қорлардың сақтауы қажетті өндіріп алады. Қосу анықтаулары бастаушы (белсенді тарапты), клиент үлгімен сәйкес, клиентпен дейміз, онда сервермен уақыт арқылы клиентпен байланыс орнатуға тырысқан (пассивті) тарапты деп атаюға сияқты.

Бір немесе екі бағытталған ағынның құру арқылы пайдалы мәлімет болатын IP – дестелермен деректерді тарату.

Байланысты аяқтау байланысты орнату барысында резервіленген ресурстар босатылады.

Желілік және көлік деңгейлердің қолданылатын хаттамалардың бұл кезеңдеріне байланысты бөлшектердегі өзгешелене алады. Мысалы, деректерді тарату TCP хаттамасы бойынша қосу онату кезеңде мүмкін емес, ал UDP хаттамасы бойынша деректерді тарату кезеңі байланысыт орнату кезеңімен біріктқрілген. TCP хаттамасы байланысты аяқтаудың анық процедурасын қолданады сонымен бірге, UDP хаттамасы үшін басқару, мұндай процедура тағы басқалар ICMP сияқты хаттамаларда ескерілмеген, және байланыстың аяқталуы анық емес болады.

Сонымен, виртуалды байланыстың IP-ші кейбір жиын жұмылған түрде бола алады - ұйымдастырған және желілік қосымшалардың арасындағы шеңберінде ақпараттық айырбасты тапсырылған дестелер. Демек, тап қалған түйін үшін кез келген виртуалды байланыс мұндай IP-ші тізбегімен бірмәнді анықтала алады - дестелер. Бұл қолдану бұдан әрі рұқсаттың шектеуіне жолдың дәйектемесінде IP болатын маңызды жағдай виртуалды қосулардың параметрлерінің талдауын негізде желілер атап өтеміз. Қосулардың параметрлерінің талдауын негізде желілер атап өтеміз. Бұдан әрі виртуалды байланысқа бұл жағдайымен сәйкес торлық қосымшалардың торлық қорлардың логикалық ұйымымен бұл сабақтас өзара әрекеттесулерін өздің процедурасынғана емес, IP-десте тізбек - осы процедура шеңберінде өңдеген деп түсінеміз.

Жоғарыда айтылғандай, IP-желілердегі виртуалды байланыс қосымшаларының өзара әрекеттесу бір жақты және екі жақты бағытталған бола алады. Бәр жаңа бағытталған виртуалды байлаынста IP- дестелер клиенттен серверге ғана бағытталады. Ол айтарлықтай сирек жағдай және оның мысалы болып IMCP эхо сұраныстар болуы мүмкін[13].

2.3 IP – желілердегі рұқсаттылықты шектеудің мәселелерін шешудің қолайлы жолдары

Виртуалды байланысты параметрлердің талдауын негізде рұқсаттың шектеуін негізгі идея қарастыруда әрбір IP дестені бір жаңа виртуалды байланысты ұйымдастырушы виртуалды байланысқв тәуелді ретінде қарастыру. Параметрлер де, хаттама бастары және мәліметтердің ішкі құрылымы да ұйымдастырушыға капсуладан шығарылған хаттамасына байланысты, сонымен бірге барлық келесі IP – дестеге IP-ші алуды уақыт есепке алатын қатысты әр түрлі талаптарының көрсетеді. Мәндер де, қабылданған дестенің бастарының параметрлері де мүмкіндік немесе рұқсаттың тыйымы туралы шешім талдау негізінде қабылданады, деректерді өңдеу виртуалды байланыс күй кезге IP мінездейтін параметрлер дестесі.

IP – желілерінің объекттеріне алып тастаған шабуылдардың жүзеге асыру мүмкіндігі. Бұл шабуылдардың мақсаттары, бұрын келтірілген классификацияға сәйкес, құпия ақпаратқа заңсыз рұқсаты, мәліметтің бүтіндігін бұзу, олардың қол жетімділігін шектеу болып табылады.

Интернетті қоғамның тіршілік әреткеттерінің барлық салаларында қолдану, әр түрлі объекттердің ақпараттық қауіпсіздігінің бұзылу ықтималдығын жоғарылатады, соның ішінде ұлттық қауіпсіздікті қатамасытамасыз етуге де.

Дерекөздердің мәліметтері бойынша, IP желілерде ақпараттық қауіпсіздік қорғаныс объектісінде қауіпсіздікті жүзеге асыруының келесі техникалық әдістері бүгінгі күнге көкейкесті болып табылады:

– зиян келтіретін бағдарламалық қамтамасыз ету;

– сұраусыз (спам) мәліметтің алуы;

– «троя» бағдарламалары;

– жалған ақпараттық қорға сұрау салуды қайта бағыттаудамәліметтердің құпиялығыны бұзылуы(фишинг);

– «қызмет көрсетуден бас тарту» түрде таралған шабуылдары(DDoS - шабуыл);

– қорлардың компрометациясы(бұзу);

– ботнетов - желілер, жасырын түрде қойылған программалық қамтамасыз етуі бар, жасырын қызмет үшін қолданылатын компьютер тұратын желілер жасау, соның ішінде спамды тарату және таралған шабуылдардың ұйымы;

– IP – желілер қорларын мақсаттық емес қолдану, сонымен бірге ұйымның қызметімен үйлесімді емес ақпаратқа қол жеткізу;

– бағдарламалық қамтамасыз етудің қателері және тағы басқалар.

IPжелілердің архитектуралық ерекшеліктерін пайдаланатын өте көкейкесті шабуылдар мыналар болып табылады:

– жасырын тыңдау(sniffings);

– мәліметтердің өзгерісі;

– желілік трафиктің талдауы;

– сенімді субъектіні ауыстырып жіберуі;
– шифрланбалған кілттерді айырбастағы делдалдық;
– сеанстықағып алу (session hijacking);
– құприя сөз шабуылдары;
– қосымшалар деңгейіндегі шабуылдар.

Жойылған деструкциялы әсерлер шабуыл объектісінің ашықтылығын бұзатын, қызмет көрсетуді қабыл алмағанда кездегі шабуыл класына жатады. Шабуылдардың бұл класы косымшаның күйреуіне, жүйенің қайта қосуына, жүйелік қорлардың тапшылығына, желінің өткізу қабілетінің төмендетуіне және автоматтандырлған жүйенің штаттық жұмыс жасау процесін бұзатын тағы басқа оқиғалар.

Қазіргі уақытта қызмет көрсетуді қабыл алмаған кезіндегі шабуыл ұйымдары келісім механизімі белгілерін тасиды, олар бәсекешілердің беделін түсіруі, бопса мақсаттарындағын, кибертеррорлық қызмет мақсатында қолданылады. Мұндай шабуылдардың объекттері интернеттің әр түрлі желілік қорлары болып табылады, соның ішінде электрондық төлемдердің жүйесі, жаңалықтар порталдар, компанялар сайты, әр түрлі мемлекеттік қызметтердің порталдары. Осыған байланысты бұдан әрі IP-желілердің қорлар көмегімен өңделетін үлгі, әдістер және желілердің жұмыстанылатын ақпаратына қорғау құралын қарап шығамыз.

Ақпаратты қорғау жүйенің автоматизацияланған жүйесін,соның ішінде IP-желілерде таралғанынқұрған кезде, ақпараттық қорғанысқа келтіретін қауіпке қарсы әрекеттің келесі әдістерін қолданылады:

– ақпараттық қорғаныс саясатыбасқару стратегиясын және қолданылатын шаралар тактикасын, ұйымның қорларының қорғауы үшін ақпарттық қорғанысқа келтірілетін қауіпке төтеп беретін әдістер мен қарсы әрекеттерді анықтайды;

– ақпараттық өзара әрекеттесу процессінің әрбір қатысушысын анықталуға (айырып тану)мүмкіндік беретін идентификация;

– аутентификация,ақпарат алмасу процессіне қатысушысы дұрыс идентификацияланғанына сенімділікті қамтамасыз етеді;

– рұқсатты басқару, әдістер және өкілеттіктердің тексеруі құралдарының ұсынатын жиынтығы субъекттердің объекттерге үндеулерінде;

– субъекттер мен объекттердіңжелілік әрекеттесуінде өкілеттік өзара тексеруін өткізуге мүмкіндік беретін фильтрлеулер және экрандау;

– мәліметтерді қорғау,ақпаратты сақтауғаберілуде шифрлаудың және стеганографияны қолдану құралдары және тиесілі қорғауы;

– вирусқа қарсы қорғау, программалық құрал және компьютерлердің вирус жұқтыру ықтималдылығын төмендететін шара;

– аудит және мониторинг, ақпараттық алмасу процесінде болып жататын оқиғалардың жүйелі зерттеп отыру және талдауы өткізуге мүмкіндік беретін барлау;

– инциденттерге қарсы жауап беру, ақпараттар қауіпсіздігі қорғау объектілерінің бұзылуына күдік келтіру немесе бұзылуы кезінде процедуралар мен іс-шараларын орындау;

– кескінмен басқару, ақпараттық алмасуды құру мен қолдауды қаматасыз ететін жұмысқа қабілетті күйі;

– ақпараттық қауіпсіздік саясатының талаптарына сәйкес ақпараттық алмасу ортасын қолданушылармен басқару;

– тәуекелдермен басқару, ақпаратты қорғау жүйесін қолдауға кеткен шығын мен ақпарттық қауыпсіздік саясатының бұзылуы сәйкестіктіңжоғалуларымен болуы мүмкін;

– деструкциялы әсерлердің шарттарындағы ақпараттық қауісіздік саясаттың талаптары минималды мүмкін жұмысқа қабілетті күй және сәйкестіктегі ақпараттық алмасу, ортаның қолдап отыру үшін орнықтылықтың қамтамасыз етілуі.

Ақпараттық қауіпсіздіктің негізді аксиомаларының бірінде былай айтылады: «ақпарат қауіпсіздігінің барлық сұрақтары субъекттердің объекттерге рұқсаттарының сипаттамаларымен анықталады». Осыған байланысты қолданылатын негізгі әдістер ақпараттық қауіпсіздік объектілерінің табиғатын қамтамасыз етуде қолданылатын рұқсатын басқару болып табылады. Бұл әдісті толығыраққарап шығамыз.

Ақпарат қорғаудың қамтамасыз ету саласындағы сұрақтарда субъектпен және объекттің арасындағы қатынасы рұксттаылыққа қатысы бар операциялық типте әрекеттесудің мағынасы жағынан ұқсас термин бар болады. Бұл «рұқсаттылықтың бақылауы», «рұқсаттылықтың шектеуі», «рұқсаттылықты басқару» терминдеріне сәйкес келетін жалғыз ағылшын жалпылама термині «access control». Осыған байланысты бүл терминдердің қолданылуы көбіне қиындатылған, себебі, бұл терминдердің әрқайсысының ерекшеліктері ақпарат көздерінде жеткіліксіз айтылмаған. Бұл ерекшеліктер мынадай:

Рұқсаттылықты басқару (control ағылшынша - қадағалау, бақылау, тексеру) субъекттердің объекттерге рұқсаттылығының процедураларын қадағалаудың пассивті (орындалуына ықпал етпейтін) әдісі, мысалы, хаттама жүргізу. Басқару ұғымымен жиі қатар пайдаланылады,атап айтқанда: «бақылау және рұқсаттылықты басқару».

Бұл жерде рұқсаттылық процедурасын құрайтын активті және пассивтінің айырмашылықтары ерекше көрсетіледі.

Рұқсаттың шектеуі субъектінің объектіге үндеуінде өкілеттіктерін анықтайтын рұқсаттылық саясатынан, және осы саясатты жүзеге сыратын саясаттын тұратын қауіпсідік сервисі болып табылады. Рұқсаттың логикалық және физикалық шектеулерін танып біледі. Мысалы, рұқсаттылықтың логикалық шектеулігі аты аталған субъектілердің (қолданушылар, процесстер) аты аталған объектілерге (қорларға, процесстерге, құрылымдарға) және программалық-техникалық қорғау құралдарыменүлгілердің біреуінің

негізінде мәліметтің рұқсаттылық логикалық шектеуі. Рұқсаттылықтың физикалық шектеу процедурасы деңгейі шаралардың бөлшегі болып саналады және баспана қорғалатын аумаққа субъекттерінің және басқа ұқсас объекттергерұқсатын тексеріп шек қоюға мүмкіндік беретін.

Рұқсатты басқару –айтылғандардың арасындағы ақпаратты қорғау әдісін анықтайтын, идентификация, аутентификация, авторизация, фильтрация, рұқсаттылық логикалық немесе физкалық шектеуін жүзеге асыру ұшін хаттама жүргізу сервистерін қолданады.

Виртуалды қосулардың күй бақылауға қатысты жол үшін ағылшын тілді әдебиетте (SPF) Stateful Packct Filteringнің термині немесе (SPI) Stateful Packet Inspection қабылданған. Бұл терминдер Stateful Inspectionнің атының вариациялары болып табылады. FireWall-1ді технологияи өз желі аралық экранын тұңғыш рет қолданылған фирма Check Point Software Technologies. Бұл технологиямен, шлюз, бағдарлаушы басқару жүйесінің ядросына FireWall-1дің программалық қамтамасыз етуін қоюдың жанында сәйкес INSPECT-ші (Check Pointтің терминологиясы бойынша виртуалды машина) модулды жүктеледі және торлық хаттамалардың стегінің жыралық және тор аралық деңгейінің аралығында орын алады. Нәтижеде бұл, INSPECT-ші модул арқылы барлық IPлерді өтеді - осы шлюзбен тор аралық деңгейде өңдеулерге жататын паксты. INSPECT модул виртуалды байланыс күйлерді динамикалық кестеде виртуалды байланыстың барлық белсенді дәл осы кезделеріне туралы барлық көкейкесті мәліметті болды. Әрбір түскен INSPECT IP - десте өз виртуалды байланысының ағымдағы күйіне сәйкестікке тексереді, кейін жоғары жатқан деңгейлерге өңдеуге не беріледі. Statful Inspection технологиялар қолданбалы деңгейдегі салыстырғанда дестені фильтрлеумен және фильтрлеудің маңызды артықшылықтарын береді. Бөлек, байланусыз виртуалды қосуға десте әрбір IP өңделетін дестелі сүзгілер жеке алғанда, қолданбалы деңгейдің мәліметтерін талдамайды. Бұл қайта құрылған виртуалды Қосулар үшін порттардың нөмірлерінің динамикалық тағайындаулары өндіріп алатын хаттамалар бойынша өзара әрекеттесуді ұйым рұқсаттың саясатты бұзылысының себебімен қажеттілік жағдайда қызмет көрсете алады. Мұндай қабылдаумен FTP-дің файлдар тапсыруының хаттамасы, Oraclc SQL*Nettің торлық өнімі, шақырудың тетіктерін пайдаланады RPC-тің алып тастаған процедурасы, мультимедиа осы SIPлерін айырбастың хаттамасы және кейбір басқа. Торлық мәліметтердің өткізе өңдеуі қолданбалы деңгейдің шлюздерінің кемшіліктерімен көздің нүктесімен клиенттің үлгінің үзілуінің қажеттілігі және екі виртуалды байланысытң ұйымы болып табылады: клиент - шлюз және шлюз. Нәтижеде бұл шлюздың жүйелік қорларының саны көбірек айтарлықтай шығын шығарады, сонымен бірге торлық өзара әрекеттесу үшін қажетті ортақ уақыт қажетті үлкееді. Бұдан басқа, әрбір қолданбалы хаттама шлюздағы меншікті бағдарламаның жұмыс жасауы талап етеді. Сонымен бірге сонымен бірге IP-ші қорларға рұқсаттың тақырыптық шектеуі тиісті жүзеге асыратын қолданбалы деңгейдің шлюздерінің мүмкіндіктерінің кең спектріне ішіндегі торлық айырбастың

вирусқа қарсы талдауы жеке алғанда беруге керек - пошталық және лездік қатынастардың трафиктің бақылауының тағы басқа түрлері желілер. Stateful Inspection технология (клиент үлгінің үзілуісіз) Вс-тің күйлері және тиісті модулдардың қолданбалы деңгейдің осы хаттамаларын талдауы дестелі сүзгілер және қолданбалы деңгейдің шлюздерінің белгі қойылған кемшіліктері бақылау есебінен жеңуге мүмкіндік береді. Мысалы, Тср динамикалық ашуды есеп жеке алғанда қажетті осы уақытта – FTP-дың хаттамасына бірақ деректерді беруі үшін қосымша виртуалды байланысытың ұйымы үшін порттары) қайта ұйымдастырылатын қосу үшін порттардың нөмірлерінің виртуалды байланыстың қажетті бағдарлаушы мәндерінен шығаруы жолымен ұйғарылады. Осы FTP-лар сияқтығаннан кейін тапсырылады, қолданылатын порттар тор аралық перделермен қайта тосқауыл қояды.

