ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті»
коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Әбіләкимова Әдемі

«IPsec протоколын қолдана отырып кәсіпорын желісін жобалау»

ДИПЛОМДЫҚ ЖҰМЫС

6В06201 «Телекоммуникация» білім беру бағдарламасы

Алматы 2023 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
техн.ғыл.кандидаты
_____ Е.Таштай
«02» 06 2023 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «IPsec протоколын қолдана отырып кәсіпорын желісін жобалау»

6В06201 – Телекоммуникациялар мамандығы

Орындаған: Әбіләкимова Әдемі

Рецензент
Халықаралық ақпараттық
технологиялар университеті
т.ғ.к., кафедра меңгерушісі
_____ Бахтиярова Е.А
«02» 06 2023 ж.

Ғылыми жетекші
ЭТжҒТ каф. аға оқытушы,
техн. ғыл. магистры
_____ С. Марксұлы
«__» 06 2023 ж.
.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

6В06201 Телекоммуникация

БЕКІТЕМІН
Кафедра меңгерушісі
_____ Е. Таштай
«__» _____ 2022 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы: Әбіләкимова Әдемі
Тақырыбы: IPSec протоколын қолдана отырып кәсіпорын желісін жобалау
Университет ректорының *«23»қараша 2022 ж. №408-П/Ө бұйрығымен бекітілген.*
Аяқталған жұмысты тапсыру мерзімі *«30»сәуір 2023 ж.*

Дипломдық жұмыстың бастапқы берілістері:
1) Корпоративтік желілерге талдаудың тұжырымдамасы;
2) IPSec протоколын кәсіпорын желісінде қолданудың қауіпсіздік сипаттамасы;
3) VPN виртуалды желіні пайдалану арқылы корпоративтік қорғалған желінің топологиясын моделі;
4) IPSec протоколы арқылы берілетін деректердің қорғалуын қамтамасыз ететін хаттамалар жиынтығы.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:
1) Компьютерлік корпоративтік желілердің қазіргі жағдайы мен даму тенденцияларын талдау;
2) IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифры шешілген және шифрланған пакеттердің санын тексеру;
3) IPSec хаттамасының тиімділігін Cisco Packet Tracer бағдарламасы арқылы дәлелдеу;
4) Корпоративтік қорғалған желінің топологиясын жобалау және модельдеу;
5) желідегі арналарды пайдалану, ішкі желі маскасын және желілік трафиктің өнімділігін есептеу

Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):
Ұсынылатын негізгі әдебиеттер.
1) М. Остановский. Построение сети организации или маленького офиса //Открытая городская научно-практическая конференция «Инженеры будущего». – 2020. – С. 541-542.,
2) Э. И. Михневич. Расчет пропускной способности и устойчивости каналов //Экология и строительство. – 2020. – №. 1. – С. 23-31.

Дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Компьютерлік корпоративтік желілердің қазіргі жағдайы мен даму тенденцияларын талдау	04.01.2023 - 01.02.2023	Әдебиеттік шолу бойынша талдау
IPSec хаттамасының тиімділігін дәлелдеу	01.02.2023 - 01.03.2023	Хаттамаларды салыстырмалы талдау және *IPSec* математикалық талдау
Жабдықтар жұмысының есебі және жұмысты рәсімдеу	01.03.2023- 30.05.2023	Құрылғылар немесе бағдарламалау бойынша зерттеуді ұсыну.

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылымидәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Марксұлы С. т.ғ.м., ЭТжҒТ каф.аға оқытушысы	1.05.2023	
Теориялық ақпарат	Марксұлы С. т.ғ.м., ЭТжҒТ каф.аға оқытушысы	30.05.2023	
Норма бақылау	Ақылжан П т.ғ.м., ЭТжҒТ каф ассистенті	02.06.2023ж	

Ғылыми жетекшісі Марксұлы С.

Тапсырманы орындауға алған білім алушы Әбілакимова Ә

Күні «22» желтоқсан 2022 ж.

АҢДАТПА

Бұл дипломдық жұмыста IPSec протоколын қолдана отырып кәсіпорын желісін жобалау қарастырылды. VPN технологиясын қолдана отырып, IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифры шешілген және шифрланған пакеттердің санын тексеру, телекоммуникация жүйелерінде ақпаратты қорғау мәселелерін зерттеуге арналған.

IPSec протоколын қолдана отырып кәсіпорын желісіндегі ақпаратты қорғауды ұйымдастыру иілгіш бағдарламалық коммутатор Softwich-ті IP-телефония желілеріндегі қауіпсіздікті қамтамасыз ету қарастырылған. Сонымен қатар, негізгі түсініктемелер, функциялар, қолдану облысы және қолдану артықшылықтары қарастырылды.

АННОТАЦИЯ

В данной дипломной работе рассмотрено проектирование корпоративной сети с использованием протокола IPSec. Проверка количества зашифрованных и зашифрованных пакетов с помощью программы Cisco Packet Tracer для использования протокола IPSec с использованием технологии VPN, предназначена для изучения проблем защиты информации в телекоммуникационных системах.

Организация защиты информации в сети предприятия с использованием протокола IPSec предусмотрено обеспечение безопасности программного коммутатора softwich в сетях IP-телефонии. Кроме того, были рассмотрены основные объяснения, функции, область применения и преимущества использования.

ANNOTATION

In this thesis, the design of an enterprise network using the IPSec protocol was considered. Checking the number of decrypted and encrypted packets using the IPSec protocol using VPN technology using the Cisco Packet Tracer program, designed to study the problems of Information Protection in telecommunications systems.

Organization of Information Protection in the enterprise network using the IPSec protocol flexible software switch softwich is provided to ensure security in IP telephony networks. In addition, the main explanations, functions, application area and application advantages were considered.

МАЗМҰНЫ

КІРІСПЕ

Қазіргі уақытта телекоммуникациялық технологиялардың даму кезеңіндегі маңызды үрдістердің бірі IP (Internet Protocol) хаттамасы бойынша деректерді беруді қамтамасыз ететін көптеген жаңа технологиялармен жабдықталған IP-телефония нарығын дамыту болып табылады. Жергілікті және ғаламдық желі арқылы мультимедиялық хабарламалар (сөздер, деректер, бейнелер) арқылы пакеттерді ауыстыратын Интернет протоколын тарату болып табылды.

IP телефония тез арада дәстүрлі телефонды пайдаланудың негізгі баламасына айналды. Мұның басты себебі жаңа технология ұсынатын қызметтердің төмен құнында емес, бизнес әлеміндегі жаңа мүмкіндіктердің кең ауқымында жатыр.

Арнаны ауыстыру нарықтың қажеттіліктерін қанағаттандырмағандықтан, нарыққа белсенді және жаңа қосымша қызметтерді ұсынбағандықтан және желі көлемінің ұлғаюына сәйкес меншік құнын төмендете алмағандықтан, қоғамдық қызығушылық VoIP пакеттік байланысын қолдана отырып, желі арқылы дауыстық хаттамаларды беру бағытына ауыса бастады.

Шынында да, соңғы онжылдықта компьютерлік телефонның интеграцияланған жалпыға ортақ телефон желісінің дамуы айтарлықтай болды, бірақ заманауи компьютерлік технологияларды арна коммутацияланған желіге орналастыру құны тез өсуде.

Осыған байланысты IP телефония бизнестің негізгі нақты көзі болып саналады және оның телекоммуникация нарығындағы үлесі тез өсуде.

Ұсынылған тақырыптың өзектілігі байланыс көздерінің қолжетімділігі мен сенімділігі және біздің елімізде телекоммуникациялық қызметтердің орналасуы өзекті мәселе болып табылады, ал Интернетке жоғары жылдамдықты қосылуды, бейнебайланысты, кабельді теледидарды, ИҚ-телефонды және басқа да ақпараттық қызметтерді қолдану аясы негізінен Астана және Алматы қалаларында орналасқан. жақсы дамыған, бірақ Қазақстанның барлық өңірлерінің тұрғындары осындай қызметтерге мұқтаж.

Жұмыста қарастырылған сұрақтар.

1) Компьютерлік корпоративтік желілердің қазіргі жағдайы мен даму тенденцияларын талдау;
2) IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифры шешілген және шифрланған пакеттердің санын тексеру;
3) IPSec хаттамасының тиімділігін Cisco Packet Tracer бағдарламасы арқылы дәлелдеу;
4) Корпоративтік қорғалған желінің топологиясын жобалау және модельдеу;
5) желідегі арналарды пайдалану, ішкі желі маскасын және желілік трафиктің өнімділігін есептеу

1 IP-телефония жайлы жалпы сипаттама

1.1 IP-телефонияның даму тарихы

Кейбір дереккөздерге сәйкес, кәсіби компьютерлерді пайдаланып желі арқылы дауыстық хабарламаларды жіберу Иллинойс университетінде (АҚШ) басталған. 1993 жылы Чарли Клейн RS көмегімен алғашқы Maven audio repair бағдарламасын шығару арқылы жаңа белестерді ашты. Сонымен қатар, Интернеттегі ең танымал мультимедиялық қосымшаның cu-SeeMe, Корнелл университетінде Macintosh (Macintosh) үшін арнайы жасалған бейнеконференция бағдарламасы екендігі анықталды.

1994 жылғы сәуір. Ушу кезінде endeavor NASA-ның CU-SeeMe бағдарламасы арқылы жерге әртүрлі суреттерді жіберді. Фотосуреттермен қатар ол ушу кезінде аудио ақпарат беруге тырысты. Льюис ғылыми - зерттеу орталығынан алынған сигналдар Интернетке қосылған Махер орталығына жіберілді, осылайша кез келген адам ғарышта ғарышкердің дауысын ести алады. Кейінірек бір бағдарламаны екіншісіне орнату арқылы cu-SeeMe толық аудио және бейне мүмкіндіктері бар Mac және ДК үшін енгізілді.

1995 жылғы ақпан. Израильдік vocaltec компаниясы Windows амалдық жүйесін басқаратын мультимедиялық компьютерлер үшін интернет-телефон бағдарламасының бірінші түрін жасады. Бұл интернет-телефония дәуірін дамытудағы маңызды қадам болды. VocalTec танымал Internet Relay Chat (IRC) арнасын ұқсас мүдделері бар екі адам арасындағы байланыс құралы ретінде пайдалануға үлкен үміт артты. Дегенмен, IRC жетекші компаниясы Eras Free network (Feet) байланыса алмады, сондықтан Internet Phone жалпыға қол жетімді арналарға қол жеткізе алмады, бірақ олар көп жұмыс істеді және кестенің ұлғаюы мүмкін екенін жариялады.

Бірнеше аптадан кейін VocalTec пен EFnet арасындағы келіспеушіліктер қайта басталды. Осы уақыт ішінде жеке интернет-телефон серверлерінің желісі құрылды және мыңдаған адамдар vocal tec жергілікті желісінен бағдарламаларды жүктеп алып, бір-бірімен сөйлесе бастады. Дәл қазір олар бұл жұмыспен айналысады.

Биыл 1995 жыл. Көптеген компаниялар бұл жетістікті жоғары бағалады, өйткені олар бір-бірімен жер шарының әртүрлі жарты шарларында өмір сүре алады, сонымен қатар халықаралық байланыс үшін көп ақша төлемеуі керек. Нарықта бірнеше түрлі желілік құралдар өнімдері пайда бола бастады.

Осы қыркүйекте бөлшек сауда нарығында бірінші DigiPhone пайда болды - Далластағы (Техас штаты) шағын компания әзірлеген, бір уақытта сөйлесуге және тыңдауға мүмкіндік беретін "дуплекс" мүмкіндігі бар құрылғы. Осы уақытта абоненттер үшін нақты интерактивті байланыс қызметі пайда болды. Біз ізбасарлар үшін дыбыстың қандай жолмен берілетіні маңызды емес.

Кейінірек энтузиастар пайда болды, олар осыған ұқсас көптеген бағдарламаларды ашып, жарыстар ұйымдастырды. Жұмыстың мақсаты барлық елдердің тұрғындары Интернетке қосылып, қарапайым телефон құрылғысы

арқылы "сөйлесу сеансын" өткізетін бірнеше сағаттық сөйлесу науқанын жүзеге асыру болды.

1996 жылы наурызда тағы бір есте қаларлық оқиға болды. Сол кезде екі танымал vocal tec және Dialogic компаниялары, компьютерлер мен телефондардың ірі өндірушісі арасындағы "Internet Telephone Gate" деп аталатын жоба жарияланды, олар неге интернет пен телефон арасында арнайы шекара орнатқысы келетінін айтты.

Ақырында, Dialogic аудио ақпаратты пайдаланатын VocalTec Telephony Gateway деп аталатын арнайы бағдарлама жасады. Көп арналы аудио беру, біріншіден, бір VTG жүйесінде сегіз тәуелсіз желілік телефон қоңырауларын қамтамасыз етеді, екіншіден, IP мекенжайындағы әдеттегі телефон нөмірлерін ауыстырады және қажетсіз мәселелерді болдырмайды. Осы өнімнің көмегімен бір адамның сөйлесу жылдамдығы 11 Кбит/с құрайды, осыған байланысты арнаны толық пайдалану және төмен халықаралық төлемдер телекоммуникация әлемінде түбегейлі өзгерістерге әкелді. Бүгінде бұл жаһандық мультимедиялық коммуникациядағы алғашқы қадам екені анық.

Бір жылдан кейін ғаламшардың қарама-қарсы шетіндегі екі телефон абоненті арасындағы байланыс Интернет арқылы күнделікті тәртіпке айналды. Осы екі жыл ішінде телефон байланысы балама әдістердің бірі болды.

1.2 IP-телефония жайлы негізгі түсініктер

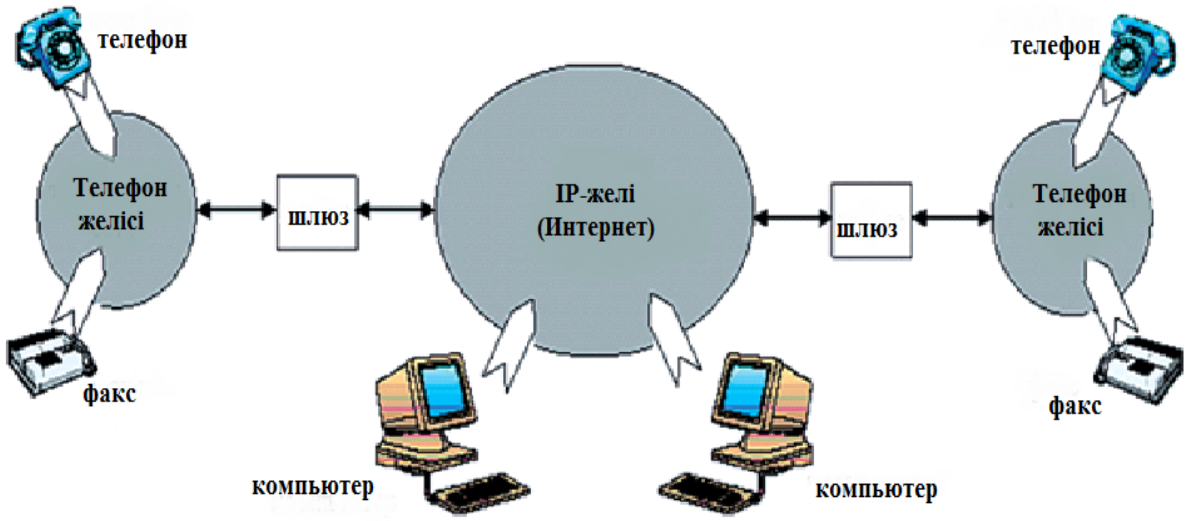
ИҚ-телефония-ИҚ-хаттама негізінде пакеттік коммутациямен жабдықталған желіні бірлесіп пайдалану арқылы сөйлесулердің және факсимильді хаттамалардың кез келген түрін заманауи беру технологиясын енгізу тұжырымдамасымен түсіндіріледі. Ең көп таралған желі, әрине, Интернет. Кейде біз VOIP (IP арқылы дауыс беру) терминін кездестіреміз, басқаша айтқанда "IP арқылы дауыс", яғни ол дауыстық ақпаратты тікелей IP желісі арқылы жібере алады.

Әдетте VoIP IP телефония синонимі ретінде қолданылады, дегенмен IP телефония тек арна деңгейінде ғана емес, сонымен қатар құрылғы деңгейінде де кеңірек ұғым болып табылады. (институционалдық автоматты телефон станцияларын қоса алғанда - АТС).

Бірнеше уақыт бойы желілер арналық коммутациялармен (яғни, телефондық желі) және пакеттік коммутациялармен (IP-желі) бір - біріне тәуелсіз жұмыс жасап келді. Арналардың бірін дауыстық ақпараттарды жіберу үшін пайдалансақ, ал екіншілерін - мағлұматтарды жіберуге пайдаланып отырдық. IP - телефония, қарапайым тілмен айтқанда шлюз арқылы екі желіні біріктіруге мүмкіндік берді, яғни телефон мен IP- желіні қосты.

Біраз уақыттан бері желілер бір-бірінен тәуелсіз жұмыс істеп келеді, арна коммутациясы (яғни телефон желісі) және пакеттік коммутация (IP). Біз дауыстық хабарларды жіберу үшін арналардың бірін, ал екіншісін деректерді жіберу үшін қолданамыз. IP телефония, қарапайым тілмен айтқанда, екі желіні

шлюз арқылы қосуға мүмкіндік берді, яғни ол телефон мен IP желісін байланыстырды.



1.1-сурет – IP-телефония құрастырудың қарапайым көрінісі

Қабылдаушы шлюзде алынған IP пакеттері қайта өңделеді және телефонның дабыл жүйесіне жіберіледі, сол кезде қоңырау сигналы абонентке жетеді.

Жоғарыда келтірілген мысал IP арқылы дауысты жіберудің жалғыз мүмкіндігі емес екенін атап өткен жөн. Сол қоңырау компьютерден телефонға, телефоннан компьютерге немесе екі компьютер арасында дауыстық режимде сөйлесуге мүмкіндік береді. Тиісінше, мұндай қосылу кезінде тек бір шлюз жұмыс істей алады немесе тіпті бірде-бір шлюз (ДК-ДК) жұмыс істей алмайды.

Алайда, ережелерге сәйкес, әдеттегі дауыстық трафик IP желісі арқылы арнайы жоғары құндылық аймағында беріледі. Бұл режимдегі дауыстық байланыс компьютерлер арасындағы байланысқа қарағанда қымбатырақ, бірақ оның сапасы әлдеқайда жақсы және оны пайдалану өте ыңғайлы.

—Бұл құрылғымен жұмыс істеу үшін алдымен провайдерге қоңырау шалып, телефон құрылғысынан қызмет провайдерінің шлюзіне қоңырау шалушының коды мен нөмірін теріп, телефонмен сөйлескендей сөйлесуді жалғастырасыз. Барлық қажетті қоңырау операциялары шлюз арқылы жүзеге асырылады.

—"Қазақстан Республикасының Ұлттық қауіпсіздік туралы Заңы" мынадай негізгі ұғымдарды қамтиды:

—- желідегі ақпараттық қауіпсіздік-бұл желідегі ақпараттық жүйені көптеген басқа қауіптерден қорғау жағдайы;

- желілік ақпараттық қауіпсіздік жүйесі, Қосымша қорғау жүйесі, - желідегі ақпараттық қауіпсіздіктің көптеген қатерлерінен қорғаудың құқықтық нормаларының, техникалық шаралары мен тетіктерінің жиынтығы;

-ақпараттық қауіпсіздік саясаты-бұл ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған іс-қимыл жүйесі.

-Сонымен қатар, осы тезисте бірнеше рет қолданылатын ұғымдарға тоқталайық:

- аутентификация-белгілі бір Идентификаторды белгілі атаулар бойынша тексеру процесі. IR телефония операторы жағдайында-карталар саны мен pin кодтарын тексеріңіз;

- авторизация-бұл клиенттің кез-келген ресурсты пайдалану мүмкіндігі бар-жоғын тексеру процесі;

- аудит - пайдаланылған қызметті есептеу процесі;

- хэш функциясы-бұл көбінесе хэш коды деп аталатын тұрақты ұзындық мәнін өзінің мәтінімен сәйкестендіретін хабарлама.

Желінің жұмыс істеуі кезінде ықтимал қауіптер туралы алдын-ала білу қажет. Егер қауіптердің саны мен жіктелуі нақты қауіптің ықтималдығын бағалаумен сәйкес келсе, негізгі аналитикалық жұмыс нақты қауіпке алдын-ала қарсы тұруға және қорғаныс жүйесін орналастыруға бағытталған. Тәуекелдерді жіктеудің түпкі мақсаты-ақпараттық қауіпсіздік жүйесіне теріс әсер етпейтін және нақты қауіптің пайда болуын күтпестен шығындар көлемін арттырмайтын қарқынды құрылғыларды таңдау.

1.2.1 IP - телефонияның келешекте дамуы

Осылайша, соңғы бес жылда байланыс қызметтері нарығының жылдық үлесі 40% құрады.

Соңғы жылдары федералды бюджет шығыстарының құрылымында арнайы инвестициялық қор пайда болғанын көріп отырмыз. Бұл қордың шығыс бағыты қоғамдағы қарқынды коммуникация мен басқару құрылымына жұмсалатыны расталды.Сондай-ақ инфекциялық қордан телекоммуникациялық жобаларды, ең алдымен ұлттық ауқымда цифрлық инфрақұрылымды құруға бағытталған жұмысты қаржылай қолдауға болады.