Қазіргі уақыттағы бар (байбаламдардан қорғаумен UTM, бір ізге салған басқару) Unified Threat Managementтің жолы, ақпараттық қорғаныс сервистерінің жиыны сәйкес, соның ішінде және Трға рұқсатының шектеуі - желілер, біртұтас бағдарламалы-аппаратты платформаларда жүзеге асырылады.

Ұқсас жол іске асыратын бастаушы өндірушілердің құрылымдарының жұмыстың ерекшелігі және функционалдығын қарап шығамыз.

(Check Point Software Technologies) UTM-1. Check Point серіктестігінің өнімі желілердің ақпарат қорғау IP қамтамасыз етуге қатысты әр түрлі есептері үшін программалық және бағдарламалы-аппаратты шешімдердің алуантүрлігімен айырмашылығы болады. UTM-1 өнім сызғышты программалық болады - әрбірі қажетті (Check Pointтің терминологиясы бойынша блэйдов) модулдардың қосындысы өз функционалдығын ол көрсетілетін талаптарға байланысты жолымен өсіп жетілдіруге мүмкіндік берген масштаб жасалатын құрылымдар. Негізгі модулдар төменде атап көрсетілген, UTM-1дің барлық сызғышы, қолдалатын мүмкіндіктердің қысқаша тізімімен үшін түсінікті.

Желі аралық экран: Kazaa, Gnutella, BitTorrcnttің нүктенің желілері үшін 200 хаттамадан астам және қосымшалар, NAT, MSN, Yahoo, Skyreның лездік қатынастарының айырбасымен басқаруды S1P және H323, мультимедиа трафигінің қорғауы, Skype, қосуларды одақтасу қолдау. AES-тың шифрлауын IPsec VPN: қолдау, 3DES, VPN, SSL-ның негізінде алып тастаған рұқсатты клиенттердің жұлдыз және толық байланысты желі, қолдаудың топологияларының кірістірілген куәлік орталық, қолдауын пароль, RADIUS, TACACS, X509, негізінде шындықтың тексеруі.

Басып кірулерден қорғаудың жүйесі: қабыл алмауға шабуылдарының қызмет көрсетуінің бітеу, порттардың сүзіп шығуы; FTP-ның хаттамасы бойынша қосымшалардың DNS-тың қызметінің жадының кэшінің бұрмалауы, шабуылдарынан деңгейденің қорғау сигнатуралардың негізі және хаттамалардың аномалиялы мінез-құлығындағы табылуы.

Вирусқа қарсы бағдарлама және тыңшы бағдарламалардан тіккен: HTTP, SMTP, Pop3, FTP-дың хаттамаларының вирустардан қорғауы схемалардың тыңшы негіз тіліндегі программаларының бітеуі; сигнатуралардың орталықтандырылған жаңартуы.

URL - фильтрлеу: URLның деректер қорын қолданылады - (webтің 3 миллиарды - беттер) мекенжайлар, 70 тілдер, күн сайынғы жаңарту. Антиспам және электрондық почтаның қауіпсіздігі: SMTPның хаттамалары шабуылдардан қорғау, Pop3, IMAP, сигнатуралардың негізі, IP-ші абыройдың тексеруіне жағымсыз қатынастардың бітеуі - пошталық сервердің мекенжайы, вирустардан қорғау, домендер және қолданушылардың қара және ақ тізімдері.

Торлық мүмкіндіктер және сенімділік: жыралық деңгей, қателік жасамайтын кескіннің ұйымы (бірлестігі), қызмет көрсетуді салмақты үлестіру, сапаны қамтамасыз ету, интернеттің қызметтердің резервтегі провайдері, OSPF, RIP маршрутизациясының хаттамалары, жұмыс жасауға мүмкіндік беретін шлюз ретінде.

UTM-1дің сызғышының құрылымдары нарықтың әр түрлі секторлары үшін арналған және торлық интерфейстердің санмен және өткізу қабілеті, бір уақытта қолдалатын виртуалды қосулардың өнімділікпен, саны және аппаратты кескіндерден айырмашылығы болады.

(Cisco Systems) ASA. Cisco Systems фирмасы желілік жабдықтың нарығының дүниелік жетекшісі болып табылады. Мәліметтің қорғау құралдары IP - өндіруші ол үшін желілер (Point Software Technologies Checkтарға қарағанда) қызметтің негізгі бағыттары болып табылмайды, дегенмен Иб-тың төңірегідегін оның шешімі тұрақты сұраныстармен пайдаланады. үйлесімдікпен де, ақпарды қорғау міндеттерінің кең жиынымен де бұл ұғындырылады, бұл өндірушінің бұрын қойылған жабдығымен.

ASA-ның ортақ аббревиатурасымен біртұтас аппаратты платформа жүзеге асырылған (тор аралық перде, басып кірулерді сақтап қалуды жүйе және желілердің виртуалды бөлінділерінің ұйымы) қауіпсіздіктердің үш әр түрлі функционалдық сервистерін түсінеді. Ерекшелік және ASA-ның сызғышының мінездемесін қарап шығамыз.

Меншікті ақпараттық қауіпсіздікті қамтамасыз етуді құрылғыны басқаруы үшін адаптерленген қорғал қалған басқару жүйесі. Cisco Systems фирма желілік жабдықтың нарығының дүниелік жетекшісі болып табылады. Мәліметтің қорғау құралдары IP - өндіруші ол үшін желілер (Point Software Technologies Checkтарға қарағанда) қызметтің негізгі бағыттары болып табылмайды, дегенмен ақпараттқ қорғаныстың төңірегідегін оның шешімі тұрақты сұраныстармен пайдаланады. үйлесімдікпен де, ақпарды қорғау міндеттерінің кең жиынымен де бұл ұғындырылады, бұл өндірушінің бұрын қойылған жабдығымен. (қауіпсіздіктің Adaptive Security Appliance, адапттивті құрылымы) ASA-ның ортақ аббревиатурасымен біртұтас аппаратты платформа жүзеге асырылған (тор аралық перде, басып кірулерді сақтап қалуды жүйе және желілердің виртуалды бөлінділерінің ұйымы)

қауіпсіздіктердің үш әр түрлі функционалдық сервистерін түсінеді. Ерекшелік және ASA-ның сызғышының мінездемесін қарап шығамыз.

Меншікті ақпараттық қауіпсіздікті қамтамасыз етуді құрылғыны басқаруы үшін адаптерленген қорғауға арналған басқару жүйесі.

Statcful Inspectionнің бұрын қарастырылған технологиясының өзімен ұсынатын аналогінің (Adaptive Security Algorithm) қауіпсіздігінің адапттивті алгоритмы.

Сыртқы сервер де, қолданушылардың ішкі деректер қоры да тесіп өткен аутентификацияның технологиясы HTTP, Telnet және қолдануы бар FTP хаттамалары бойынша рұқсатқа қолданушы аутентификациясын сұрау салуда өткізуге мүмкіндік береді, TACACS+ немесе RADIUS.

Хаттамалар және қосымшалардың тексеруі қауіпсіз қолдану үшін қолданбалы деңгейдің мәліметтерінің жұмыстанылатын трафигіндегі талдау ойлайды шешілген (FTP, SQL*Nettың H323,) қосымшалардың ашылатын порттары динамикалық.

Торлық интерфейстердің жиыны, рұқсаттың саясаты, маршрутизация кестесі және әкімдік етумен бір физикалық құрылымның базасында меншікті кескіні бар бірнеше логикалық Мэларды анықталуға мүмкіндік беретін (Cisco - Security Contexttің терминологиясы, қауіпсіздіктің контексті бойынша) виртуалды тор аралық перде.

Құрылымға жыралық деңгей шлюз ретінде жұмыс істеуге мүмкіндік берген мөлдір Мэнің тәртібі.

Қателік жасамайтын кескін схемалар ASA-ның құрылымдарының сенімді жұмыс жасауы қолдану есебінен белсенді - белсенді және белсенді - резервтегі қамтамасыз етеді.

Сонымен қатар UTM-1, Cisco ASA-ның сызғышының өкілдерімен жағдайда бір-бірімен әр түрлі өнімділікпен, аппаратты кескінмен, сонымен бірге құраммен және функциялардың жиынының сандық мінездемелерімен айырмашылығы болады. Құралдардың рұқсаттың шектеулері ортақ ерекшелік IP - ұйымның Ибының саясаттың талаптарының орындау қиналатын желілер қорғалатын объекттеріне алып тастаған деструкциялы әсерлерінің ұйымының мүмкіндігі виртуалыд байланыстың саясат шешілген рұқсаттарынан кейін болып табылады. Әсерлердің автроизацияланбаған ұқсас сортының белгісі төмендетулер үшін қолданылады тағы басқалар әр түрлі әдістер, басып кірулерді табылудың кірістірілген жүйелері, вирусқа қарсы тексеру, берілетін мәліметтердің шифрлауын қосады[13].

3 Есептеу бөлімі

3.1 Витруалды жалғастырулардағы рұқсаттылықты шектеуде тапсырма қойылуы

Виртуалды қосылулар параметрлер анализі арқылы рұқсаттылықты шектеу мәселерін шешудегі негізгі артықшылық – клиент пен сервер арасындағы алмасу сеанстарын желі аралық әрекеттесуден қолданбалы деңгейге дейінгі бақылауға мүмкіндік береді. Мысалы:

– транспортты TCP хаттамасының виртуалды жалғастырудың түрлі фазаларында, оқшауланған шабуылдар әрекетінің параметрлерін бақылау;

– виртуалды жалғастырудың қолданбалы хаттамасын қолданылатын порт номерінен тыс анықтау;

– рұқсаттылықты шектеу саясатына сәйкес, қолданылып отырғын қолданбалы хаттамаға сәйкес, деректерді бақылау;

– бірден көп виртуалды жалғастыруларды қолданатын желі қызметтері үшін қосалқы виртуалды байланыстарды орнату мақсатында ресурстарды автоматты түрде резервілеу (мысалы, FTP хаттамасы бойынша ақпараттырмен алмасу).

Рұқсаттылықты шектеу жүйелерінде виртуалды байланысты идентификациялайтын, IP-желілеріндегі әрекеттесуші қосымшалар жайындағы ақпараттық жалғыз көз болып табылады. Мысалы, WEB браузер бағдарламасы HTTP хаттамасымен TCP танспортты хаттама ретінде қолдана отырып әрекеттеседі[12].

3.2 Витруалды жалғастырудың теориялы-көпмүшелі үлгісі

IP- желілеріндегі рұқсаттылықты шектеудің қарапайым компьютер желісіндегі міндеттермен салыстырғандағы ерекшелігі болып, IP- дестелердің желілік бір сегментінен екінші сегментіне таратылуын түсіндіру мүмкіндігі болып табылады. Бұл жағдайда сараптаудың IP-дестелері негізінде құралатын витруалды жалғастырулардағы рұқсаттылықты шектеу жүйелері болмақ.

Кез-келген желінің торабындағы IP-дестелер виртуалды жалғастырулар арқылы анықталады. Бір виртуалды жалғастыруға жататын, IP-дестелердің «клиент-сервер» үлгісі терминдеріне қойылатын талаптарға толығырақ тоқталайық. Мұндағы, клиент – желілік әрекеттесудің инициаторы, ал сервер – сұраныс бойынша кейбір желілік қызмет көрсететін жақ.

IP-дестелер көпмүшелігі қабылдауыш жақ пен көз болып табылатын жаққа бөлінеді.

Клиент пен сервердің IP-адрестерімен бірдей болуы тиіс.

IP-дестлерге инкапсуляцияланған TCP және UDP хаттамалар бастарындағы қабылдауыш және көзі болып табылатын порт номерлері клиент немесе сервер порттары номерлеріне сайкес болуы керек.

IP-дестеге инкапсуляцияланған хаттама (TCP, UDP немесе кез келген хаттама) көпмүшенің барлық IP-дестелеріне бірдей болуы тиіс.

IP-дестелердің уақыттық оқшауланыу инкапсуляцияланған хаттама ерекшелігін қанағаттандыруы керек. Бұл дегеніміз, кез келген виртуалды байланыстың таратылушысы өңделу барысында екі десте арасындағы уақыттық интервал қанадай да бір белсенділіксіздіктің таймаутынан аспауы қажет. Керісінше болған жағдайда, таймаут өткеннен кейін келіп түскен десте, берілген виртуалды жалғастыруларды сипаттайтын, IP-дестелер көпмүшесіне тиісті болып саналмауы мүмкін.

Бір виртуалды жалғастыруға тиісті, IP-дестелер тізбегін сипаттау үшін көпмүшелер теориясы терминдерінде қажетті белгілеулерді енгізейік.

P–p IP-дестелерінің ақырғы көпмүшелігі. $P=\{p_j\}$, $j=1..|P|$. Бұл көпмүшеліліктің қуатының жоғарғы шегі $|P|$. Бұл желі сегментінде қабылданған IP-дестенің максималды көлемі ретінде анықталады. Мысалы, Ethernet желісі үшін, IP-дестенің максималды көлемі 1500 байтқа тең және, $2^{8\cdot 1500}$ мәнінен аспайды. P көпмүшелілігі берілген желі сегментіндегі IP-дестелерді өзіне қосады.