Қазіргі уақытта біз осындай өңіраралық цифрлық магистральдардың құрылысын талқылап жатырмыз (бұл жоба Экономика және IT саласындағы басқа сегменттерді дамытудың катализаторы болар еді) және инфекциялық қордан сапалы қызмет түрлерін ұсынатын желінің цифрлық ақпараттың өткізу қабілетін түбегейлі ұлғайту жөніндегі жұмысқа байланысты инфрақұрылымдық жобаларға қаражат бөлу. Мүмкін болатын жұмыс орындарының ауқымы тарылатыны сөзсіз.

Осылайша, 2005 жылдың қыркүйегінде Сан-Диегода (АҚШ) кезекті конференциялар мен көрмелер өткізілді. Қазіргі уақытта біз осындай өңіраралық цифрлық магистральдардың құрылысын талқылап жатырмыз (бұл жоба Экономика және IT саласындағы басқа сегменттерді дамытудың катализаторы болар еді) және инфекциялық қордан сапалы қызмет түрлерін ұсынатын желінің цифрлық ақпараттың өткізу қабілетін түбегейлі ұлғайту

жөніндегі жұмысқа байланысты инфрақұрылымдық жобаларға қаражат бөлу. Мүмкін болатын жұмыс орындарының ауқымы тарылатыны сөзсіз.

Осылайша, 2005 жылдың қыркүйегінде Сан-Диегода (АҚШ) кезекті конференциялар мен көрмелер өткізілді.

Бұл lambdagrid идеясын дамытқан халықаралық қозғалыс болды, мұнда Lambda сөзі толқын ұзындығын білдіреді, ал Grid - географиялық параллельдер мен меридиандар торын білдіретін "тор". Жалпы, хакерлік қозғалыс көп жаңалық әкелмеді және оның технологиялық нұсқаулары бұрын жасалған. Бұл көрмедегі маңызды тақырып DWDM технологиясы (толқын ұзындығын бөлетін тығыз мультиплекстеу), яғни цифрлық байланыстың жаһандық мультиплекстеуі болады.

Мүмкін, бұл технологияны жақынырақ түсінудің және аналогты дәл талдаудың негізі телеграф пен Маркони мен Поповтың ұшқын радиосынан заманауи көп диапазонды радиоға ауысу болып табылады, яғни желі әлемі қарапайым көтерме деректер технологиясынан бір уақытта әртүрлі толқын ұзындығында хабарлама жіберу мүмкіндігінің деңгейінде деп түсіндіріледі. Тиісінше, тасымалдаушы түссіз кең жолақты жолақта орналасқан, нақтырақ айтсақ, кең жолақты жарық сәулесін түсіретін ішкі тасымалдаушылар талшықтардың бағытына байланысты аз шығындармен сәулеленуге қосылуы мүмкін, нәтижесінде жаңа кабельдерді қайта салудың қажеті жоқ.

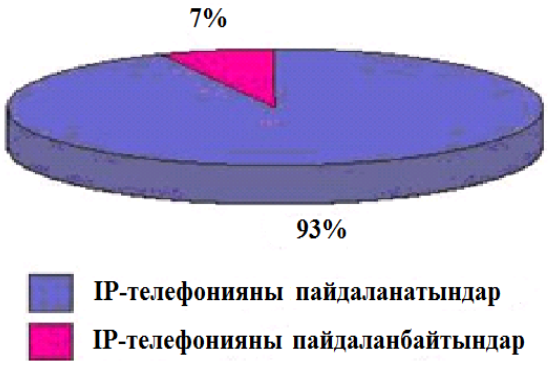
Сонымен қатар, жаңа DWDM трансиверлері квази - дуплексті болып табылады, яғни деректерді бір уақытта бір талшыққа екі бағытта беруге болады. Ұсынылған мәліметтерге сәйкес, он гигабиттік жоғары жылдамдықты арнадағы DWDM технологиясы деректерді бір уақытта 160 ағынға дейін, тіпті дауыстық магистраль арқылы, трансконтинентальды арналарды қоса алғанда, ұзын арналар арқылы жібере алады.

Сонымен, Интернеттің пайда болуы адам өмірінің сыйы сияқты болды. Сонымен қатар, тәуелсіз арналардың көбеюі оларды қажеттіліктері мен деректеріне сәйкес бір арнаға параллель бағыттады. Бұл тек жаңа ақпараттық және бағдарламалық шешімдерді және желіні басқаруға біріктірілуі керек Бірегей ақпараттық инфрақұрылымды қажет етеді.

Өкінішке орай, біздің еліміз жаһандық цифрлық коммуникациялар картасында жоғары жылдамдықты желілермен толтырылмаса да мұндай технологиялар Қазақстанға жақын арада келмейді.

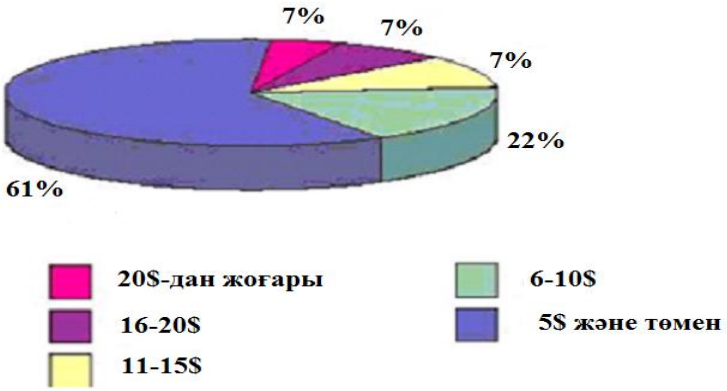
1.2.2 Қазақстандағы IP-телефония

Егер Қазақстандағы IP телефония жайлы айтсақ, бұл технологияны екі топқа бөлеміз: заңды тұлғаларға қызмет көрсету түрлері және физикалық.



1.2-сурет – Елді мекендер мен ірі қалалардағы IP-телефон қызметін пайдаланып отырған абоненттер статистикасы

Бірінші типке Ducat және Nursat компаниялары ұсынып отырған карталы IP - телефондары жатады.



1.3-сурет – ҚР-ның қалалары мен елдімекендердегі жетпіс мыңнан астам тұрғындардың IP-телефония қызметін пайдаланып және қызмет көрсетулерге төлеп отырған бір айлық орташа ақысы көрсетілген

Алайда, классикалық телефонмен салыстырғанда төмен тарифтік жоспарға қарамастан, 2010 жылғы ақпанда "КОМКОН-2 Еуразия" компаниясы жүргізген зерттеу нәтижелеріне сәйкес, тұрғындардың тек 7%-ы күнделікті өмірде және негізінен шетелдік таныстарымен немесе туыстарымен байланысу үшін пайдаланатын ИҚ телефон қызметін пайдаланады. Жалпы құны айына 5 долларды құрайды.

Осы компанияның есебіне сәйкес, Қазақстан Республикасының 70 000-нан астам халқы бар қалаларында тұратын жеке тұлғалар үшін ИҚ-телефон байланысы қызметтері нарығының ағымдағы көлемі айына 928 090 долларға бағаланады, ал егер біз қосатын болсақ, ИҚ-телефон байланысы қызметтерінің жалпы нарықтық әлеуеті, оның ішінде нарық мөлшері мен ir-телефон байланысы жеке тұлғалардың ашық сұранысы, жалпы сомасы айына 13 миллион долларды құрайды.

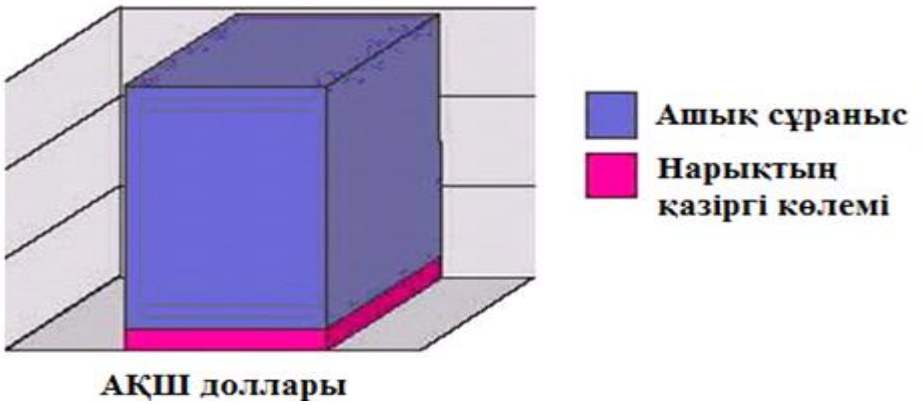
Басқаша айтқанда жұмыс коммерциялы клиенттерге байланысты болып тұр. Барлық ұйымдар IP-телефонданудің шешімін корпоративті желілерді дамытумен сәйкестендіреді. Бұл, әрине түсінікті жағдай ,себебі осы технология бизнесті дамытуда үлкен мөлшерде мүмкіндіктер береді: клиенттер қоңырауларын қайта өңдеудегі әртүрлі алгоритмдер, қызмет көрсетудің сапасын бақылау, абонент жайлы максималды толық ақпарат беру, қабылданған байланысты бірінші секундта қосу - осының барлығы классикалық телефонды байлыныста жоқ. Дегенмен, жоғарыда айтылған артықшылықтарға қарамастан, біздің елдің тұрғандарының үйреншікті, қарапайым телефоннан бас тартуы қиынға соғып тұр.

Ағымдағы сұраныс бірдей деңгейде. Дәстүрлі телефон станцияларына сұраныс қаншалықты көп болса, ИҚ телефонына да сұраныс бар. Бірақ қазіргі уақытта екі сұраныстың арақатынасы шамамен 20:80 құрайды, яғни 20% ИҚ телефония қызметін пайдаланады. Бұл нәтиже олардың телефон қызметі тым көп жарнамаланбағанына байланысты болуы мүмкін. Мәселе мынада, клиент қарапайым функционалды IP телефонының орнына қарапайым шағын АТС сатып алуға ақшасын босқа жұмсайды. IP телефоны-корпоративті ұйымдар үшін ең жақсы нұсқалардың бірі.

Баға тұрғысынан бұл шешім аналогтық телефоннан әлдеқайда жақсы. Аналогтық шағын АТС күнделікті жаңартуларды, толықтыруларды және жаңа тақталарды орнатуды қажет етеді. 10 000 абонентке дейінгі IR телефондарында телефон жабдықтарын сатып алу ғана қалады.

Енді осы жұмыс жоспары заң аясында қалай шешілетінін қарастырайық. IP телефония қызметтерін ұсынуға арналған лицензиялардың нақты түрлері бар ма? Мұндағы мәселе қазіргі уақытта коммуникацияның барлық мәселелерін реттейтін заңды өзгерту болып табылады.

"Байланыс туралы" жаңа заң шығарылды, жаңа заңнамалық актілер, оның ішінде қалааралық және халықаралық байланыс операторларына қойылатын біліктілік талаптары тіркелді. Мұндай балама қызметтерді ұсыну үшін арнайы лицензия қажет. Бүгінгі күні IR телефон карталары түсініксіз мәртебеге ие. Оқшауланған топта: операторлар Қазақтелекомға бармай-ақ барлық желіаралық қосылыстарды ұсынатын корпоративтік клиенттер, кампустың немесе бизнес-орталықтың клиенттері ИҚ-телефония қызметін пайдалану кезінде деректерді беру қызметінде арнайы лицензиялар бойынша жұмыс істейді.



1.4-сурет – Еліміздегі елдімекендердегі көп санды тұрғындардың ішінде IP-телефония қызметін пайдаланып отырған және қызмет көрсетулердің физикалық тұлғалар үшін орташа айлық нарықтық шамасы диаграммасы

1.2.3 Телефон желісі мен мәліметтерді жіберудің ықпалдастығы

Соңғы бірнеше жылда деректер желілері негізінен Интернеттің дамуына байланысты телефон желілеріне қарағанда жылдам қарқынмен өсті. Жақын арада деректер трафигі дауыстық трафикті басып озады. Бұл тенденцияның нәтижесі телефон желісі арқылы (V. 34 және v. 90 модемдері арқылы) дауыстық желі арқылы (кадр бойынша дауыс беру, IP арқылы дауыс беру және ATM арқылы дауыс беру) деректердің көбеюі болады.

2020 жылдардың басында Frame Relay енгізілген кезде, оның технологиясы деректерден басқа дауыстық хабарламаларды жіберуді қамтымады. Дауыстық хабарламаларды кадрларға жіберудің сенімділігіне күмәнданғанымен, "тегін қоңырау" туралы ақпараттың төменгі жағы жаңылыстыратын нәтижеге әкелді. Содан кейін тұтынушылар Frame Relay арқылы дауыстық хабарламаларды жіберуді тоқтатты, дегенмен құрылғы өндірушілері voice over Frame Relay (VoFR) шындыққа айналдырумен айналысты.

Дауыстық хабарламалармен қатар деректерді беру үшін қолданылатын заманауи пакеттік желілер (Frame Relay, IP және ATM) өте жоғары деңгейде болғанымен, бүгінгі нарық талаптары - бұл технологиялардың шектеулеріне қарамастан байланыс қызметтерін біріктіретін шынайы конвергенция технологиялары. Бұл жағдайдағы келесі міндет-Frame Relay, IP және ATM арқылы дауыстық хабарламаларды жіберуді қоса алғанда, желіаралық байланысты реттейтін стандарттарды әзірлеу.

1.3 IP–телефонияны қолданудың алға қойған мен мақсаттары артықшылықтары

IP телефонын пайдаланатын Клиент бұл құрылғыдан жалпыға ортақ телефон желісі қызметтерінің кең ауқымын, пайдаланудың қарапайымдылығын, дауыс беру сапасы мен сенімділігін ғана емес, сонымен қатар келесі артықшылықтарды алады:

- дәстүрлі телефон қызметі үшін әдеттегіден төмен баға;

- IPsec протоколын пайдаланатын IP телефоны бір уақытта дауыс пен деректерді қабылдай алады. Конвергенция талаптарына жауап береді. Бұл дегеніміз, тұтынушылар үнемдеуден дамуға дейін бір желіні пайдаланудан пайда көре алады, сонымен қатар трафиктің көлемін және шаблондарды деректерді беруден дауыстық байланысқа және керісінше жылдам ауыстырып, клиенттерді қорғай алады;

- IPsec протоколын пайдаланатын IP телефон желісі ұсынатын клиенттердің керемет ұтқырлығы: қоңыраулар мен факстар әлемнің басқа нүктесіне жіберіледі, клиенттер желіге қай жерде және қалай қосылғанына қарамастан бір желіге қосыла алады.

Бұл керемет мүмкіндік қызметтің орналасқан жеріне байланысты емес және үлкен икемділікке ие;

- құрылғылардың жаңа жиынтығына қол жеткізу-дәстүрлі телефондар мен факстардан бастап компьютерлерге дейін;

-қосымша деректерді өңдейтін ауқымды дерекқордағы ашық интерфейстің архитектуралық бейнелері арқылы жаңа қызмет көздеріне (дауыстық пошта, конференц-байланыс, факс жіберу және т. б.) қол жеткізу**;**

- сервистік жиынтықтарды жөндеу мүмкіндіктері;

- IR - телефон қызметтеріне ақы төлеудің қарапайымдылығы (әдетте телефон карталарымен төленеді);

- клиенттің шотындағы қаражатты бақылаудың қарапайымдылығы (Интернет арқылы);

- сіздің ұйымыңыз алған телефон қоңырауы IP телефонында қоңырау шалушы туралы хабарламаны автоматты түрде көрсетеді, мысалы: ол кім, оның ағымдағы тапсырыстары қандай, олардың мәртебесі қандай, ол соңғы рет қандай менеджермен сөйлескені туралы ақпарат, сондай-ақ сіздің дерекқорыңызда барлық тіркелген ақпарат көрінеді;

- егер абоненттің балансы көрсетілген сомадан аз болса, ол алдын ала Қолдау қызметіне қоңырау шалса да, автоматты түрде жинақ шотына аударылады. Жинақ агенттері абоненттің несие тарихы туралы ақпаратты компьютер экрандарынан біле алады;

– егер қоңырау VIP абоненттен келсе, бұл қоңырау Компанияның білікті менеджеріне қосылады;

- Қоңырау түскен кезде, IP жүйесі оны қай агентке жіберу керектігін өзі шешеді, мысалы, соңғы қоңырауды басқалардан бұрын жасаған менеджерге қосылу үшін;

- егер осы уақытта барлық желілер бос болмаса, жүйе қай желінің жақында босатылатынын бақылайды және абонентке желіде күтуін айтады;

- әлемнің кез келген елінде орналасқан уәкілетті пайдаланушы өз компаниясының желісіне кіріп, оған қалдырылған АВТО хабарламалар хаттамаларын тыңдай алады;

- егер біз өз АТС-тан ir-telephone серверіндегі телефон нөміріне басқа мекен-жай бойынша "бос емес" хабарлама жіберетін болсақ, онда абонент нөмірін терсек, интернет-сеанс кезінде компьютер экранында " кіріс қоңырау "деген жазу пайда болады, осы қоңырауды қабылдай отырып, сіз абонентпен сөйлесіңіз Интернет.

Интернет - провайдерлер үшін интернет-телефон байланысы қызметі мынадай артықшылықтарды ұсынады:

- ашық компьютерлік платформаларды пайдалану мақсатында капитал қаражатын жинақтау;

- бірегей желі шеңберінде түрлі қызметтерді ұсыну нәтижесінде пайдалану шығындарын төмендету;

Бұл тезисте пакеттік хабарламалардың ерекшеліктері, олардың телефон желісінің құрылымы және IPsec протоколын пайдаланатын телефон желісіндегі байланыс түрлері туралы айтылады. IPsec протоколын пайдаланатын телефон желісін дамытудағы ең маңызды мәселе оның қауіпсіздігі болып табылады, өйткені кәдімгі телефон да, ir телефоны да ұқсас, олардың артықшылықтары да, кемшіліктері де бар. Сондықтан менің жұмысымда олардың телефон желісіндегі байланыс қауіпсіздігі талданады.

IP телефон ақпаратын қорғау мәселесін шешу үшін қорғалатын ақпараттың бағасына, зақымдану ықтималдығына, қауіпсіздік жүйесінің бағасына және жүйенің жұмысына қарамастан жүйенің қауіпсіздігін бағалау қажет. Сонымен қатар, мен дауысты тануды, дауыстық диалогтың сапасын жақсарту жолдарын талдаймын, пакеттің оңтайлы ұзындығын және кәсіпорын желілерінің сенімділігін есептеймін.

1.4 Пакеттік жолдаудың ерекшеліктері

"Классикалық" телефон желілері әр телефон қоңырауы үшін арнайы физикалық қосылымды қажет ететін арнаны ауыстыру технологиясына негізделген. Тиісінше, бір телефон қоңырауы телефон арнасы арқылы бір физикалық байланысты қамтиды. Бұл жағдайда ені 3,1 кГц аналогтық сигнал ең жақын шағын АТС-қа беріледі, онда сигнал уақытты бөлу технологиясын қолдана отырып, осы шағын АТС-қа басқа абоненттердің сигналдарымен мультиплекстеледі.

Әрі қарай, топтық дабыл станция аралық арналар желісі арқылы беріледі. Тағайындалған АТС бөліміне жеткеннен кейін дабыл демультиплекстеледі және оның мекен-жайына келеді. Коммутацияланған телефон желісінің басты

кемшілігі-ол арна желілерін қарқынды пайдалана алмайды, яғни даму кезеңінде арна ешқандай пайдалы жүктемені көтермейді.

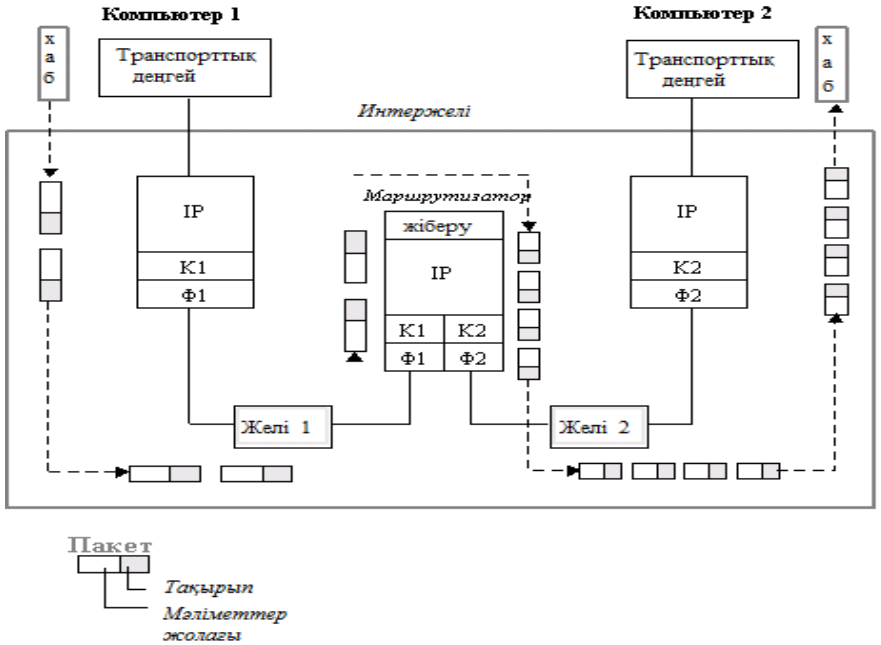
Аналогтардан цифрлық технологияларға көшу қазіргі заманғы цифрлық телекоммуникациялық желілерді дамытудағы үлкен қадам болып табылады. Осындай үлкен қадамдардың бірі цифрлық телефонияның пакеттік коммутацияға өтпелі кезеңін дамыту болды.