T−t, IP-дестелердің берілген желі торабына келу уақытымен ассоцацияланатын, уақыттық белгілердің есепті көпмүшелігі. Бұл көпмүшелік санаулы болып келеді. Себебі есептеу техникасы үшін арналған уақыт дискретті шама болып табылады. Уақыттық белгі, бір виртуалды жалғастыруға жататын, IP-дестенің өңдеуге келіп түсу мезетін 10^{-6} с дәлдігімен анықтайды деп есептейік. Бұл бір виртуалды байланысқа жататын, IP-дестелер ағынының статистикалық сипаттамаларын анықтауға жеткілікті болып табылады.

Әрқайсысы уақыттық белгімен ассоцацияланатын, p IP-дестелер тізбегін $\{p_{ti}\}$, $i=1..N$, $N\in[1,\infty)$ ретінде анықтауға болады. Тәжірибе жүзінде $\{p_{ti}\}$ тізбегі ақпараттық алмасу барысында таратылатын деректер сияқты шекті болып келді. Алайда, виртуалды жалғастырулар IP-дестелердің шексіз тізбегі бола алады, егер генерация көзінің инфраструктурасы абсолюстті сеніміді болса. Осындай виртуалды байаныстың мысалы тұрақты түрде қосылған санды бейнекамера ақпаратын IP-желі арқылы тарату болып табылады.

$\{p_{ti}\}$ тізбегі виртуалды байланысты орнықтыра алады, егер де келесі талапатар орындалса: біріншіден, IP-дестелер көпмүшелігінің қабылдауыш жақ пен көзі болып табылатын жақ IP-адрестері клиент пен сервердің IP-адрестерімен бірдей болуы тиіс. Екіншіден, IP-дестлерге инкапсуляцияланған TCP және UDP хаттамалары бастарындағы қабылдауыш және көзі болып табылатын порт номерлері клиент немесе сервер порттары нөмерлеріне сайкес болуы керек. Үшіншіден, IP-дестеге инкапсуляцияланған хаттама (TCP, UDP немесе кез келген хаттама) көпмүшенің барлық IP-дестелеріне бірдей болуы тиіс. Төртіншіден, IP-дестелердің уақыттық оқшауланыу инкапсуляцияланған хаттамалар ерекшелігін қанағаттандыру керек. Бұл деген кез келген виртуалды байланыстың қатар таратылушы, өңделу барысындағы екі десте арасындағы уақыттық интервал қандай да бір белсенділіксіздіктің таймаутынан аспауы қажет. Керісінше болған жағдайда, таймаут өткеннен кейін келіп түскен десте, берілген виртуалды жалғастыруларды сипаттайтын,

IP-дестелер көпмүшесіне тиісті болып саналмауы мүмкін. Сонымен, v виртуалды байланысы келесі теория көпмүшемен сипаттала алады.

$$v = \{ p_{t_i} \}$$
$$i = 1..N$$
$$N \in [1, \infty)$$
$$v_i \subset P \times T : \forall p_{t_i},$$
$$p_{t_j} (i, j \in [1, N])$$
$$\{A_{si}, A_{di}\} = \{A_{sj}, A_{dj}\}$$
$$\{B_{si}, B_{di}\} = \{B_{sj}, B_{dj}\}$$
$$C_i = C_j$$
$$|t_i - t_j| < T_c$$

Мұндағы: A_{si}, A_{sj} – ақпарат көзі IP-адресі

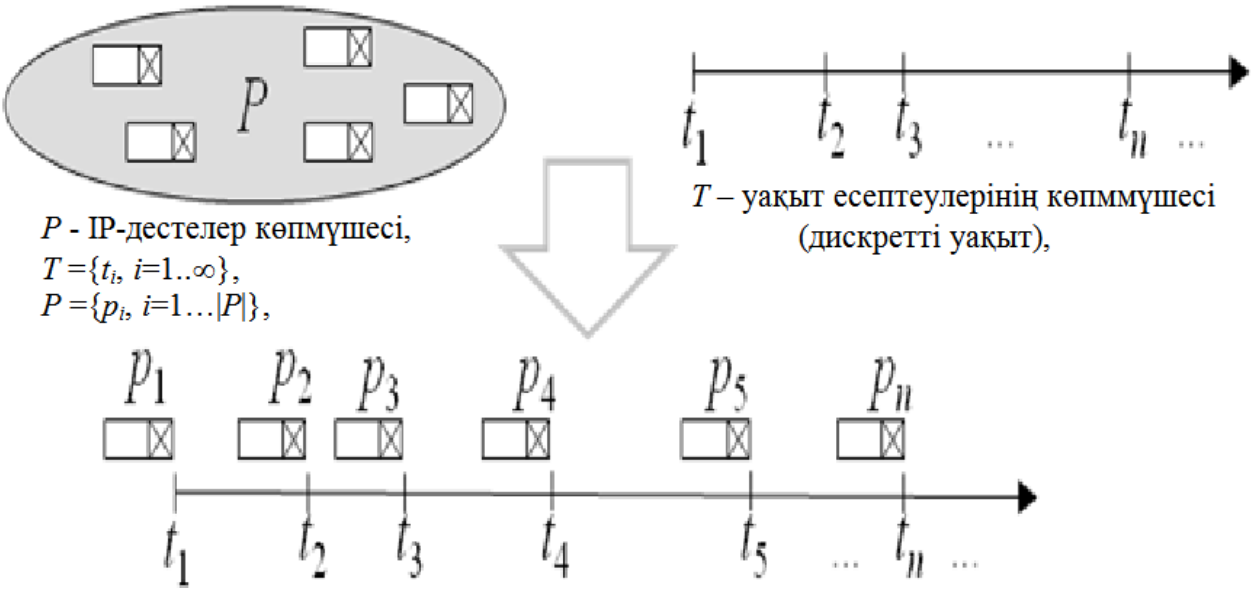
A_{di}, A_{dj} – ақпарат қабылдаушы IP-адресі;

B_{si}, B_{sj} – ақпарат көзі порт номері;

B_{di}, B_{dj} – ақпарат қабылдаушы порт номері;

C – IP-дестеге инкапсуляцияланған хаттама номері;

Тс–берілген хаттама үшін белсенді болмауының таймауты.

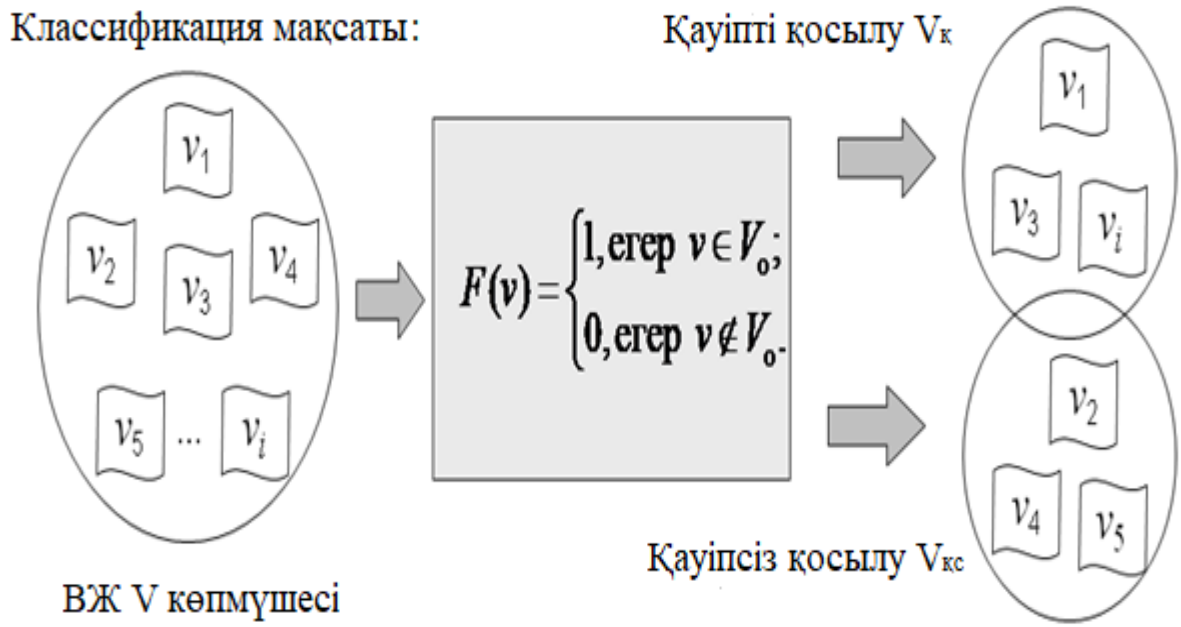


3.1 –сурет. IP-дестелер тізбегі

Бұл құралған модельдің өзектілігі болып, суреттелген виртуалды модельден тізбекке кіретін IP-дестелердің пайдалды жүктемесінен олардың бастарында орналасқан кез-келген анықталған параметрлері алынуы мүмкін. Алайда, әр дестеге тән уақыттық белгілер ағынның динамикалық сипаттамаларын анықтауға және сараптауға мүмкіндік береді. Сонымен, виртуалды байланыстың көпмүшелік моделін ала отырып, ағынның құрамы жайында және оның динамикасы жайында сараптама жүргізуге болады.

Бұл жерде, виртуалды байланыстың жағдайы векторы ұғымы Y енгізіледі. Ол желі аралық әрекеттесу моделінің қолданбалы, транспортты және желілік деңгейлерінің y_k парамертрлерін біріктірді: $Y=\{y_k\}$. Бұл параметрлер келсілерді анықтайды: субъект, объект және IP-желіде рұқсаттылықты жүзеге асырған кездегі пайда болатын ақпараттық ағын. Жағдай векторы парамертлеріне келесілер енгізіледі: сервер мен порттың IP-адрестері мен порттары, тарнспортты және қолданбалы деңгейлер хаттамалары, транспортты хаттама жағдайы (қосылу фазасы), WEB серверге қарағандағы доменді есім, HTTP және FTP хаттамаларымен файл алмасқан кездегі сұралатын файлдың аты, сондай-ақ SMTP хаттамасы үшін жіберуші мен қабылдаушының электронды пошта адрестері. Жайғдай векторларына IP-дестелер ағынының статисткалық параметрлері беріледі. Соның ішінде, ағын екпінділігі, таратылған дестелер саны мен пішімі.

Қорытындылай келгенде, кез-келген V көпмүшелігіне жататын, виртуалды жалғастыру үшін, жалпы келіп түсетін виртуалды жалғастырулардағы дестелер көпмүшесі, $V_к$ қауіпті (яғни, бұл виртуалды жалғастыруға жатпайтын) және $V_{кс}$ ағымдағы виртуалды қосуға жататын көпмүшелердің бірігуінен тұрады: $V=V_к \cup V_{кс}$.



3.2 – сурет. IP-дестелерді классификациялау

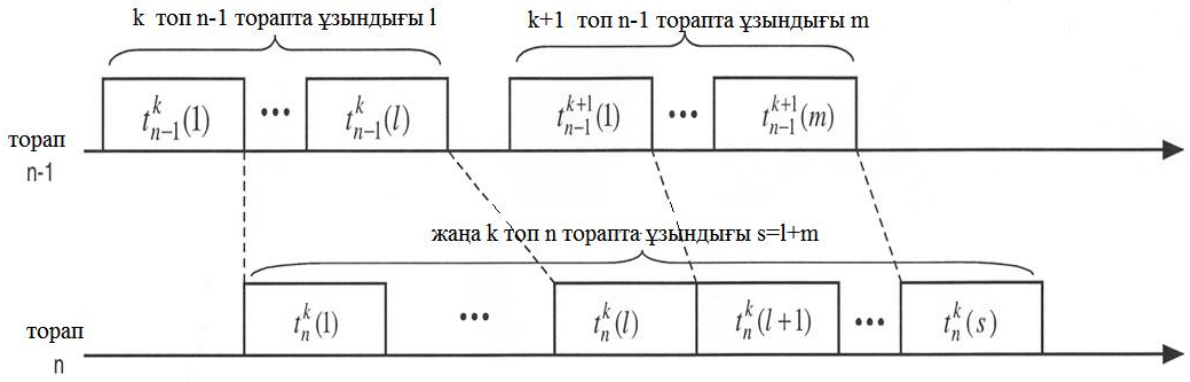
3.3 IPsec хаттамасындағы тунельдеу эффектінің математикалық моделі

IPsec тунельдеу эффектінің математикалық моделі тізбектеулі кезекті жаппай қызмет көрсету желісі болып табылады.

Келесілер өлшенетін параметрлер болып табылады:

– үздіксіз қызмет көрсету уақыты (бос болмау уақыты);

– дестенің n-ші торапта болуының орташа уақыты.



3.3 – сурет. Дестелердің ілінісуі

Бос болмау уақыты кезіне дестелер түйін шығысында топ құрады (үздіксіз бос болмау кезінде). Осындай топтың орташа ұзындығы дестелер санымен анықталады. Бірінші шекаралық түйіннің кірісіне Пуассон хабарламалар ағыны келіп түседі. Берілген ағынның кіріс интенсивтілігі λ және қызмет көрсету уақыты $1/\mu$ және жүйеде стационарлы жағдай M/M/m ($\rho = \lambda/(\mu m) < 1$ болған кезде де λ интенсивтілікті Пуассондық ағын болып табылады). Тізбектей жалғанған кезде біз әр түйінде жеке жеке, басқаларынан тәуелсіз қарастыра алмаймыз.

Егер біз n (n ≥ 2) торапта бір бірінен кейін тізбектеліп бара жатқан хабарламаны қарастырсақ, осы екі хабарлама түскен уақыт интервалы алдыңғы тораптарда көрсетілген қызмет көрсету уақытына тікелей байланысты болады.

Бірінші тораптың (n = 1) ерекшелігі болып, айқын көрініп тұрғандай, хабарламалар ешқандай тораптан өтпестен тікелей келіп түседі.

Ал, екінші тораптың (n = 2) жұмыс істеу ерекшелігі болып, ол хабарлмама топтарының көзі ретінде қарастырылатындығында.