Байланыс арналары арқылы пакеттерді ауыстыратын желілерде физикалық торапқа ақпарат бірлігіне аз беріледі. Мұндай бірліктер пакеттер, кадрлар және ұяшықтар болуы мүмкін (хаттамаға байланысты), бірақ кез - келген жағдайда олар әртүрлі желілер арқылы және физикалық ортаға тәуелсіз жеке виртуалды арналар арқылы беріледі.

Әрбір пакет пайдаланылған арна туралы ақпарат алады, оның бастапқы шығу тегі (көзі немесе жіберушісі) және мақсаты (алушы) анықталады және оның тақырыбы да орнатылады.

IPsec протоколының негізгі желісіндегі барлық ақпарат - дыбыс, мәтін, бейне, компьютерлік бағдарламалар немесе басқа формалардағы ақпарат - пакеттер түрінде беріледі. Әрбір компьютерде және осындай желілік терминалда өзінің бірегей IP-мекен-жайы бар және осы мекен-жайға жіберілген пакеттер алушыға еркін жете алады.

IP желісінде қандай да бір проблемалар туындаған жағдайда, ол осы желі бойынша деректерді басқа мекен-жайға жібере алады. Сондықтан олардың хаттамасы көрсетілген арнада ешқандай дабыл сигналдарын тудырмайды. Дыбыстарды олардың желісі арқылы жіберу бірнеше бөліктен тұрады



1.5-сурет – Пакеттердің әртүрлі максималды өлшемдері бойынша желіаралық жіберу кезіндегі IP – пакеттердегі IPsec протоколының фрагментациясы

Қабылданған пакеттерден жіберілген аудио ақпаратты іздеу процесі бірнеше бөліктен тұрады. Аудио пакеттер қабылдаушы терминалға келгенде, олар алдымен реттілікке тексеріледі. Шын мәнінде, IP желілері жеткізу уақытына кепілдік бермейді, сондықтан үлкен сериялық нөмірлері бар пакеттер ертерек келуі мүмкін және жеткізу уақыты әр түрлі болуы мүмкін. Бастапқы реттілік пен сәйкестікті қалпына келтіру үшін пакеттерді стекке уақытша төсеу бар.

Дегенмен, жеткізу кезінде кейбір пакеттер толығымен жоғалып кетуі немесе жеткізу шегінен асып кетуі мүмкін жағдайлар да бар. Қарапайым жағдайда қабылдаушы терминал жоғалған немесе бүлінген ақпаратты қайтаруды сұрайды. Бірақ дыбыстық беріліс беру уақыты өте маңызды, сондықтан бұл жағдайда жуықтау алгоритмі іске қосылады, бұл алгоритм жоғалған пакеттерді шамамен қалпына келтіреді немесе жоғалған пакеттер бір жаққа лақтырылады, ал қалған Бос орындар басқа ақпаратпен басқа ретпен толтырылады.

IP телефониясын кеңінен енгізуге негізгі кедергі IR протоколы бойынша жоғары сапалы қызмет көрсетуге кепілдік беретін механизмнің болмауы болып табылады, бұл қазіргі уақытта IR телефониясын дауыстық трафикті берудің сенімсіз әдістерінің біріне айналдырады. IP протоколының өзі пакеттердің жеткізілуіне кепілдік бере алмайды, сонымен қатар нақты жеткізу уақытын көрсетпейді, бұл келісу кезінде дыбыстардың үзілуі және "бөлек дыбыстар"сияқты мәселелерді тудырады.

Бүгінгі күні бұл мәселелер шешілуде: стандарттау ұйымдары жаңа хаттамаларды ойлап табады, өндірушілер жаңа құралдарды шығарады, бірақ стандарттау жұмысы мен дыбыстарды пакеттерге "орау" арасындағы жұмыс жылдамдығы өте тегіс емес. Айта кету керек, егер жеке корпоративті желіде дауыстық сигналдың сапасы төмендесе, онда қауіптің орташа көрсеткіші болмайды, бірақ жалпыға ортақ желіде мұндай мәселелерге назар аудару керек.

Көптеген операторларға олардың жұмысы үшін ақы төленетіндіктен, олар өз жұмысының сапасына кепілдік беруі керек. Клиент келіссе де (телекоммуникация нарығындағы бәсекелестік жағдайларға байланысты оның ықтималдығы өте аз болса да), уақыт өте келе олар сапаның өте жоғары емес екенін түсініп, нақты немесе ұзақ мерзімді ақаулармен жұмыс істей алады. Қалай болғанда да, операторға барлық желілерде табылмайтын оператор орындайтын жұмыстың сапасын бақылайтын ауқымды бейімделген аппараттық құралдармен және ақпараттық қолдау құралдарымен жабдықталған қымбат құрылғы берілуі керек.

1.4.1 IP телефония желісінің құрылымдары

Сымсыз телефония желісі (ITU-T h323 ұсынысы бойынша) IR желісіне қосылған келесі құрылғылардан тұрады:

- шлюз (gateway);
- диспетчер (қақпашы);

- монитор (әкімшілік менеджері).

IR телефония желісінің құрылымы IR желісі арқылы қосылған шлюз желісінің абоненттік интерфейске тікелей қосылатын телефон желісіне қосылуын, дыбыстарды/деректерді кодтауды, пакеттеуді және қысуды, сондай-ақ қайта құруды қамтамасыз етеді.

Шлюз және тіркеу механизмін диспетчер бақылайды. Монитор қашықтағы конфигурацияланған және әкімшілік желілерді пайдалануды жеңілдету үшін қолданылады. Бұл үш компонентті әртүрлі өндірушілер деп атауға болады, бірақ олардың барлығы жоғарыда аталған функцияларды орындайды.

Жоғарыда аталған талаптардан басқа, IP - желісі құрылғылары бірқатар басқа мүмкіндіктерді қолдайды.

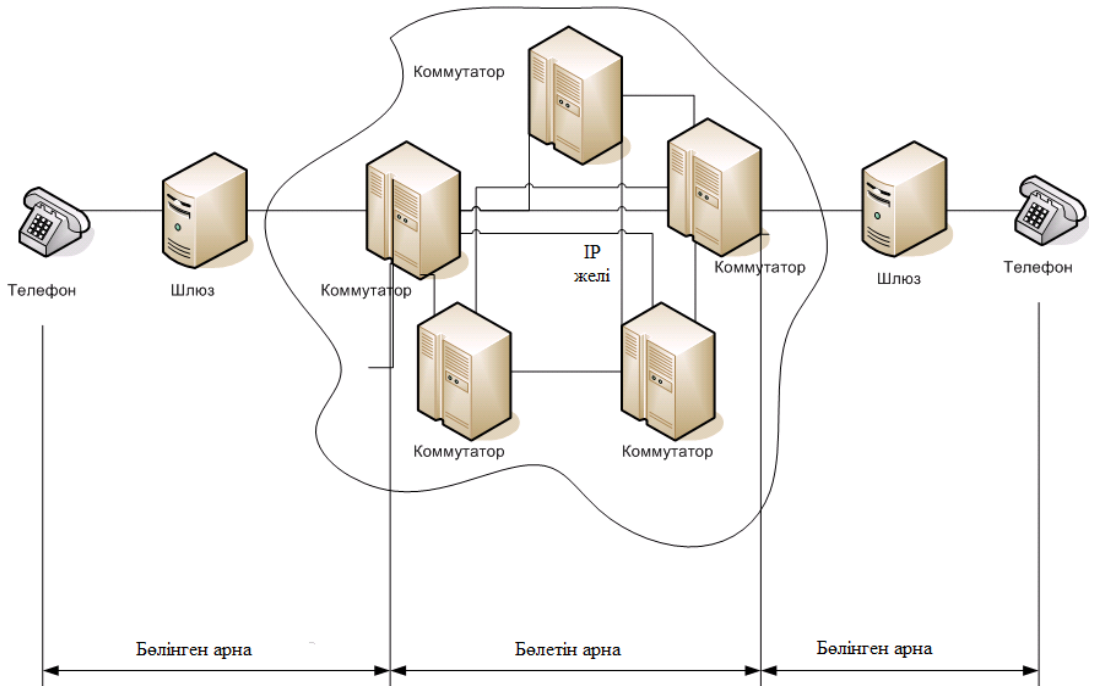
Шлюз-бұл IP желісіне және телефон желісіне (PBX/PSTN) қосылған қажетті құрылғы. (Жеке филиалдың АТС, кеңсенің немесе мекеменің шағын АТС, жалпыға ортақ пайдаланылатын телефон желісі, ТФОП - жалпыға ортақ пайдаланылатын телефон желісі).

1.6-суретте пакеттік коммутацияланған желі көрсетілген.

Міндеттері:

АТС/ТФОП қоңырау шалушы абонентіне жауап;

Қашықтағы шлюзге қосылуды орнату;



1.6-сурет – IPsec протоколының коммутациялық пакеттердің желімен байланысы

- mini-ATS/TFOP-қа қоңырау шалатын абонентпен байланыс орнату;

-Дыбыстарды/ рұқсаттарды қысу, орау және қайта құру.

Осыған байланысты шлюз оларды тікелей байланыстыратын ИҚ телефония құрылымының негізгі және ажырамас бөлігі болып табылады-желі және телефон желісі.

Әр түрлі өндірушілердің шлюздері телефон желісіне қосылу тәсілімен, өткізу қабілеттілігімен, құрылғы платформасымен, кодектерімен, интерфейсімен және басқа сипаттамаларымен ерекшеленеді. Бірақ барлық шлюздер жоғарыда аталған тапсырмаларды орындайды, олар ИҚ телефония технологиясының негізі болып саналады.

Менеджер немесе қақпашы - бұл тек IP желісіне қосылатын және IP телефония желісінің барлық логикалық операцияларын орындайтын қосымша құрылғы.

Міндеттері:

Жазылушының аутентификациясы және авторизациясы;

Шлюздер арасындағы қоңырауларды бөлу;

Шот-фактура.

Ережелерге сәйкес, менеджер есепшот бағдарламасының өзін сақтамайды, тек стандартты интерфейске негізделген мамандандырылған үшінші тарап есепшот жүйесінен тұрады, сонымен қатар оператордың жеке есепшот бағдарламасын өңдейтін API-мен жабдықталған.

Кез-келген IP телефония желісі екі немесе одан да көп шлюзі бар диспетчерді қажет етеді. Бастапқы шлюздерде (vocaltec, Vienna және т.б. негізіндегі алғашқы нұсқалар) диспетчердің міндеттерін шлюздердің өздері орындады. Технологияның дамуына және интернет-телефония желісінің қарқынды өсуіне байланысты диспетчердің міндеттері арнайы модульдің көмегімен шешілді. Тіпті кейбір өндірушілерде диспетчер физикалық түрде шлюз сияқты бір жүйеде болуы мүмкін, логикалық тұрғыдан бұл бөлек модуль.

Монитор-бұл IP телефония желісіндегі қосымша модуль, ол тек монитор қашықтағы конфигурацияны және басқа желілік құрылғыларды - IP желісіне қосылған шлюздер мен менеджерлерді қосу үшін қолданылады.

1.4.2 IP - телефония желісіндегі байланыстардың түрлері

IP телефония тарифтік жоспарлардың үш түрімен ұсынылған:

- "компьютер-есептеу машинасы";
- "компьютер-телефон";
- "телефон-телефон".

"Компьютер - компьютер" жоспары Интернетке қосылған мультимедиялық құрылғылармен жабдықталған тұрмыстық компьютерлер негізінде жүзеге асырылады. Ең көп таралған бағдарламалық жасақтама-MicroSoft NetMeeting.

"Компьютер - телефон" тарифтік жоспары кез-келген анықтамалық және ақпараттық интернет-қызметтерде, мысалы, веб-беттердегі техникалық қолдау қызметтерінде қолданылады.

"Телефоннан телефонға" тарифтік жоспары IP-телефонияның басқа тарифтік жоспарларынан ерекшеленеді, өйткені оны пайдалану қарапайым абоненттерге жергілікті және халықаралық телефон қоңырауларын шалумен шектеледі. Қызмет провайдері өзінің шлюз құрылғысын HTS коммутациялық орталығына қосады және Интернет немесе көрсетілген арна арқылы басқа қалада немесе елде орналасқан абонентпен байланысады.

"Телефон - телефония" тарифтік жоспары бойынша қызмет қарапайым тәсілмен ұсынылады. Қызмет провайдері өзінің телефон картасын немесе мекен-жай картасын шығарады.

Бұл жоспарды жүзеге асырудың басқа нұсқалары болуы мүмкін: телефон картасының орнына балама төлем ақпаратын пайдалануға болады. Қоңырау шалғаннан кейін абонентке қоңырау құны үшін шот-фактура жасалады, бұл процесс кез-келген қалааралық қоңыраумен бірдей.

1.4.3 Заманауи желілердегі қауіпсіздікті ұйымдастыру

Мүмкіндігінше, желілік жабдыққа, соның ішінде коммутаторларға рұқсатсыз кіруге тыйым салынуы керек және мүмкіндігінше абоненттік емес барлық жабдықтар арнайы жабдықталған қызметтік бөлмеде сақталуы керек. Бұл компьютерлерді зиянкестерден қорғауға мүмкіндік береді. Сонымен қатар, сіз әрқашан рұқсат етілмеген желілік құрылғыларды тексеріп отыруыңыз керек, олар кейде тікелей желілік кабельдерге "соғылуы" мүмкін. Мұндай құрылғыларды әртүрлі жолдармен анықтауға болады, мысалы, желіде "бөтен" құрылғының болуын анықтайтын сканерлерді (Internet Scanner, Nessus) пайдалану.

Инфрақұрылымды қорғаудың тағы бір оңай жолы-мекенжайларды бақылау. (FR, IP, ATM) - белгісіз мекенжайлары бар телефондарды шлюздерге немесе дауыстық деректерді жіберетін басқа желілік құрылғыларға қосуға болмайды. Бұл чаттарға немесе chats сияқты есептік жазбаларға рұқсатсыз кіруге жол бермейді. MAC мекен-жайы жалған болуы мүмкін, бірақ мұндай қарапйым қорғаныс шараларын ескермеңіз және болашақта үлкен проблемаға тап болыңыз.

Диспетчерлерге, шлюздерге және телефондарға дауыстық трафик үшін арнайы VLAN тағайындалады. Жоғарыда айтылғандай, виртуалды желілер зиянкестердің өмірін қиындатады, бірақ олар барлық байланыс мәселелерін шеше алмайды. Шабуылдаушылардың коммутация ортасында деректерді ұстаудың өзіндік әдістері бар.

2 ВИРТУАЛДЫ ЖЕКЕ ЖЕЛІЛЕРДІ АНЫҚТАУ

2.1 Пайдаланушылық виртуалды жеке желілерді анықтау

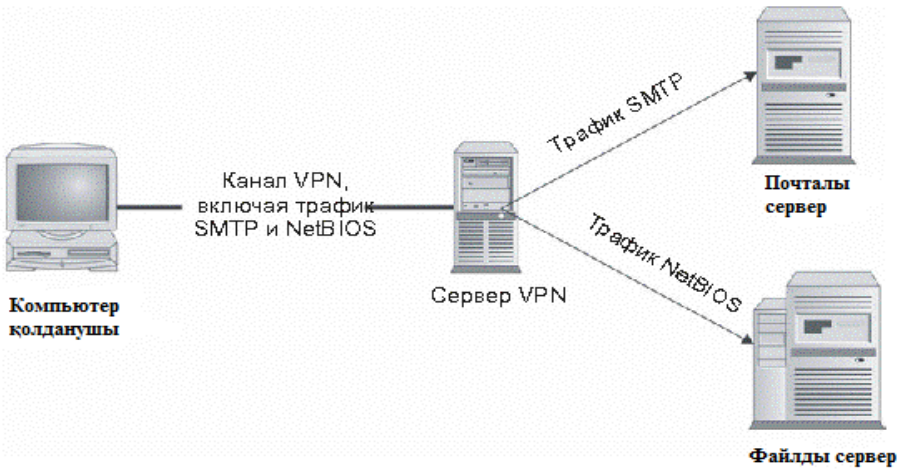
Біз Интернет арқылы жалға алынған байланыс арналарын пайдаланбай және трафиктің құпиялылығын қамтамасыз ету үшін барлық мүмкін шараларды қолданбай, ұйымға құпия деректерді беруге тырысамыз. Біздің трафикті басқа ғаламдық желі пайдаланушыларынан қалай ажыратамыз? Бұл сұрақтың жауабы-шифрлау.

Интернеттен трафиктің кез-келген түрін таба аламыз. Бұл трафиктің көп бөлігі жалпыға қол жетімді және оны осы трафикті бақылайтын кез-келген қолданушы тани алады.

VPN әр сипаттамасын нақты сипаттамаларын қарастырайық. Жоғарыда айтылғандай, VPN трафигі тыңдаудан қорғау үшін шифрланады. Шифрлау өзектілігі жойылғанға дейін берілетін ақпараттың құпиялылығын сақтауға жеткілікті қуатты болуы тиіс. Пароль 30 күнге әрекет ету уақытына ие (парольдерді өзгерту саясаты әр бір 30 күн сайын қарастырылды); бірақ парольдер көптеген уақыт бойы өз құндылығын ешқашан жоғалтпайды. Осыған сай шифрлеу алгоритмі сонымен қатар VPN-ды бірнеше жыл бойы пайдалану трафикті рұқсатсыз шифрлеудің алдын алады.

Екінші сипаттама қашықтағы сайтты сәйкестендіруді жүзеге асырумен сипатталады. Осы сипаттама орталық серверде бірнеше пайдаланушыларды сәйкестендіруді немесе VPN қосатын 2 тораптарды сәйкестендіруді талап етеді. Қолданылатын сәйкестендіру тетігі саясатпен бақыланады. Саясат пайдаланушыларды екі параметрі бойынша немесе динамикалы парольдерді пайдалана отырып сәйкестендіруді көздеуі мүмкін. Өзара сәйкестендіру кезінде екі сайтта да ортақ құпияларды ұсыну талап етіледі (құпия ретінде екі сайтқа бұрыннан анық ақпарат алынады) немесе сандық сертификаттар талап етіледі.

Виртуалдық жеке желі әр түрлі хаттаманы, әсіресе қолданбалы деңгейлі хаттамаларды қолдауды қамтамасыз етеді. Мысалы, қашықтағы пайдаланушы файлдық сервермен бір уақытта қосылуы үшін NetBIOS арқылы пошта серверімен байланыс үшін SMTP хаттамасын пайдаланады. Көрсетілген екі хаттама 2.1-суреттегідей бірдей байланыс циклімен немесе VPN арнасымен жұмыс істеуге болады.



2.1-сурет – Виртуалды жеке желілер көптеген хаттамаларға ие

VPN екі нысандарды біріктіреді, сонымен қатар ол арқылы екі абоненттің арасындабір арнаны орнатады. VPN әр шықпалы нүктесі екінші шықпалы нүктесі бар көптеген VPN қосылыстарын қолдай алады, бірақ нүктенің әрқайсысы басқасымен салыстырғанда бөлек болып келеді, және трафиктер шифрлаумен бөлінеді.

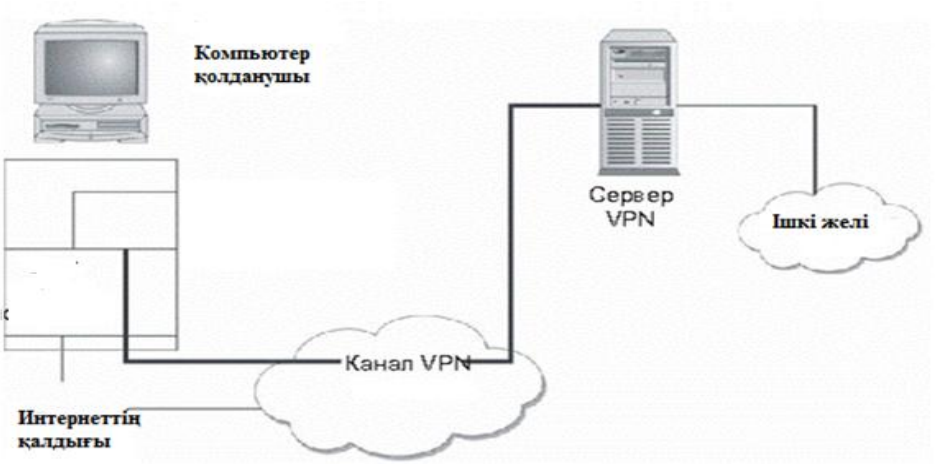
Виртуалды жеке желілер әдетте екі түрге бөлінеді: VPN пайдаланушысы және торапты VPN. Желідегі трафикті бөлудің әрбір тәсілінде, олардың арасындағы айырмашылықты әдістерде пайдалану көзделеді.

Пайдаланушы VPN жеке қолдану жүйесі мен желі немесе ұйым торабы арасында құрылған виртуалдық жеке желілерді көрсетеді. Көптеген жағдайларда пайдаланушы VPN жолға шыққанда немесе үйде жұмыс істейтін қызметкерлер пайдаланады. VPN сервер ұйымның желіаралық экран немесе жеке VPN сервері болуы мүмкін. Пайдаланушы жергілікті қызмет жеткізушілеріне телефон арқылы, DSL арнасы немесе кабельдік модем арқылы интернетке қосылады және ұйымның VPN-байланысын интернет арқылы анықтайды.