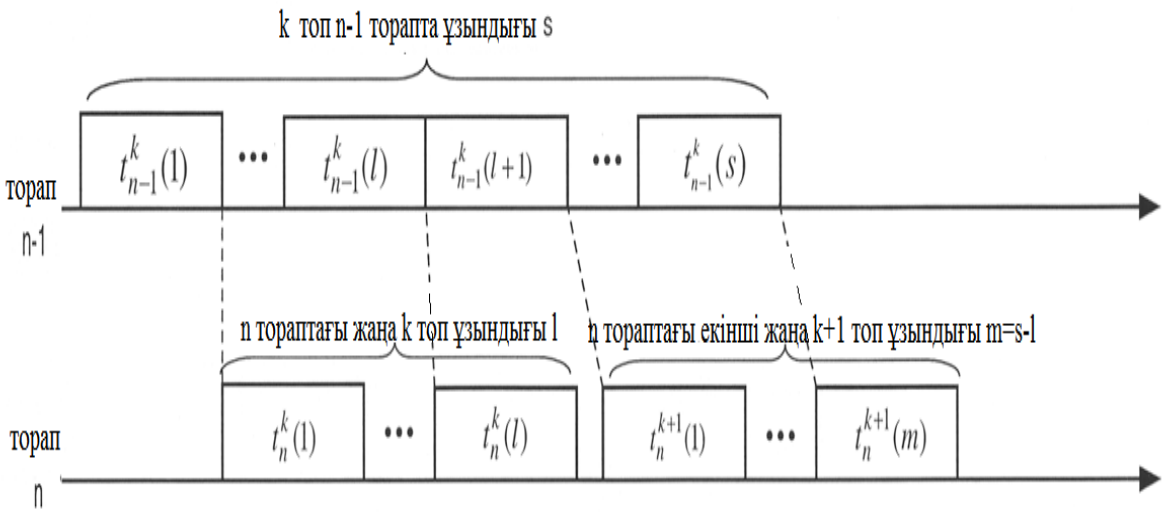
Дестелердің оларда жүруі қиындығы екі құбылысқа шатталған:

– бірінші тораптан шығатын топтардың, бір біріне қыстырылуы;

– сол топтардың фрагментациясы.

Бірінші құбылыс, тек қана екіншіге емес, сондай-ақ кез келген бірінші емес n (n ≠ 1) түйінге қатысты. Және ол k топтың бірінші дестесі осы торапта соңғы (k - l)-ші топтың және k мен (k-1) топтың екі дестесін де өзіне қосып алады (3.3 сурет). Екінші фрагментаця құбылысы, 3.4-суретте көрсетілген,

екінші түйіндегі орыны айтарлықтай емес. Бірінші торапта t номерлі, k топтағы дестеге қызмет көрсетілсін және сол уақыт аралығында келесі t+1 номерлі k топтың дестесі келіп түседі, әрі оның қызмет көрсетілу уақыты бірінші дестеге қарағанда артық болады. Осы арлықта екінші торапта кезек жоқ болсын және t десте бірінше торапты қызмет көрсетітіп болғаннан кейін ол екінші торапқа келіп түседі, ал t+1 десте бірінші және екінші тораптарда қатар қызмет көрсетіледі. t десте екінші торапты босатқаннан кейін t+1 десте бірінші торапта қызмет көрсетіле береді, себебі оны қызмет көрсету уақыты ұзағырақ.



3.4– сурет. Деректер фрагментациясы

Осы екі IPsec тунелін құру құбылыстың математикалық анализі келесі дестенің N тораптан тұратын тунельде болу уақыты келесі формуламен анықталады. Ал, тораптар ретінде маршрутизаторлар қабылданады:

$$V_1(N) \cong \ln\left[(N-2)!\left(\frac{\rho}{1-\rho}\right)^{N}\right] + N(1+\gamma) \qquad (3.1)$$

Мұндағы: γ −Эйлер тұрақтысы ($\gamma \cong 0{,}577$);
N−түйіндер (маршрутизатор) саны;
ρ−түйінге келетін жүктеме шамасы.

3.1 формула қандай болсын дестенің тунелде орналасу уақытын есептейді. Ол IP sec хаттамасындағы тунельдік режиміндегі дестенің тунельде орналасу уақытына сай келеді[22].

Екінші жағдай, берілген IPsec хаттамасының транспортты режимі. Бұл режимде тунель құрылмай дестелер қосымша IP дестеге орнатылуы арқылы таратылады. Бұл жағдайда, дестенің N тораптар арқылы жолда болуын келесі формуламен анықтауға болады[15]:

$$V_2(N) = \sum_{n=1}^{N} m \cdot \frac{1}{\mu} \cdot \frac{1-(K_n+1)\rho^{K_n} + K_n \rho^{K_{n+1}}}{(1-\rho^{K_n})(1-\rho)}, \qquad (3.2)$$

Мұндағы: N−түйіндер (маршрутизаторлар) саны;

ρ−түйінге келетін жүктеме шамасы;

m−түзету коэффициенті;

$\frac{1}{\mu}$ – жүйеде қызмет көрсетудің орташа уақыты;

K_n– топ көлемі.

Берілген хаттамаға сараптама жасау мақсатында, келесідей бастапқы мәндерді қабылдаймыз[14]:

3.1– кесте. Бастапқы мәндер

N тораптар (маршрутизаторлар) саны	ρ_1, Эрл	ρ_2, Эрл	ρ_3, Эрл	μ, c^{-1}	m
30	0,6	0,7	0,8	900	1,06

3.4 IPsec хаттамасымен таратылатын дестелер тобының ұзындығын анықтау

Аралық тораптар саны N = 30 деп алайық. Ал, дестелер тобының ұзындығы K_n үшін n қабылдайтын мәндер n = 1,2, ..., N деп қабылдайық.

K_n дестелер тобының ұзындығы келесі формуламен анықталады:

$$K_n \approx 1 + n\frac{\rho}{1-\rho} \qquad (3.3)$$

Мұндағы: n- натурал сан;

ρ−түйінге келетін жүктеме шамасы;

Келесіде шамалардың мәндердің барлығы MATHCAD жүйесінде есептелді[10].

3.2– кесте. ρ=0,6 Эрл болғандағы десте тобы ұзындығы

Шама	ρ=0,6 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Kn, байт	2,5	4	5,5	7	8,5	10	11,5	13	14,5	16	17,5	19	20,5	22	23,5	25

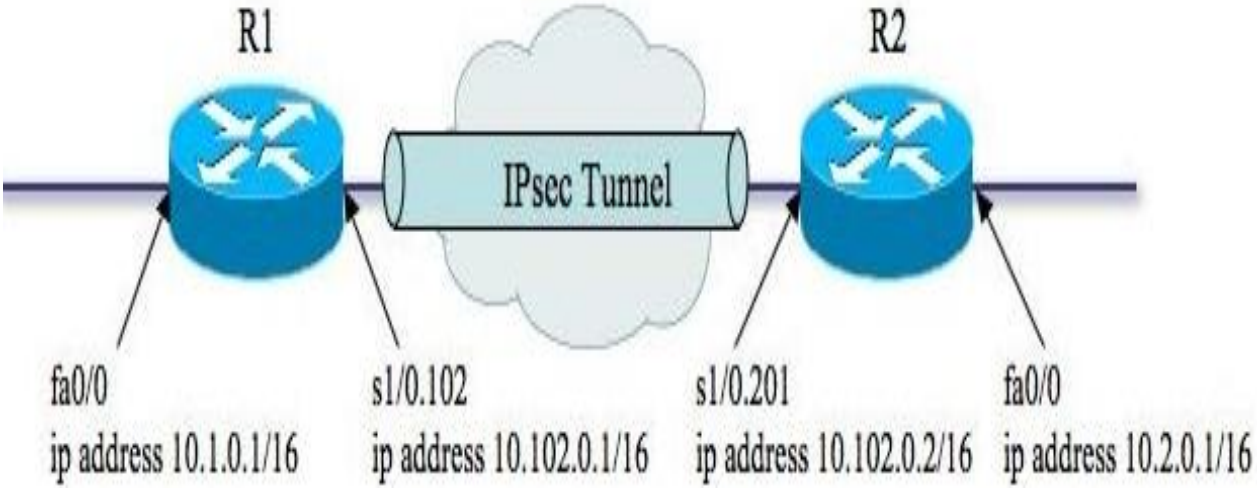
3.3 – кесте. ρ=0,7 болғандағы десте тобы ұзындығы

Шама	ρ=0,7 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Kn, байт	3,3	5,7	8	10	12,6	15	17,3	19,7	22	24,3	26,6	29	31	33	36	38

3.4 – кесте. ρ=0,8 Эрл болғандағы десте тобы ұзындығы

Шама	ρ=0,8 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Kn, байт	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65

3.5 IPsec тунельдік режимінде дестенің тунельде болуы



3.5– сурет. IPsec тунелінің қарапайым мысалы

IPsec дестенің N тораптан тұратын тунельде болу уақыты 3.1 формуласымен анықталады[10].

3.5– кесте. ρ=0,6 Эрл болғандағы уақыт

Шама	ρ=0,6 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V1(N), мкс	3,9	5,9	8,6	12	15	18	22	26	30	34	38,8	43	47	52	56,9	61,6

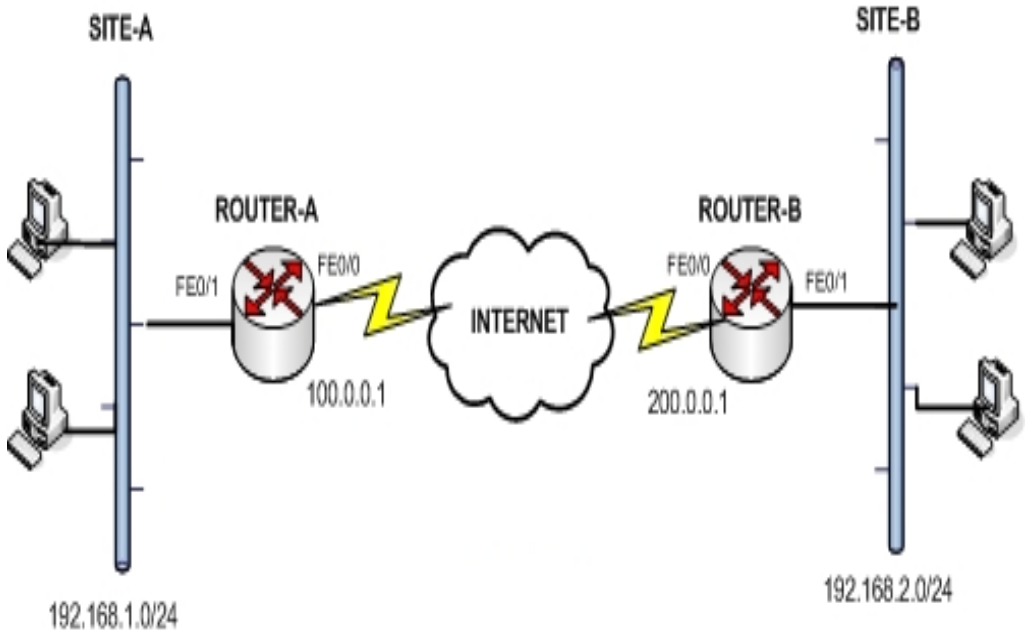
3.6 – кесте. ρ=0,7 Эрл болғандағы уақыт

Шама	ρ=0,7 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V1(N, мкс	4,8	7,2	10	13,9	17,7	21	25,9	30,3	34	39	44	49	54	58	63	69

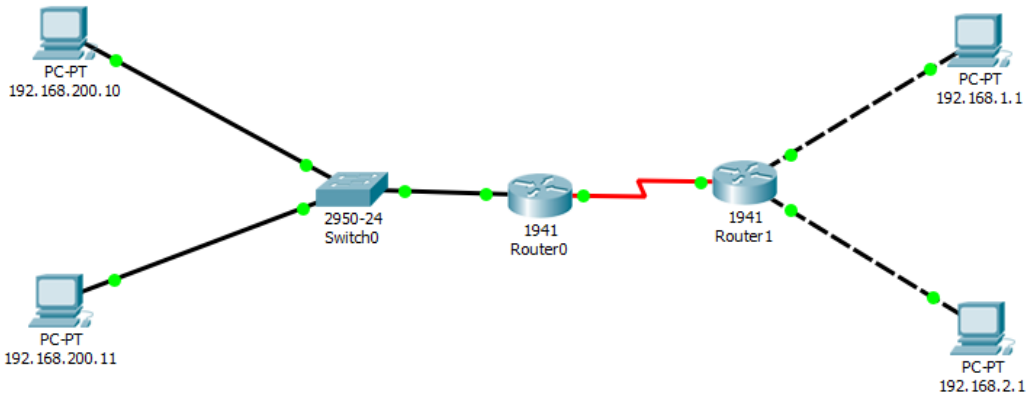
3.7 – кесте. ρ=0,8 Эрл болғандағы уақыт

Шама	ρ=0,8 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V1(N), Мкс	6	8,8	12,5	16,6	20,9	25	30	35	40	45,3	51	56	61	67	72	78

3.6 IPsec транспорттық режимінде дестенің болуы



3.6– сурет. IPsec транспорттық режимінің мыслы



3.7 - сурет. IPsec транспорттық режимінің сұлбасы

IPsec транспортты режиміндегі, тунель құрмай дестелерді таратудағы уақыт 3.2 формулаға сай анықталады.

3.8 – кесте. ρ=0,6 Эрл болғандағы уақыт

Шама	ρ=0,6 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V2(N), Мкс	3	5,3	7,6	10,1	12,6	15	17,9	20	23	25,8	28	31	33	36	39	41

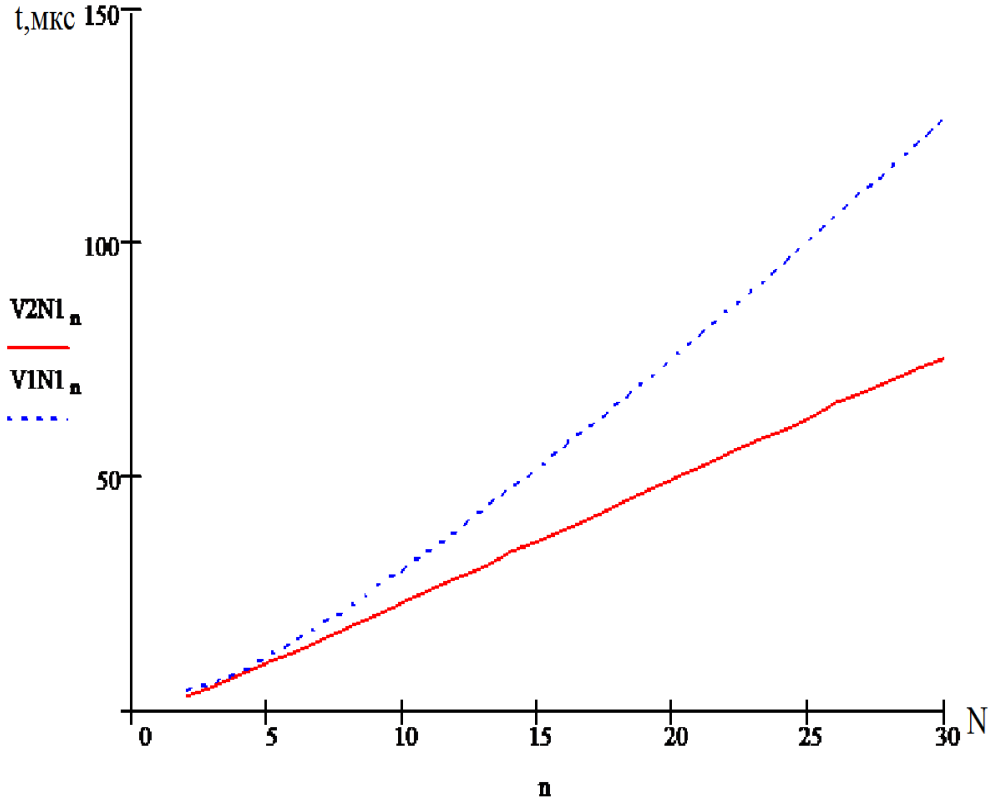
3.9 – кесте. ρ=0,7 Эрл болғандағы уақыт

Шама	ρ=0,7 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V2(N), Мкс	2,4	4,9	7,9	11	14,6	18	21	25	28	32	35	39,3	42,8	46	49	53

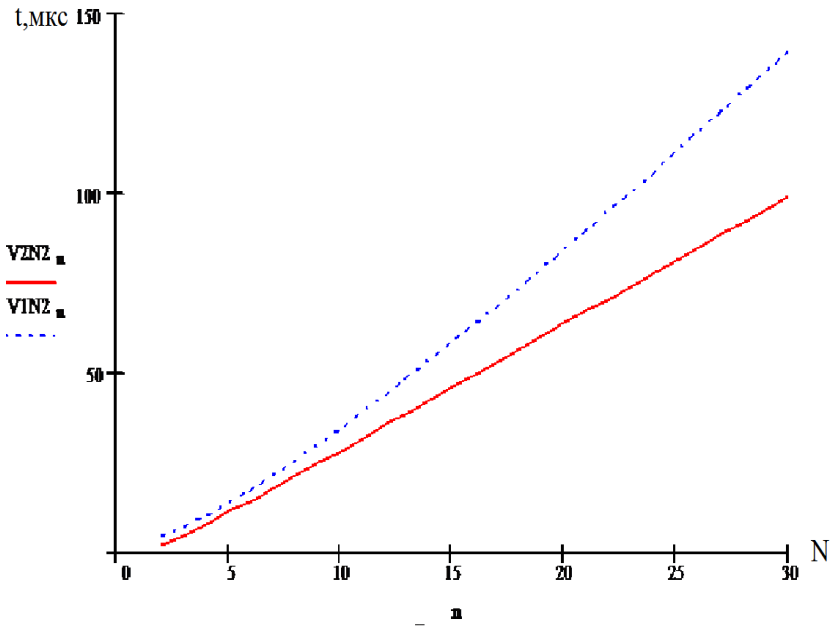
3.10 – кесте. ρ=0,8 Эрл болғандағы уақыт

Шама	ρ=0,8 Эрл болғандағы шамалар мәндері															
N	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
V2(N), Мкс	1,3	1,5	5,6	10,3	15	20,5	25,7	31	36	41	46	52	57	62	68	73

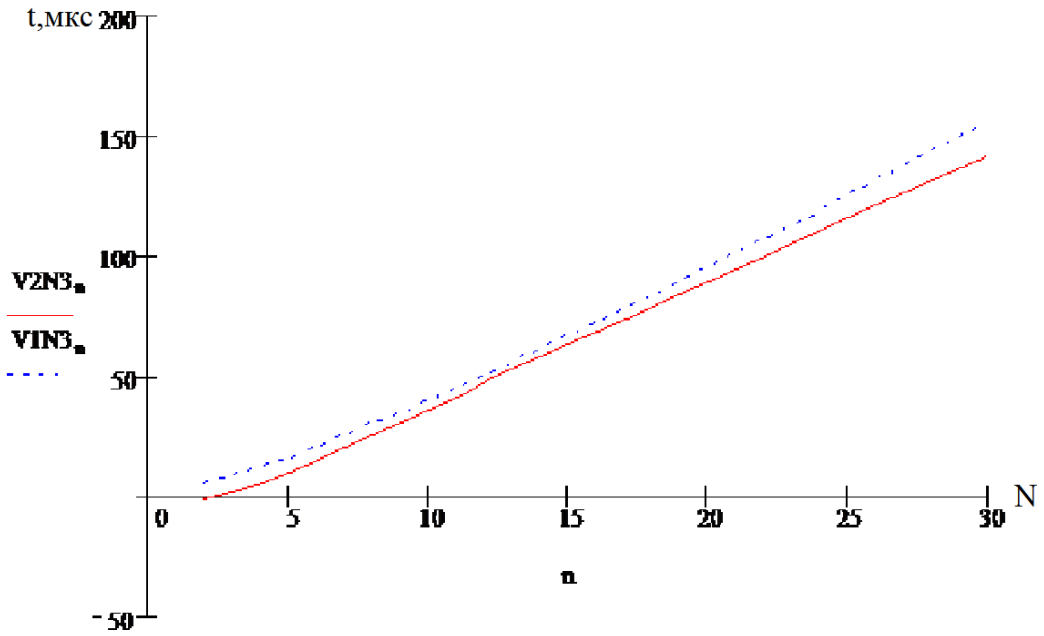
$V_1(N)$ және $V_2(N)$ шамалары мәндерін салыстырайық. Алынған мәндер бойынша Mathcad жүйесінде график тұрғызайық.



3.8 –сурет. ρ=0,6 Эрл болғанда V1(N) және V2(N) мәндері мен N арасындағы тәуелділік графигі



3.9 –сурет. ρ=0,7 Эрл болғанда V1(N) және V2(N) мәндері мен N арасындағы тәуелділік графигі



3.10 –сурет. ρ=0,8 болғанда V1(N) және V2(N) мәндері мен N арасындағы тәуелділік графигі

Берілген есептеулер барысында, IPsec тунельді және транспортты режимінің математикалық моделін, Mathcad бағдарламасын қолдана отырып есептедік, ρ = 0,6 Эрл болған кезде N≤5 тунель құру тиімді, ал басқа жағдайларды ақпататты IPsec хаттамасының транспорттық режимін қолданған тиімді болады. Себебі, тунелдік режиммен таратқандағы уақыт шамасы транспорттық режиммен таратқан кездегі уақыт шамасынан көп.

4 Өмір тіршілік қауіпсіздігі бөлімі

4.1 Еңбек шартын талдау

Бұл дипломдық жобаның тақырыбы - «IP желілеріндегі виртуалды қосылулардың рұқсаттылығын шектеуді зерттеу».

IP желілеріндегі виртуалды қосылулардың рұқсаттылығын шектеуді зертеу. Бұл дипломдық жобаның мақсаты болып виртуалды қосылулар жағдайы негзінде IP - желілердегі рұқсаттылықты шектеуді зерттеу болып табылады. IP- желісі Интернет желісін және басқа да желілерді қосуға және қолдануға мүмкіндік береді. Біз IP- желісі арқылы дүниежүзімен байланысқа шыға аламыз. IP-желісі арқылы бірнеше ақпараттар түрін (мәтіндік, бейнеақпарат, дыбыс және т.б.) тарата аламыз. IP - желісі арқылы телефондық байланысты ұйымдастыру үшін IP-телефонияға арналған арнайы құрылғы қолданылады. Әрбір шлюз телефон апаратымен, АТС абоненттік линиясымен байланыста болуы керек және тұтынушылар IP-шлюздың абоненті болып табылады.

Осыған байланысты өмір тіршілік қауіпсіздік бөлімінде қарастырылатын тапсырма - радиация.

Қауіпсіздік – сыртқы және ішкі қауіп-қатерден сақтайтын тірі организмнің қажетті шарасы. Ал адам қауіпсіздігінің ерекшелігі, адамның басқа тірі жандардан айырмашылығы, табиғи ортадан өз тіршілік ортасын жасай алады. Сол себептен болуы ықтимал қатерлер табиғи қатерлердің қатарына енбеуі де мүмкін.

Радиация – кез-келген құрылғыдан тарайтын радиотолқын формасындағы энергия ағыны.

Радиация латын тілінде радиус-сәуле деген сөз. Радиацияға күннің сәулесі, ғарыштық сәуле, жердің табиғи радиоактивтік заттарының сәуле шығаруы және жасанды радиоактивті изотоптар жатады.

Мемлекеттердің кейбір құжаттарында радияцияның нағыз мөлшері белгіленген. Халықаралық деңгей бойынша қазіргі кезде адамдарға радияциялық доза 0,1 бэрден аспауы керек. Профессионал мамандар дайындау оқу орындарына ППД-ның (предельно допустимая доза) 5 бэрден аспауы тиіс, иондалған сәуле таратын аймақта да тұратын адамдардың ағзасында радиацияның мөлшері 0,5 бэр болуы мүмкін. 70 жыл өмір сүрген адам радияциялық қайнар көздерінен 14-15 бэр алуы мүмкін. Бұл көрсеткіш ағзаларға онша қауіп төндіре қоймайтыны анықталған. Жер шарында тіршілік ететін әрбір адам өзінің өмір сүру кезеңдерінде жылына 250-400 мбэр радияция алатыны сөзсіз.

4.2 Радиацияның өлшем бірліктері

Рентген. Рентгенмен тек рентген және гамма - сәулеленуді ғана өлшейді. Бұл өлшем бірлікпен тек экспозиционды дозаны ғана өлшеуге болады, яғни

құрғақ ауада сәулелену қанша ионды бөледі. Бұл ионизациялық камерамен өлшеген кезде өте ыңғайлы, себебі датчиктің бұл типі иондардың санын ғана өлшей алады. Рентгеннен дозаны тікелей алады. Бірақ бұл доза адамға қандай зиян беретінін көрсетпейді.

Келесі бірлік - рад. Рад - бұл кез-келген сәулеленудегі жұтылған дозаның өлшем бірлігі. Яғни, бірлік зат массасы иондалған сәулеленудің қанша энергиясын жұтқандығы. 100 эрг 1 грамм радқа немесе 0,01 Дж 1 кг радқа тең. Және де радта керма өлшенеді. Керма - иондалған сәулелердің затпен жұтылған кезіндегі осы заттың зарядталағн бөлшектері қанша кинетикалық энергия алатындығы. Көп жағдайда жұтылған доза жәнет керма бір-бірімен сәйкес келеді. Егер ауада 0,88 рад гамма сәуле жұтылса, онда 1Р ион пайда болады. Дәлірек айтсақ, 1 Р=0,88 рад, ал 1 рад гамма сәулелену 1,14 Р-ге тең. Адамның терісі әртүрлі болғандықтан, дозиметр 20% ауытқушылық болуы мүмкін. Сондықтан 1 Р=1 рад деп жуықтап алуымызға болады.

Келесі түрі - радтың биологиялық эквиваленті (бэр). Бэр. эквивалентті доза бірлігі. Яғни бұл жерде бірдей энергиямен гамма немесе бета - сәулелермен салыстырғанда адам организміне нейтрондар 10 есе, альфа-бөлшектер 20 есе көп зиян келтіреді. Және де бэрмен әртүрлі организмдердің әртүрлі сезімталдығы ескерілетін тиімді доза өлшенеді. Егер адам толықтай біркелкі сәулеленсе, онда эквивалентті және тиімді доза сәйкес келеді. Бірақ адам денесі әртүрлі сәулеленсе, онда айтарлық айырмашылық байқалады. Бэрде дозаның амблевалентті эквиваленті өлшенеді - бұл «вакуумды сферикалық доза».

Келесі өлшем бірлік түрі - грей (Гр). Грей - СИ жүйесіндегі радтың аналогты түрі. 1 Гр=1 Дж/кг немесе 100 радқа тең.

Ең соңғысы, зиверт (Зв). Бұл бэрдің СИ жүйесіндегі аналогты түрі. 1 Зв=1 бэр. 1 мЗв=0,001 Зв немесе 0,1 бэр-ге тең.

Дозалардан басқа радиоактивті заттардың белсенділігі деген ұғым қоланылады. Бұл арқылы белгілі бір уақыт ішінде қанша ыдырау болатындығын білеміз. Белсенділікті кюри (Кл) немесе беккерельмен (Бк) өлшейміз. Кюри - 1 грамм Радий-226 белсенділігі. Беккерель - 1 секундтағы ыдырау. 1 Кл=37 ГБк.

Жұмыс барысында білу керек цифрлар:

– жұмыс орнындағы гамма-радиациясы 7 мкР/сағ, 0,07 мкГр/сағ және 0,07 мкЗв/сағ;

– сәулелік ауру туғызатын доза 100 Р, 1 Гр, 1 Зв;

4.3 Радиацияны өлшейтін құрылғы

Радиацияны өлшейтін құрылғылардың түрі өте көп. Солардың ішінде ең негізгілері «радиоактивті индикатор», «дозиметр», «дозиметр-радиометр». Осыларға жеке-жеке тоқталып өтсек.

Алғашқы түрі - СБМ-20 типті Гейгер счетчигі незінде жасалған. Кейбір түрлері СБМ-21 кішірейтілген базасында немесе альфа-сәулеленуге сезімтал

счетчигі базасында дайындалған. Мұндай аспаптардың көрсеткіші төмендейді.

Кейбір тәжіребиелердің көрсеткіші бойынша гамма-сәулеленудің энергиясы 30-100 кэВ деңгейінде СБМ-20 және СБМ-21 негізінде жасалынған аспаптар нәтижені төмендетіп көрсетеді. Егер гамма-сәулелену төмен болған жағдайда, бұл аспап оны сезе алмайды.

4.1 - сурет. Радиоактивті индикатор

Дозиметр - СБМ-20 базасында жасалынған құрылғы. Бұл гамма-сәулеленудің деңгейін кең энергия диапазонында жоғары дәлдікпен өлшей алады. Дозаны және доза қуатын көрсету арқылы нәтижені ұзақ уақыт ішінде интеграциялай алады.

Аспап Бета 1 және Бета 2 датчиктерімен және де төменгі энергиядағы альфа және бета сәулелері үшін слюдалы терезелермен, фильтрлармен жабдықталған. Бағасы жағынан бұдан қымбаттырақ аспаптар гамма-сәулелеріне сезімтал және оның бөлшектерін таба алатын, энергиясын өлшейтін жартылай өткізгішпен және сцинтиллярлы датчиктермен жабдықталған. Бұл дозаны максималды дәлдікпен өлшеуге мүмкіндік береді. Ал кейбір түрлері сәулеленуді тудырған бөлшектің изотопын анықтай алады.

4.2 - сурет. Дозиметр

Дозиметр-радиометр. Бұл гамма-сәулелердің дозасынан басқа бета-бөлшек ағынын да (егер тиісті датчик болса альфа-бөлшектерді де) өлшейді. Алдыңғы екі тармақ та бета-сәулелерін табады (дозиметр - фильтрді алған кезде), бірақ олар гамма-сәулелері секілді рентген және зиверт көрсетулерін есептеуді жалғастырады.Нәтижесі мүлде басқашга болып шығады. Егер гамма-сәулеленуі үшін Гейгер есептеуіші мен бөлшектерін табу ықтималдығы кең диапазондағы оның энергиясына тура пропорционал. (0,3 тен 1,5 МэВ-ке дейін). Бұл диапазон фильтрмен азая түседі 0,03-0,05 МэВ шамасында. Ал бета-сәулелену үшін мұндай ештеңе жоқ. Белгіленген шекарадан көтерілген кезде алғашқы тексерісте датчик барлық бета-бөлшектерді табады, ал төмендегенде таба алмайды. Альфа-сәулеленумен де дәл осылай. Радиометрге бета сәулеленуді өлшеу керектігін алдын ала ескерту керек. Сонда ғана ол бірлік уақыт ішінде датчик шаршы сантиметрдегі бөлшектер санын есептейді. . Алдымен гамма-фонда табу үшін фильтрмен есептейді, сонан соң екіншісінен біріншісінің айырмасы арқылы бета бөлшектердің ағымын табамыз. Альфа-сәулелену үшін де дәл осылай, бірақ бұл кезде екінші фильтр қосылады. Ол бөгеуіл үшін керек.