Ұйымның торабы пайдаланушы көмегімен сәйкестендіру деректерін сұратады, егер сәйкестендіру сәтті орындалса, пайдаланушыға ұйымның ішкі желісіне қатынауды іске асыруға мүмкіндік тудырады, өйткені пайдаланушы желі ішінде және іс жүзінде желі ішінде болады. Желілік байланыс жылдамдығы пайдаланушының интернетке қосылу жылдамдығымен шектелуі мүмкін.

Қолданушылық VPN ұйымға қашықтағы пайдаланушылардың жүйемен файлға кіруін шектеуге мүмкіндік жасайды. Бұл шектеу ұйым саясатына негізделуі тиіс және VPN өнімінің мүмкіндігіне тығыз байланысты.

Бұл кезде пайдаланушы VPN-ұйымның ішкі желісімен байланысы бар, ол сондай-ақ интернетке қосыла алады немесе әдеттегі интернет пайдаланушысы сияқты басқа функцияларды орындай алады. VPN желісі 2.2 суретте көрсетілген бойынша, пайдаланушының компьютеріндегі басқа да жеке қолданбаларды қолдайды.



2.2-сурет – Пайдаланушылық VPN баптаулары

2.2 Пайдаланушылық VPN артықшылықтары

Пайдаланушы VPN екі маңызды артықшылықтары бар:

- Сапарда жүрген қызметкерлер серверлермен қосылу үшін жоғары бағамен қалааралық және халықаралық телефон қоңырауларын қажетсіз кез келген мезетте электрондық пошта, файлдар және кіші жүйеге қол жеткізе алады.

- Үйде жұмыс істейтін қызметкер жоғары бағаның бөлінген арналарын жалға алмай, ұйым қызметкерлері сияқты желі қызметтеріне қол жеткізе алады.

Бұл екі артықшылық ақша үнемдеу санына жазылуы мүмкін. Үнемдеу халықаралық және қалааралық қосылыстарды, жалға алынған байланыс арналарын қолданудан бас тартумен немесе қызметкердің кіріс телефон қоңырауын қабылдайтын серверлердің әкімшіліктік міндетін орындауымен өзара байланысты. Үй пайдаланушыларында DSL немесе кабельді модемді пайдалану 56 Кбит/с жылдамдықпен телефон байланысын пайдаланған кезде қол жетімді болуы мүмкін. Бірнеше қонақ үй нөмірі желіге қосылу мүмкіндігімен жабдықталады, сол үшін іссапарға жіберілетін пайдаланушылар үшін желіге қосылатын жоғары жылдамдықты қолжетімділіктің барлық шарттары жасалады.

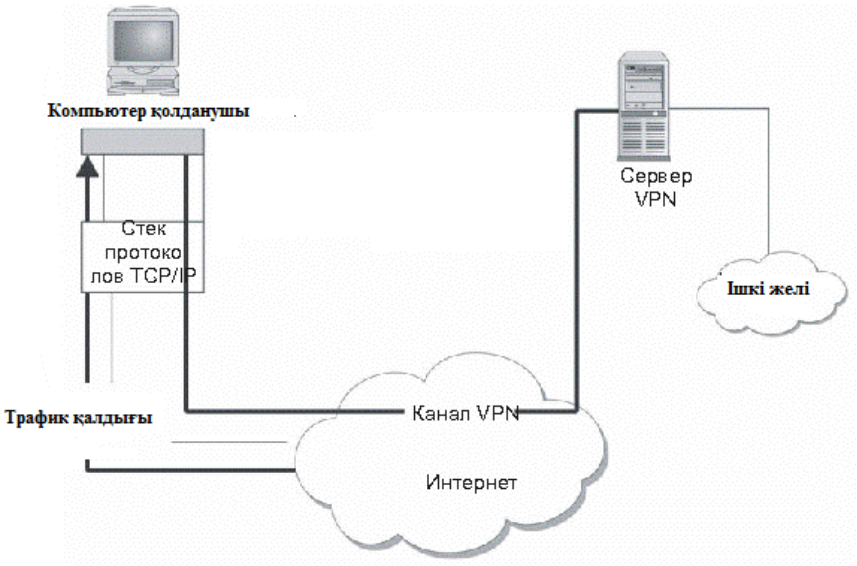
2.2.1 Пайдаланушылық VPN байланысты мәселелер

VPN пайдаланушылық қолдану ұйымның шығынын азайтуы мүмкін, бірақ VPN пайдаланушылық барлық мүмкін проблемаларды шешу болып табылмайды. Оларды пайдалану кезінде қауіпсіздікпен, іске асыру мәселелерімен байланысты елеулі қауіп туындайды, оларды ескеру керек.

VPN пайдаланғанда, пайдаланушы пайдаланатын ең үлкен қауіпсіздік мәселесі интернеттің барлық басқа сайттармен байланысын қарастырады.

Ережеге сәйкес, VPN бағдарламалық жасақтамасы пайдаланушының компьютеріндегі трафик vpn бойынша таралуы мүмкін немесе оны басқа сайтқа ашық түрде жіберу қажет екенін анықтайды. Егер пайдаланушының компьютерінде "үш есімді" пайдалану арқылы шабуыл жасалса, онда кез келген сыртқы рұқсатсыз пайдаланушы қызметкердің компьютерін ұйымның ішкі желісіне қосу үшін пайдаланады, ол 2.3-суретте бейнеленген. Бұл түрдегі шабуылдар өте қиын, бірақ нақты болады.

VPN пайдаланушы басқаратын, сонымен қатар ішкі жүйемен байланысты мәселелерді қажет етеді. Кейбір кезде VPN қолданушылары пайдаланушы идентификаторларына немесе Windows NT немесе Windows 2000 доменіндегі пайдаланушы басқарудың орталықтандырылған жүйесіне байланысты. Бұл функция пайдаланушыны басқаруды оңтайлы етеді, бірақ әкімшіге бұрынғыдай мұқият сақтау және қашықтан VPN-қол жеткізу қандай пайдаланушыларға қажет екенін бақылау қажет.



2.3-сурет – Ұйымның ішкі желісіне кіру үшін «троя атын» пайдалану

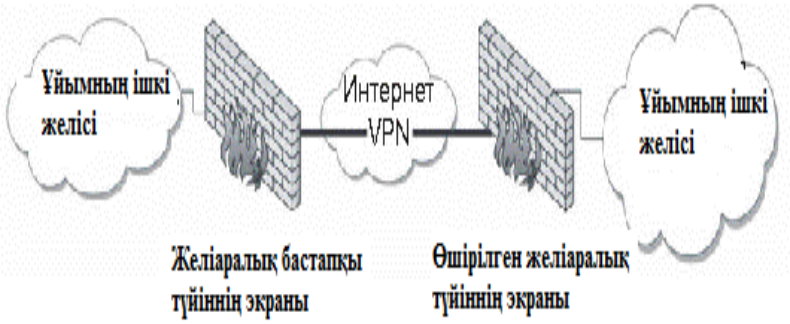
2.2.2 VPN тораптық желілерін анықтау

Тораптық жеке желілер қашықтағы тораптарға қосу немесе жоғары бағалаудың нақты арналарын қолданбай, ұйым қызметіне қатысты ақпарат алмасуды жүзеге асыру үшін қажетті екі түрлі ұйымдар арасында қосылуды жүзеге асырады. Әдетте, VPN бір желі аралық экран немесе 2.4 суретте көрсетілгендей шекаралы бағдарды басқа балама құрылғымен қосады.

Қосылысты анықтауға бір торап трафикті өзге торапқа таратуды жүзеге асырады. Нәтижесінде VPN қосылымының қарама-қарсы екі түйінінде VPN болады. Екі шығыс тораптарын қосу параметрлері тораптардың түріне байланысты анықталады. Екі сайт да бір-бірін құпиялық ортамен немесе ашық

кілт сертификатымен сәйкестендіреді. Кейбір ұйымдар VPN желісін жалға алынған арналар үшін қосымша арналар ретінде пайдаланады.

Осы баптаумен жұмыс істегенде бағдардың дұрыс құрылуын қамтамасыздандыру қажет. Сондай ақ, VPN үшін пайдаланылатын физикалық байланыс арналары міндетті түрде жалға алынған қосылыстардан ерекшеленуі тиіс. Физикалық байланыс арнасы екі бірдей қосылу арқылы жүзеге асырылуы мүмкін, соның нәтижесінде артықшылықтың керекті деңгейі қамтамасыз етілмейді.



2.4-сурет – Ғаламтор арқылы өтетін VPN торап аралық қосылысы

2.2.3 Тораптық VPN артықшылықтары

Пайдаланушы VPN сияқты, торапты VPN негізгі артықшылығы үнемді пайдалану болып табылады. Бір-бірінен алыс шағын ұйымдар бір-бірімен қашықтағы екі кеңсені біріктіретін жеке виртуалды желі құрады. Оларды пайдалану кезінде қауіпсіздікпен, есептеу үшін қажетті іске асыру мәселелерімен байланысты қауіп туындайды.

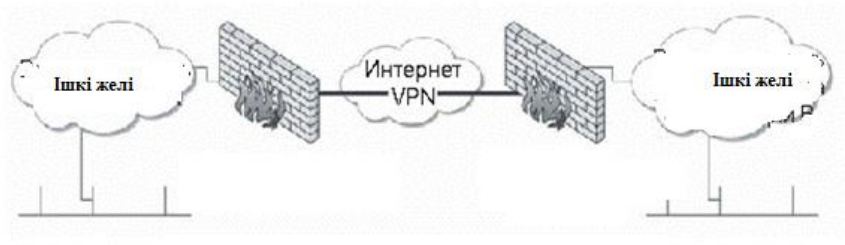
Пайдаланушы VPN пайдаланушылардың жүйелер мен файлдарға кіруін шектейді. Бұл шектеу ұйым саясатына негізделуі тиіс және VPN өнімінің мүмкіндігіне байланысты болып келеді.

Торапты VPN жаңа алыстатылған тораптарды не тіпті алыстатылған ұйымды қосу көмегімен ұйым қауіпсіздік периметрін ұлғайтады. Егер қашықтағы тораптың қауіпсіздігінің деңгейі аз болса, VPN сыншыл ойлаушыға орталық тораптарға қол жеткізуге және ұйымның басқа да ішкі жүйесіне қол жеткізуге мүмкіндік жасайды. Осыған сай ұйымдарның толықтай қауіпсіздігі үшін қатаң саясатты қолдану және аудит функцияларын жүзеге асыру қажет. Қолданылатын желіде VPN бағдарламалық қамтамасыз ету трафик VPN көмегімен таратылуы немесе басқа сайтқа ашық түрде жіберілуі тиіс екенін анықтайды.

Тораптық VPN идентификациясы қауіпсіздікті қамтамасыз етудің маңызды шарты болып табылады. Әртүрлі өндірушілер өнімді сатуды шектеу, аспекті, лицензиялау және бағдарлама бойынша ұсыныстарды шектеу сияқты

мәселелерге байланысты түрлі алгоритмдер бойынша ұсыныстарды қарастырады. Пайдаланушылық VPN ұқсас VPN-сервері VPN-трафикті шифрлеуді және дешифрлеуді жүзеге асыруы тиіс. Егер трафик деңгейі үлкен болса, VPN сервері жүктеледі. Көптеген жағдайларда бұл желіаралық экран VPN сервері болған кезде кездеседі.