4.3 - сурет. Дозиметр-радиометр

Және де қазіргі заманауи түрі - смартфондарға арналған бағдарламалық дозиметр. Бұл кезде детектор ретінде жабық мөлдір емес материалдан жасалынған фотокамераны пайдаланамыз.

4.4 - сурет. Смортфондарға арналған бағдарламалық дозиметр

Радиация деңгейі аз болған кезде барлық аспаптар дәл көрсеткіш көрсетпейтіндігін ескеру керекпіз. Мысалы бірінші өлшеген кезде құрылғы 0,07 мкЗв/сағ көрсетті. Екінші рет өлшеген кезде көрсеткіш 0,17 мкЗв/сағ болды. Бұл радиация деңгейі еке есе көп деген емес. Ол шамамен 0,10 мкЗв/сағ болды[23].

4.4 Радиация нормалары

Компьютерлік техникаларда электрлі-сәулелі мониторлар үшін сәулеленудің шектік деңгейі бекітілген.

Рентген сәулелерінің дозасының қуаты кез-келген нүктеден мониторға дейін 5 см немесе дербес компьютерде сағатына 100 мкР аспауы керек[16].

4.5 Радиация және адам денсаулығы

Радиация адам денсаулығына зиянды әсер ететіні ешкімге құпия емес. Радиоактивті сәулелену адам денесі арқылы өткен кезде немесе организмге зарядталған заттар енген кезде, толқын энергиясы және бөлшектер біздің теріміз арқылы беріледі. Нәтижесінде организмді құраушы атомдар мен молекулалар қозады да, олардың әрекеттерінің бұзылуына тіпті өлімге алып келеді. Барлығы радиация дозасына, адам денсаулығына және әрекет ету ұзақтығына тәуелді.

Радиацияның адам денсаулығына әсер етуін - сәулелену деп атайды.

Иондалаған сәулелену үшін организмде ешқандай кедергі жоқ. Сондықтан кез-келген молекулаға радиоактивтілік әсер етуі мүмкін. Нәтижесі де әртүрлі болады. Атомның қозуы заттың басқаша өзгеруіне алып келеді. Биохимиялық өзгерістер, генетикалық бүлінулер пайда болады.

Сәулелену келесідей ауру түрлерін туғызады: инфекциялық асқынулар, зат алмасудың бұзылуы, қатерлі ісік немесе лейкоз, бедеулік, катаракта және т.б.

Қалыпты жасушаның қызметі үшін керекті ақуыздар мен майлар зардап шегеді. Осылайшы радиация адамға микродеңгейде әсер етеді. Бұл уақыт өте

келе ғана білінеді. Зардап шеккен ақуыздың бөлек топтары ісік ауруын және бірнеше ұрпаққа жалғасатын генетикалық мутация туғызуы мүмкін.

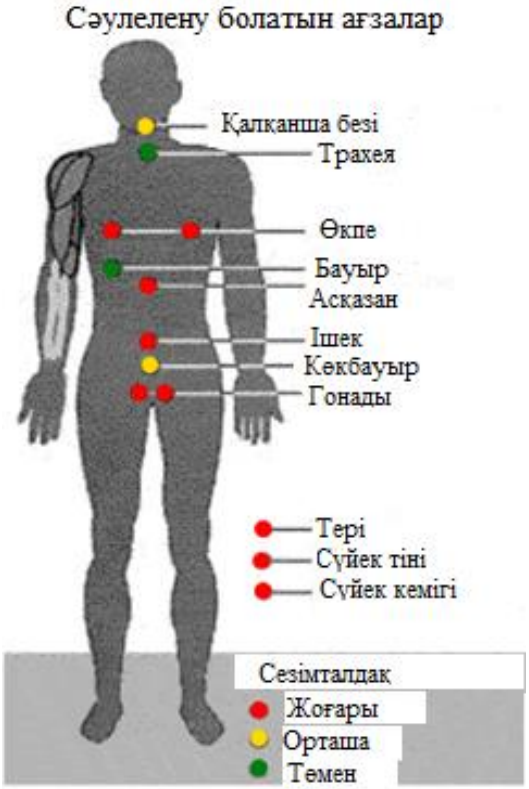
Сәулеленудің аз дозасын байқау мүмкін емес. Себебі ол біраз жылдан кейін ғана байқалады.

4.1 - кесте. Сәулелену дозасы және оның адам ағзасына әсері

Жұтылу дозасы, рад	Адамға әсер ету деңгейі
10000 рад (100 Гр.)	Өлім дозасы, орталық жүйке жүйесінің зақымдануына байланысты бірнеше сағат немесе күннен кейін қайтыс болады.
1000 - 5000 рад (10-50 Гр.)	Өлім дозасы, негізінен асқазан-ішек жолдарындағы (жасушалық мембраналардың жұқаруы әсерінен) ішкі қан кетуден 1-2 аптадан соң қайтыс болады.

4.1-кестенің жалғасы

Жұтылу дозасы, рад	Адамға әсер ету деңгейі
300-500 рад (3-5 Гр.)	Өлім дозасы, сүйек кемігінің жасушаларының зақымдануынан сәулеленгендер 1-2 ай көлемінде өледі.
150-200 рад (1,5-2 Гр.)	Алғашқы сәулелік ауру (склероьткалық процесс, жыныстық жүйенің өзгеруі, катаракта, иммундық аурулар, қатерлі ісік), Ауырлығы және алғашқы белгілері сәулеленудің типіне және дозасына байланысты.
100 рад (1 Гр)	Қысқы уақытты стерилизация: балалы болу қабілетінен айырылу.
30 рад	Асқазанды рентгенде түсіру кезіндегі сәулелену.
25 рад (0,25 Гр.)	Төтенше жағдайлар кезіндегі тәуекелге негізделген доза.
10 рад (0,1 Гр.)	Мутация ықтималдығы 2 есеге артады.
3 рад	Тісті рентген жасау кезіндегі сәулелену.
2 рад (0,02 Гр) жылына	Иондалған сәулелену көздерімен жұмыс жасайтын жұмысшылардың сәулелену дозасы.
0,2 рад (0,002 Гр. немесе 200 миллирад) жылына	Радиациялық-ядролық технология объекттерінің жұмыскерлері алатын сәулелену дозасы.
0,1-0, 2 рад (0,001-0,002 Гр.) жылына	Жердің радиациялық фоны
84 микрорад/сағат	8 км биіктікте ұшақта.
1 микрорад	Теледидар қарау



4.5 - сурет. Сәулеленуді тез қабылдайтын адам ағзалары

4.6 Радиациядан қорғану

Радиациядан қорғанудың бірнеше жолдары бар. Олар: физикалық, химиялық және биологиялық тәсілдері.

Физикалық тәсіл. Бұл тәсілдің ұйғаруы бойынша, дер кезінде қол-аяқты денені жылы сумен жуып отыру керек. Қолға арнаулы түрде дайындалған перчаткаларды кию керек. Қатты радиоактивті элементтердің бөлшектерінің кішкентай түйіршіктері ішкі органдарға өтіп кетпеуін қадағалап отыруы керек.Егер кішкентай бөлшектер ішкі органдарға өтсе, олар тез арада ағзадан шықпайды. Әсіресе уран, плутоний, стронций, иттрий және цирконий бөлшектері ағзаға өтсе өте қауіпті ісіктер туғызуы мүмкін. Олар радиоактивті сәулелер таратады. Цезий тез еритін тұздарды түзеді. Сөйтіп адам ағзаларының жұмсақ терлерінде жиналады да үнемі иондалған сәулеленуді таратады. Радиоактивті стронцийдің бөлшектерін адам ағзаларынан шығару оңай емес. Стронцийді кальциймен ығыстырып шығаруға болады.

Тез еритің цезий – 137 бөлшектерін ағзалардан ығыстырып шығару үшін көп мөлшерде су ішу керек. Радиоактивті элементтерді ағзалардан шығару үшін қымыздық сірке қышқылы мен лимон қышқылын көп мөлшерде пайдалану керек. С, Д витаминің ішу өте пайдалы (сәбіз, редис). Арақ-шарап ішуге болмайды. Олар радияцияның әрекетін күшейтіп жіберуі мүмкін.

Радиациядан қорғанудың химиялық және биологиялық жолдары. Радиацияға қарсы қолданатын препараттарды радиопротекторлар деп аталады. Олар радиоактивті элементтердің бөлшектері ағзалардан шығару

үшін неше түрлі химиялық препараттарды пайдаланады. Олар ағзаларды радияциядан сақтап қалады. Иондалған сәулеленуді ем-дом ретінде пайдалануға болады. Дерттерге диагностика қою үшін де таңбаланған атомды пайдаланады. Сәуле тератиясы мен қан, ауруларын емдеуге болады. Қауіпті ісіктерді де емдеу үшін бета-сәулесін пайдаланады. Адамдарды Радиациядан қорғау Қазақстан Республикасының алдында тұрған аса күрделі мәселе. Қазақстан Республикасында адамдардың денсаулығына өте үлкен көңіл бөлінеді. Әсіресе экологиялық аппатқа ұшыраған аймақтарда да тұратын халықтардың денсаулығы қатаң бақылауға алынған. Осы айтылғандарды қорыта келе, радияция (сәуле) дертіне шалдықпау үшін халыққа, әсіресе, жеткіншіктерге радиоэкологиядан жан-жақты білім және тәрбие беру екенін естен шығармауымыз керек. Адамзат баласы осы кезде бұрын – сонды болып көрмеген орасан көп ғылыми табыстарға жетіп, техника мен технологияны дамыта түсуде. Оларды төтенше түрде дамуы биология ғылымдарына тікелей байланысты. Ол жаратылыстану ғылымдарының көрнекті салаларының бірі. Оның басты міндеттері жер бетіндегі тіршіліктің пайда болуын, оның эволюциялық жолмен дамуын зерттеу. Биология жердің тіршілік иелері адамдар мен жануарлар өсімдіктер мен неше түрлі көзге көрінбетін микроорганизмдер әлемін зерттейді. Алынған мәліменттердің негізінде сигнал хабарды дәл тіркейтін сезімтал машиналар мен механизмдер шығару жұмыстарын жүргізеді. Кейінгі кезде биологиялық ғылымдар орасан зор ілгерлеп, алға басты. Осы уақыттың ішінде тіршілік дүниесі адамдар, жан-жануарлар, өсімдіктер әлемі туралы көптеген түсінігіміз бар. Тірі организмдердің пайда болу жолдарын, биохимиялық процестерін білеміз. Бірақ көптеген биологиялық көріністердің құпия сырлары әлі күнге дейін өз шешімін тапқан жоқ.

4.7 Роутерден сәулеленудің негізгі параметрлері

Адам организміне әсер ететін негізгі және ең маңызды параметрді сәулеленудің оптикалық қуаты деп атайды. Оптикалық қуатты децибел-миливатпен (дБм) өлшейді. Кез-келген ұялы телефон 27 дБм-ге тең сәулелену қуатын бөледі. Роутердің зияндылығы орналасқан орны мен қашықтыққа байланысты. Сымсыз роутердің сәулелену қуаты 20дБм. Ұялы телефонмен салыстырғанда роутер 1-2 метр ара қашықтықта орналасады. Сондықтан роутердің сәулеленуі ұялы телефонға қарағанда бірнеше есе кем адамға зиян келтіреді.

4.8 Компьютерге қойылатын негізгі талаптар

Дербес компьютермен пайдалану кезінде өзін-өзі қорғаудың бірнеше әдістері бар. Олар:

– Мониторды бөлменің бұрышына немесе артқы жағын қабырғаға қаратып қою керек;

– Бірнеше адам жұмыс жасайтын орында дербес копьютерлердің ара қашықтығы 2 м және бүйір жағынан 1,2 кем емес болу керек;

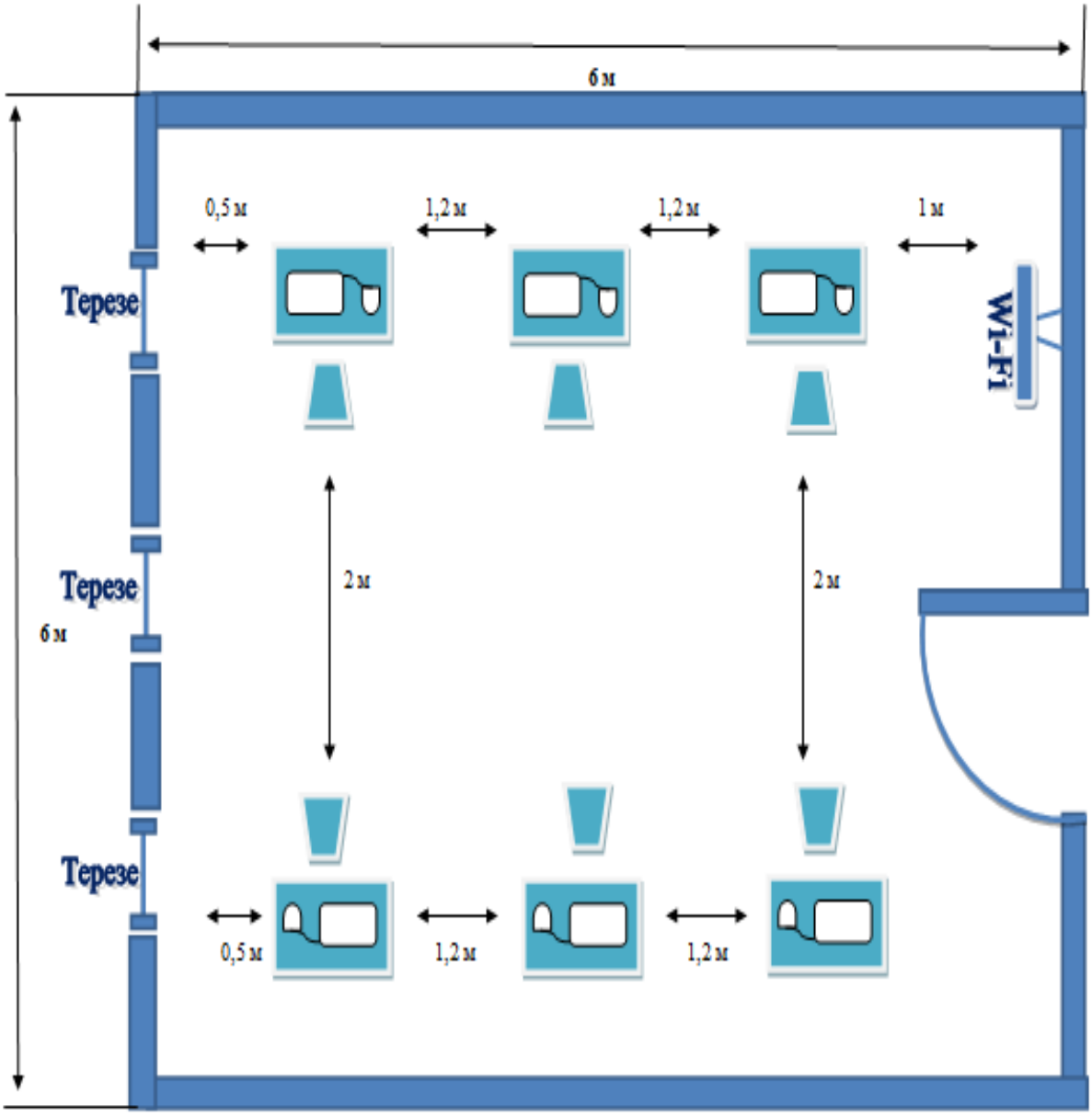
– Терезесі бар қабырғадан немесе столдың ара қашықтығы 0,25-0,5 м арасында болу керек;

– Дербес компьютерді пайдаланып жоғары мұқияттылықты талап ететін жұмыс орындарында бір-бірінен оқшаулау болуы міндетті. Оқшаулағыштың биіктігі 1,5-2 м болуы міндетті.

– Мониторды ұзақ уақытқа қосып қалдыруға болмайды;

– Жұмыс уақытында монитордан ара қашықтық 70см ескерілуі міндетті.

Осыған байланысты, өмір тіршілік қауіпсіздігі бөлімін қорыта келіп, радиацияның адам өміріне қауіптілігін анықтадық. Жұмыс барысында радиация адам ағзасына әсер етпес үшін компьютерлердің адам ағзасына әсер етпес үшін, компьютерлердің өзара орналасу ретін есептедік[16].



4.6 сурет - Бөлмедегі компьютерлердің өзара орналасуы

5 Бизнес жоспар

5.1 Түйін

Бұл дипломдық жобаның тақырыбы - «IP желілеріндегі виртуалды қосылулардың рұқсаттылығын шектеуді зерттеу».

IP желілеріндегі виртуалды қосылулардың рұқсаттылығын шектеуді зертеу. Бұл дипломдық жобаның мақсаты болып виртуалды қосылулар жағдайы негізінде IP - желілердегі рұқсаттылықты шектеуді зерттеу болып табылады. IP- желісі Интернет желісін және басқа да желілерді қосуға және қолдануға мүмкіндік береді. Біз IP- желісі арқылы дүниежүзімен байланысқа шыға аламыз. IP-желісі арқылы бірнеше ақпараттар түрін (мәтіндік, бейнеақпарат, дыбыс және т.б.) тарата аламыз. IP - желісі арқылы телефондық байланысты ұйымдастыру үшін IP-телефонияға арналған арнайы құрылғы қолданылады. Әрбір шлюз телефон апаратымен, АТС абоненттік линиясымен байланыста болуы керек және тұтынушылар IP-шлюздың абоненті болып табылады.

5.2 Маркетинг жоспары

Байланыс – қазіргі таңда, өндірістік инфраструктураның және нарықтық инфраструктураның маңызды құрамдық бөлігі болып табылады. Байланыстың дамуы Қазақстан Республикасының дүниежүзілік нарықта жаңа деңгейге шығуына, өндірістік салдардың және қоғамның басқа да тұрмыстық жағдайын жақсартуға мүмкіндік туғызады.

Қоғамның жаңа заманға сай дамуы, яғни ақпараттандыру ғасыры деп аталатын қоғамда байланыстың дамуына талап күшеюде, байланыстың дамуы адамның кәсіби және жеке өміріне қажетті кез келген ақпараттарды сапалы және уақытында таратуға байланысты болып келеді.

Нарықтық экономика жағдайында кәсіпорындардың жұмыс істеуі жеке даму жолын өңдеуді және іздестіруді талап етеді. Кәсіпорын инвестициялық жоба нәтежиелерімен, капитал салудың жаңа формаларын іздестірумен,

өндіруші мен тұтынушы арасында белсенді қызмет көрсету әрекеттерін табу арқылы өзінің экономикалық жағдайын жақсартып отыруы керек.

5.3 Ұйымдастыру жоспары

Бұл дипломдық жобаның мақсаты болып виртуалды қосылулар кезінде IP - желілердегі рұқсаттылықты шектеуді зерттеу болып табылады. Бұл жобаны іске асыру үшін қазіргі нарықта жүрген Cisco, D-Link, TP-Link компанияларының өнімдерін пайдаланамыз. Бұл өндірушілер баға-сапа жағынан пайдалы жабдықтарды қол жетімділігімен, жақсы техникалық сипаттамасымен ерекшеленеді.

5.4Қаржылық жоспары

Қаржылық жоспарды – іске қосу үшін инвестициялық жобаны қабылдау үшін негізгі шарт ретінде бизнес жоспарды ең маңызды бөлімінің бірі болып саналады. Қаржы жоспары жалпы күрделі шығындар, кірістер, операциялық шығындарды, пайданы және өзін-өзі ақтау кезеңінің есептеуін қарастырады. Керек құрал-жабдықтардың тізімі 5.1 - кестеде келтірілген.

5.1−кесте. Жабдықтауға қажетті негізгі шығындардың есебі

Атауы	Саны	Бағасы, тг	Құны, тг
Үстел КУЛ-128 1500x700x750	6	29 460	179 760
Орындық АВ03	6	13 110	78 660
Жартылай жабық сөре КУЛ ФП-3 700x320x1500	2	13 930	27 860
Шкаф КУЛ ШО-1 500x450x1820	1	15 690	15 690
Моноблок 21.5" Lenovo IdeaCentre 510 White (F0CB00P8RK)1920x1080 Intel Core i5/2.4 Гц/	6	239 990	1 439 940
ПринтерМФУлазерліSamsungSL-M2070W/XEV Printer/scanner/copi	2	56 990	113 980

Серверлік шкаф SHIP 19" 20U 600x800 мм	1	82050	82 050
СымсызVDSL/ADSL Модем/Роутер, TP-LinkArcherVR400, 4 порт + Wi-Fi, 867 Mbps (ArcherVR400)	1	29 990	29 990
UPS SVC, 2000VA/1400W, AVR:145-275В, 2Shuko, LCD, Тазасинусоида, Black (PTL-2K-LCD)	1	106 790	106 790
Коммутатор D-link DGS-1210-28/F1A (10/100/1000 Mbit, 4 SFP портты)	2	50 923	101 846
Кондиционер Beko BRH-245 2191Вт, 60м^2	1	249 990	249 990
Кабель бұралған жұп SHIP желілік кабель D135-P, Cat.5e, UTP, 305 м/б	1	25 254	25 254
Коннектор Rj45 UTP	50	50	2 500
Автоматты көпфункционалды стриппер	2	6 474	12 948
Кеңсе тауарлары		70 000	70 000
Картридж қара түсті	1	8 090	8 090
Барлығы	75	998 781	2 445 348

5.4.1 Капитал шығындарды есептеу. Жабдықтардың капиталы шығындар сатып алу бағалары 5.2 кестеде көрсетілген. Жабдықтардың капитал шығындарына тағы жабдықтарды тасымалдау, орнату және басқа да шығындардың құны кіреді. Жалпы капиталдық каржыландырудың келесі формуламен анықталады:

$$K_к = K_{КК} + K_{орн} + K_{тр} + K_{жобалау} \quad (5.1)$$

мұндағы $К_{кк}$ – алатын қондырғы құны;

$К_{орн}$ – қондырғыны орнату құны;

$К_{тр}$ – қондырғыны транспортау құны;

$К_{жобалау}$ – жобалау шығыны.

Алатын қондырғы құнын есептеймін:

$К_{кк}$ = 2 445 348 (теңге)

Орнату құны, жабдықтар құнының 5% алады, онда:

$$K_{орн} = K_{КК} * 0{,}05 \quad (5.2)$$

Қондырғыны орнату құны:

$$K_{орн} = 2445348 * 0{,}05 = 122267 \text{ (теңге)}$$

Транспорттау құны жабдықтар құнының 6% құрайды, сонда:

$$K_{тр} = K_{КК} * 0{,}06 \qquad (5.3)$$

Жабдықтарды транспорттау құнын есептеймін:

$$K_{тр} = 2445348 * 0{,}06 = 146721 \text{(теңге)}$$

Жобалау шығынын келесідей анықталады:

$$K_{жобалау} = K_{КК} * 0{,}03 \qquad (5.4)$$

Сонда жобалау шығыны:

$$K_{жобалау} = 2445348 * 0{,}03 = 73360 \text{ (теңге)}$$

Сондағы жалпы капитал шығындар құрайды:

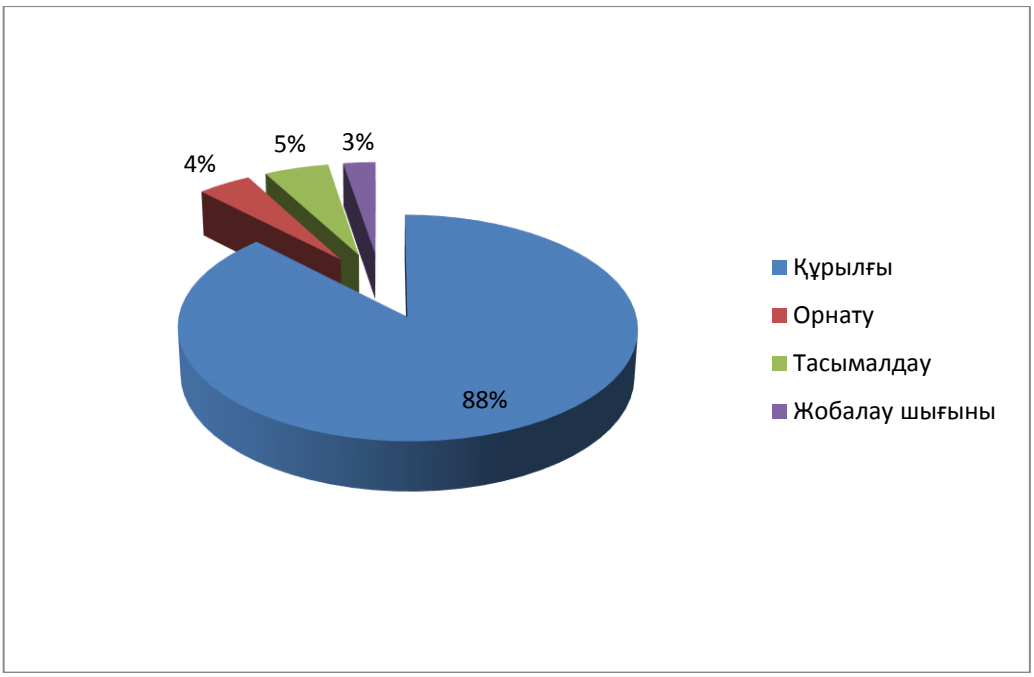
$$K_{к} = 2445348 + 122267 + 146721 + 73360 = 2787696 \text{ (теңге)}$$

5.2-кесте. Жоба бойынша капиталды шығындар

Шығыстардың атауы	Құны, теңге
Құрылғы	2 445 348
Орнату (жабдықтар құнының 5%)	122 267

5.2-кестенің жалғасы

Шығыстардың атауы	Құны, теңге
Тасымалдау (жабдықтар құнының 6%)	146 721
Жобалау шығыны (жабдықтар құнының 3%)	73 360
Капиталды шығындар	2 787 696
Барлығы	5 575 392



5.1-сурет. Капиталды салым құрылымы

5.4.2 Пайдалану шығындарын есептеу. Коммуникация қызметінің техникалық қызмет көрсету және қамтамасыз ету барысында, кәсіпорын ресурстарын тұтынуды талап ететін қызметті жүзеге асады. Жылына арналған шығындар сомасы және өндірістің нақты құны немесе жылдық эксплуатациондық шығындар сомасы болады[17]:

$$Э_П = Ш_{жал} + Ш_{ас} + Ш_{мат} + Ш_{ам.ауд} + Ш_{элек} + Ш_{устеме} + Ш_{ГЖ} \qquad (5.5)$$

Мұндағы $Ш_{жал}$ - жұмыс ақы қоры;

$Ш_{әс}$ - әлеуметтік қамтамасыз етуге кеткен шығындар;

$Ш_{мат}$ - материалдар мен қосалқы бөлшектерге кеткен шығындар;

$Ш_{элек}$ - электрожнергияны төлеуге кеткен шығындар;

$Ш_{ам.ауд.}$ - амортизациялық аударымдар;

$Ш_{ғж}$ - ғимаратты жалдау;

$Ш_{үстеме}$ - үстеме құны;

5.2 – кесте. Қызметкердің жалақысы

Орындаушы	Жұмыс мазмұнының атауы	Бір айлық еңбекақысы, тг	Бір жылдық еңбекақы,тг

Жетекші инженер	Әртүрлі жобаларды әзірлеу және оны орындау бойынша басшылық ету	150 000	1 800 000
Бағдарламашы	Қондырғыларға бағдарламалық қамтамасыздандыру ды орнату	120 000	1 440 000
Зерттеуші инженері	Қондырығыларды ұйымдастыру	100 000	1 200 000
Зерттеуші инженері	Қондырығыларды таңдау және суреттеу	100 000	1 200 000
Көмекші инженер	Жабықтарды жөңдеу және орнату	70 000	840 000
Көмекші инженер	Жабықтарды жөңдеу және орнату	70 000	840 000
Барлығы		610 000	7 320 000

Жалақының құны келесі формула бойынша анықталады:

$$Ж = Ж_{нег} + Ж_{кос}$$

$$Ж_{НЕГ} = Ж_{кыз} * 12 \qquad (5.6)$$

Мұндағы Ж - жалақы

$Ж_{қыз}$ - қызметкерлердің жалақысы

Қызметкерлердің жалақысы 5.2 - кестеде көрсетілген.

Қызметкерлердің негізгі жалақысы:

$$Ж_{нег} = (150000 + 120000 + 2*100000 + 2*70000)*12 = 7320000 \text{ (теңге)}$$

Негізгі жылдық жалақы ішіне қосымша жалақы енгізілген 30% мөлшерде негізгі жалақыдан (мереке, қосымша жұмыс үшін және т.б):

$$Ж_{кос} = Ж_{нег} * 0{,}3 = 7320000 * 0.3 = 2196000 \text{ (теңге)}$$

Осылайша жылдық жалақы:

$$Ж = 7320000 + 2196000 = 9516000 \text{ (теңге)}$$

Жалақы қызметкерлердің белгіленген нормаларды өндірілген әлеуметтік қажеттіліктері үшін қаржы бөлу (отчисления), таза зейнетақы шығыстар:

$$O_{CH} = H*(Ж - ЗК) \qquad (5.7)$$

Мұндағы $О_{сн}$ – әлеуметтік қажеттіліктері үшін қаржы бөлу;

ЗҚ – зейнетақы қоры (ЕТҚ 10%);

Н – қаржы бөлу белгіленген нормалардан (жалақыдан 11%).

Әлеуметтік салық сомасы қаржы бөлу:

$$Ш_{AC} = 0.11(9516000 - 0{,}1*9516000) = 942084 \text{ (теңге)}$$

Амортизациялық аударымдар Ао ретінде есептеледі:

$$A_O = H_A * K_{сал} / 100 \qquad (5.7)$$

Мұндағы На – амортизация нормасы (капиталды сомадан 18%).

Байланыс жүйесінің амортизациялық қаржы бөлуі:

$$A_O = 18*2787696/100 = 501785 \text{ (теңге)}$$

Өндірістік қажеттіліктері үшін энергетикалық шығындар электр жабдықтарына арналған шығындарды және қосымша қамтиды:

$$Ш_{эп.эл} = Ш_{эп.эн.жабдык} + Ш_{косымша} \qquad (5.8)$$

Жабдық үшін электр энергиясының құны мына формула бойынша табылады:

$$Ш_{эп.эн.жабдык} = W*T*S \qquad (5.9)$$

$$T = 24 сагат*365 кун = 8760(сагат)$$

мұндағы W – стансаның қолданатын қуаты, W=16,8 Вт;

Т – қондырғының бір жылдық жұмыс істеу уақыты, Т=8760 сағат;

S – электр энергиясының киловатт-сағат құны, S=21,99тг/кВт сағат.

$$Ш_{эп.эн.жабдык} = 16{,}8*8760*21{,}99 = 3236224 \text{(теңге/жыл)}$$

Қосымша қажеттіліктері құны жабдықтардың электр энергиясын тұтыну 5%:

$$Ш_{косымша} = 0.05 * 744775 = 37239 \text{ (теңге/жыл)}$$

Электр энергиясын шығындарды есептеу:

$$Ш_{эп..эн} = 744775 + 37239 = 782014 \text{ (теңге/жыл)}$$

Материалдардың қосалқы бөлшектер және техникалық қызмет көрсету құны капиталды салымның 0,5% құрайды[19].

$$Э_{м} = 0{,}005 * K \qquad (5.10)$$

Материалдардың құны:

$$Э_{м} = 0{,}005 * 2787696 = 13938 \text{ (теңге)}$$

Үстеме сомасы:

$$Ш_{устеме} = 0{,}75 * ЕТК \qquad (5.11)$$

$$Ш_{устеме} = 0{,}75 * 9516000 = 7137000$$

Алматы қаласында орналасқан ғимаратты жалға алу, ауданы 36 ш.м. айына 1 шаршы метрі 4200 теңге тұрады:

$$Ш_{гж} = 36 * 4200 * 12 = 1814400 \text{ (теңге/жыл)}$$

Өзіндік құн келесідей есептеледі:

$$С = Ш_{жал} + Ш_{АС} + Ш_{Ам.ауд.} + Ш_{эл} + Ш_{уст.}$$

$$С = 9516000 + 942084 + 501785 + 3236224 + 7137000 = 21333093 \text{ (теңге)}$$

Осылайша, эксплуатациондық шығындар сомасы:

$$Э_{П} = 9516000 + 942084 + 501785 + 3236224 + 13938 + 7137000 + 1814400 = 23161431$$
(теңге/жыл)

5.3 - кесте. Эксплуатациялық шығын құрылымы

Аталуы	Абсолютті шама, теңге	Меншікті салмақ,%
Еңбекақы қоры, Ж	9 516 000	41

Әлеуметтік салық аударымдары, $Ш_{э.с.}$	942 084	4
Амортизациялық аударымдар, $А_0$	501 785	2
Электроэнергия шығындары, $Ш_{Эл.\ Эл.}$	3 236 224	14
Материалдар мен қосалқы бөлшектер шығындары, $Э_м$	13 398	1
Үстеме шығындар, $Ш_{үстеме}$	7 137 000	31
Жалға алу шығындары, $Ш_{ғ.ж}$	1 814 400	7
Жалпы	23 161 431	100

5.2 –сурет. Эксплутациондық шығындар құрылымы

5.5 Интеллектуалды еңбек бағасы

Интеллектуалды еңбек – өнімді жасайтын жұмыс органдарының жүзеге асырған кезіндегі еңбегі, мый шығынды ойлау энергиясымен арттырады, еңбек өнімі – басқаларға тарату үшін немесе іске асыру үшін қағазға білдірілген ой (идея)[18].

Баға –өзіндік құнмен таза табыстың қосындысы, яғни

$$Ц_П = С + П \qquad (5.12)$$

Мұндағы: С – өнімнің өзіндік құны;

П – таза табыс.

Бастапқы бағаны анықтау кезінде телекоммуникация саласы үшін рентабелдіктің (40%) қажетті деңгейі беріледі:

$$Ц_П = C * \left(1 + \frac{P}{100}\right) \quad (5.13)$$

мұндағы Р - рентабелділік (40%)

$$Ц_П = 18404975 * \left(1 + \frac{40}{100}\right) = 25766965 \text{ (теңге)}$$

Іске асыру бағасын дайын өніммен табамыз:

$$Ц_Р = Ц_П + ККС \quad (5.14)$$

Сонымен ҚР ҚҚС(НДС) - тің бүгінгі күнгі мөлшері 12 % құрайды:

$$ККС = Ц_П * 12\% \quad (5.15)$$

$$ККС = 25766965 * 0{,}12 = 3092036 \text{ (теңге)}$$

$$Ц_Р = 25766965 + 3092036 = 28859001 \text{ (теңге)}$$

Экономикалық тиімділігін есептеу. Дамыту туралы қорытынды жұмыстар, байланысты кеңейту және қайта жаңартуды экономикалық тиімділігін келесі көрсеткіштермен есептеледі:

$$E = П / К_{эл} \quad (5.16)$$

$$E = 7361990 / 2787696 = 2{,}64$$

Капиталды өтемділіктің мерзімі – қаражатты қайтару мерзімі кері коэффициенті жалпы (абсолютті) тиімділігінің көрсеткіші болып есептеледі:

$$T = 1 / E \quad (5.17)$$

Капитал қаражатын бөлу сомасының өтелуінің мерзімі:

$$T = 1 / 2{,}64 = 0{,}37 \text{ жыл} = 3{,}7 \text{ ай}$$

IP-желісі үлкен жүктемелер кезінде жоғарғы қызмет көрсетуге кепілдік беру үшін құрылған желі. Бірақ IP-желісі әрдайым бізге жоғарғы сапаға кепілдік бере алмайды, өйткені үлкен жүктемелер кезіінде, ол кедергілердің, бөгеуілдердің салдарынан төмендеп кетеді. Сондықтан, IP-желісінде

ақпаратты, бейнеақпараттарды, дыбысты және тағы басқа ақпарат түрлерін тарату кезінде байланыс сапасын жоғарлату мақсатпен, міндетті түрде зерттеу жұмыстарын жүргізу керек.

Экономика бөлімін қорытындылай келе, негізгі құралдар үлкен көлемде жұмыс орнын жарақтандыруға және амортизациялық аудармаға кетеді.

Штаттағы қызметкерлердің саны түсетін салмаққа байланысты болады. Екінші орында барлық шығындардан еңбек ақы қоры тұр.

Интеллектуалды еңбек функциясын орындау - қызметкердің белгілікті интеллект деңгейіне, жоғарғы жалпы білімінің және кәсіби деңгейіне сәйкес қабілеттілігін талап етеді. Осыған байланысты сәйкес интеллектуалды еңбек мамандарын реттеуге арнайы және жалпы білім мағынасы өседі.

Қорытынды

Қорытындылай келе, бұл дипломдық жобада виртуалды қосылулар жағдайы негізінде IP - желілердегі рұқсаттылықты шектеуді зерттедім.

IP- желісі Интернет желісін және басқа да желілерді қосуға және қолдануға мүмкіндік береді. Біз IP- желісі арқылы дүниежүзімен байланысқа шыға аламыз. IP-желісі арқылы бірнеше ақпараттар түрін (мәтіндік, бейнеақпарат, дыбыс және т.б.) тарата аламыз. IP - желісі арқылы телефондық байланысты ұйымдастыру үшін IP-телефонияға арналған арнайы құрылғы қолданылады. Әрбір шлюз телефон апаратымен, АТС абоненттік линиясымен байланыста болуы керек және тұтынушылар IP-шлюздың абоненті болып табылады.

Витруалды жалғастырулардағы рұқсаттылықты шектеуде тапсырма қойылып, витруалды жалғастырудың теориялы-көпмүшелі үлгісін оқып үйрендім. IPsec хаттамасындағы тунельдеу эффектінің математикалық моделі жазылып, IPsec хаттамасымен таратылатын дестелер тобының ұзындығын есептеп таптым.

Сондый-ақ, өмір тіршілік қауіпсіздік бөлімінде арнайы ғылыми жұмыстар жүргізетін бөлмедегі радиация нормалары келтіріліп, қауіпсіз және тиімді жұмыс орнын ұйымдастырдым.

Экономикалық бөлімде жобаға арнайы бизнес жоспар жасалынды. Жабдықтауға қажетті негізгі шығындардың есебі құрылып, жоба бойынша капиталды және эксплуатациялық шығандыр, интеллектуалды еңбек бағасы есептелінді.

Қысқартулар тізбесі

АТС – автоматты телефон станциясы

ЛЕЖ – локальді-есептегіш желі

ОҚТЖ –ортақ қолданушы телекоммуникациялық желі

АДИКМ – адаптивті дифференциальді ИКМ

АЦТ – аналогты-цифрлы түрлендіргіш

ATM (Asynchronous Transfer Mode) – асинхронды таратылу әдісі

ISDN (Integrated Services Digital Network) –интеграциялау қызметінің цифрлы желісі

IP (Internet Protocol) –желіаралық хаттама

UDP (User Datagram Protocol) –дейтаграмманы тұтынушы хаттамасы

TCP (Transmission Control Protocol) – таратуды басқару хаттамасы

ITU-T (International Telecommunication Union) –стандартизациялаудың халықаралық ұйымы

FTP (File Transfer Protocol) –файлды тарату хаттамасы

ICMP (Internet Control Message Protocol) —хабарламаларды желіаралық басқару хаттамасы

SNTP (Simple Network Time Protocol) — компьютер желісі бойынша уақытты синхронизациялау хаттамасы

SNMP (Simple Network Management Protocol) — қарапайым желілік басқару хаттамасы

IGMP (Internet Group Management Protocol) —Интернет топтарын басқару хаттамасы

HTTP(Hyper Text Transfer Protocol) –гипертекстті тарату хаттамасы

RAS (Registration, Admission and Status) – жасырынды соңғы құрылғының өзара әрекет ету хаттамасы

RSVP (Resource ReSerVation Protocol) – ресурстарды резервтеудің хаттамасы

MCU (Multipoint Control Unit) —көпнүктелік конференция сервері

RTCP (Real-Time Transfer Control Protocol) – нақты уақыт режиміндегі таратуды басқару хаттамасы

DTMF (DualToneMultiFrequency) –көпжиілікті теру

MP MLQ (MultyPulse Multy Level Quantization) – көп импульстік, көпдеңгейлі кванттау

CSACELP (Conjugate Structure Algebraic Code Excited Linear Prediction) – басқарылатын алгебралық коды бар кездесетін құрылым

QoS (Quality of Service) –қызмет көрсету сапасы

DNS (Domain Name System) — домендік аттар жүйесі

BGP (Border Gateway Protocol) - шектік шлюздің хаттамасы

Әдебиеттер тізімі

1 К.С.Чежимбаева, С.А.Калиева. Дестелік коммутация технологиялары: 5В071900 – Радиотехника, электроника және телекоммуникациялар мамандығының барлық оқу бөлімінің студенттеріне арналған дәрістер жинағы - Алматы: АЭжБУ, 2012.- 52 б.

2 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. - СПб.: Питер, 2010.

3 Дуглас Камер. Сети TCP/IP, том 1. Принципы, протоколы и структура = Internet working with TCP/IP, Vol. 1: Principles, Protocols and Architecture. — М.: «Вильямс», 2003. — С. 880. — ISBN 0-13-018380-6.

4 ITU-T Recomendation H.323. Packet based miltimedia communication systems. - Geneva,1998.

5 ITU-T Recomendation H.245. Packet based miltimedia communication systems. - Geneva,1998.

6 Голубицкая Е.А. Экономика связи: М.:- Ирмас, 2006.

7 Олифер В.Г., Олифер Н.П. Глава 24. Сетевая безопасность // Компьютерные сети. Принципы, технологии, протоколы. — 4-е. — СПб: Питер, 2010. — С. 887-902. — 944 с. — ISBN 978-5-49807-389-7, ББК 32.973.202я7.

8 Andrew Mason. IPSec Overview. — Cisco Press, 2002.

9 Роман Луковников, Практическое применение IPSec, журнал "Хакер"

10 Andrew Mason, IPSec Overview, 2002, How IPSec works.

11 Таненбаум Э. Компьютерные сети.- СПб.: Питер, 2007 г., 992 г.

12 А.В. Висков, М.Б. Фомин «Актуальные области применения технологии MPLS» Российский Университет Дружбы Народов, г.Москва

13 Стивен Браун Виртуальные частные сети. – Москва: Лори, 2001, 504с.

14 А.Б. Гольдштейн, начальник сектора ЛОНИИС «Механизм эффективного туннелирования в сети MPLS» Журнал\\ Вестник связи №2 2004

15 IPSec - протокол защиты сетевого трафика на IP-уровне [Электронный документ]/Станислав Коротыгин. - http://www.ixbt.com/comm/ipsecure.shtml

16 СанПиН 2.2.2/2.4.1340-03 Общие требования к организации рабочих мест пользователей ПЭВМ

17 Базылов Қ.Б., Алибаева С.А., Нурмаганбетова С.С. Бітіруші жұмысының экономикалық бөлімі үшін телекоммуникациялық мамандығының барлық оқу түрінің студенттеріне арналған. АЖБИ, 2009. – 19 с.

18 Голубицкая Е.А.. Экономика связи. – М.: Радио и связь, 2006.

19 Баканов М.И. Шеремет А.Д. Теория экономического анализа. М.. Финансы и статистика. 1994.

20 http://citforum.ru/internet/nist/glava1_2.shtml

21 https://ru.wikipedia.org/wiki/IPsec
22 ttp://www.firewall.cx/networking-topics/protocols/870-ipsec modes.html
23 http://otravlenie103.ru/izluchenie/pribor-dlya-izmereniya-radiatsii
24 https://www.intuit.ru/studies/courses/636/492/lecture/11127?page=2
25 Ұйым стандарты. Оқу әдістемелік және оқу жұмыстары. Оқу-әдістемелік және оқу жұмыстарының құрылуына, жазылуына, рәсімделуіне және мазмұнына қойылатын жалпы талаптар. КЕАҚ СТ 56023-1910-04-2014. - Алматы: АЭжБУ, 2015