Адресацияға байланысты мәселені ойластыру керек. Бұл жағдайда, егер сіз тораптық VPN ұйым ішінде пайдалансаңыз, онда барлық тораптарды адрестеу схемасы қажет. Бұл кезде адресация қандай да қиындықтар әкеледі. Егер VPN екі түрлі ұйымдарды қосу үшін қолданса, онда адресацияға қатысты барлық келіспеушіліктер туралы шешім қабылдау керек. 2.5 суретте туындаған даулы жағдай бейнеленді. Бұл ретте екі ұйым бірдей мекенжай кеңістігін пайдаланады (10.1.1.X желі).



2.5-сурет – Тораптық VPN адрестелумен байланысты келіспеушіліктерді тудыруы мүмкін

Бір-бірімен адрестеу схемасы келіспеушілік болатыны белілі, бағдарлану жұмыс жасамайды. Бұл кезде VPN-ның әрбір жағы желілік мекенжайды жіберуді және басқа ұйымдардың жүйесін өзінің жеке адресация сұлбасына бағыттауды орындауы тиіс.

2.2.4 VPN фукнциясының стандарттық технологиялары түсінігі

VPN желісінің төртмаңыздықұрамдас бөліктері:

- VPN сервер.
- Шифрлаудың алгоритмі.
- Сәйкестендіру жүйелері.
- VPN хаттама.

Аталған құрамдас бөліктер қауіпсіздік бойынша талаптар, өнімділік және өзара әрекеттесік қабілеттілігі бойынша сәйкестікті жүзеге асырады. VPN архитектурасы қаншалықты дұрыс жүзеге асырылғаны талаптардың дұрыс анықталуына байланысты болады.

Талаптарды анықтау мынадай аспектілерден тұруы тиіс.

- Ақпаратты қорғауды қамтамасыз ету үшін қажетті уақыт саны.
- Пайдаланушылардың бір мезгілдегі қосылыстар саны.

- Пайдаланушыларды қосудың күтілетін түрі (үйде немесе сапарда жұмыс істейтін қызметкерлер).
- Қашықтағы серверлік қосылыстар саны.
- Қосылу қажет болатын VPN желісінің түрі.
- Қашықтағы тораптардағы кіріс және шығыс трафигінің күтілетін көлемі.
- Қауіпсіздік параметрлерін анықтайтын қауіпсіздіктің саясаты.

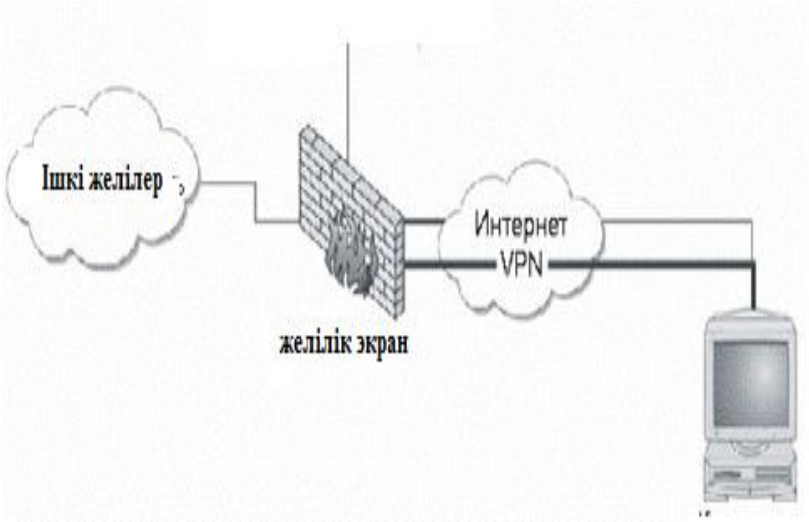
Олардың негізінде көптеген жұмыс принциптері бар, бірақ дұрыс баптағанда құралдың екі түрі шектеулі трафикті бұғаттаумен сипатталатын қауіпсіздіктің қызметінің дұрыс болуын қамтамасыздандырады.

2.3 VPN сервері

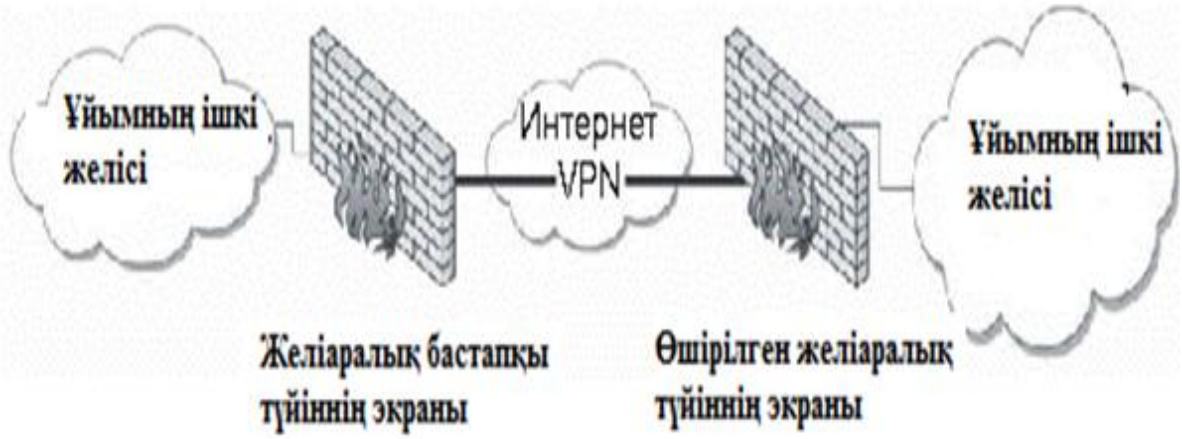
VPN сервері VPN шығыс байланыс торабының рөлінде берілетін компьютер ретінде сипатталады. Бұл сервердің күтілетін жүктемені қолдау үшін жеткілікті сипаттамалары болуы тиіс. Көптеген VPN бағдарламалық жасақтама өндірушілері VPN-қосылыстар санына қарамастан процессордың өнімділігі мен жадыны баптау туралы нұсқаулықты ұсынуы тиіс.

Күтілетін жүктемені қамтамасыз ету үшін көптеген VPN серверлерін құру керек болуы мүмкін. Бұл кезде күтілетін VPN қосылымы жүйе ішіндеаз уақыт ішіндетаралуы тиіс.

VPN-сервері желіде орналасады. Ол 2.6-суретте бейнеленгендей желіаралық экран не шекаралық бағдарлауыш та болуы мүмкін. Балама ретінде сервер жеке жүйе ретінде қарастырылуы мүмкін. Мұндай жағдайда сервер 2.7 суретте көрсетілген белгілеген демилитаризацияланған жерде (DMZ) орналасуы тиіс. Нақтырақ айтсақVPN демилитаризацияланған аймақ тек VPN серверінен тұруы тиіс және DMZ интернеттен жойылуы тиіс. Бұл VPN-сервері авторизацияланған пайдаланушыға ішкі жүйеге қолжетімділікті ұсынып, тиісінше, сенімді пайдаланбайтын адамдар арасында ғана орын алатын жоғары сенімділік объектісі ретінде қарастырылуы тиіс. Желіаралық экран және VPN трафик ережелері, таралу аймағы және милитаризацияланған қызметкерлер тек қана жиынтықтармен қорғалады.



2.6-сурет – Желіаралық экран VPN-сервер болып табылатын VPN желісінің архитектурасы



2.7-сурет – Жеке VPN сервері үшін VPN желісінің архитектурасы

2.3.1 Шифрлау алгоритмі

VPN қолданатын шифрлаудың алгоритмі стандартты ең қуатты шифрлау алгоритмі болуы тиіс. Негізінен VPN құру кезінде барлық стандартты қуатты алгоритимдер тиімді қолданылады. Әр түрлі өндіруші компаниялар өнімді сатуды шектеумен, аспектілер, лицензиялау және бағдарлама бойынша ұсынысты шектеуге байланысты әр түрлі алгоритмдерге ұсыныстарды қарастырады. VPN программалық пакетін алып, маманның пікірін тыңдау керек сонымен қатар өндірушілер шифрлеудің қуатты алгоритмдерін қолданады.

Қате іске асырылған жүйе шифрлаудың ең қуатты алгоритмін пайдасыз ете алады. VPN көмегіменберілетін ақпаратқа қол жеткізу үшін қастықойлау міндеттері:

– барлық қосылу сеанстарын қамту, яғни тыңдау құрылғысы барлық VPN трафигімен берілуі тиіс;

– үлкен есептеуіш қуатты және үлкен көлемді уақытты ауыр күш пен трафикті шифрлеу арқылы кілтті алу үшін пайдалану.

2.3.2 Сәйкестендіру жүйесі

Архитектураның үшінші буыны ретінде VPN сәйкестендіру жүйесі қаралатын болады. VPN сәйкестендіру жүйелері екі фактордан тұрады. Пайдаланушыларды сәйкестендіру олар білетін ақпарат арқылы немесе жеке басын білетін тұлғаны пайдалана отырып жүргізіледі. Пайдаланушы VPN қолданғанда бірінші екі нұсқаға ұсыныс қарастырылуы тиіс.

Сәйкестендіру құралының оң құрылымы түрінде сәйкестендірілген нөмірмен немесе парольмен байланысты смарт-карталар қарастырылады. Бағдарламалық жасақтаманы өндірушілер ұйымдарға ережеге сәйкес таңдалған бірнеше сәйкестендіру жүйелерін ұсынады.

2.3.3 VPN хаттамасы

VPN хаттамасы, сондай-ақ басқа да ұйымдармен ғаламторда әрекет ететін және жүйенің қорғау деңгейін анықтайды. Егер қарастырылып отырған ұйым VPN-ды тек ішкі деректер алмасуға пайдаланса, өзара іс-қимыл туралы мәселені жауапсіз қалдыра алады. Бірақ, егер де ұйым басқа ұйымдармен байланысқа VPN пайдаланса, онда өз хаттамасын пайдалану мүмкін емес болады. VPN хаттамасы жүйенің жалпы қауіпсіздігінің деңгейіне ықпалын көрсетеді. Бұл VPN протоколы екі шығыс түйіндерінің арасында шифрлау кілтімен алмасуға қолданылады. Егер бұл тарату қорғалған болмаса, онда қолтық асты кілтін алуға және VPN барлық артықшылығы бар трафик оқуға болады.

Қосылған кезде стандартты хаттамаларды пайдалану ұсынады. Қазіргі кезде IPSec VPN үшін стандартты хаттама болып есептелінеді.

InternetProtocolSecurity (IPSec) стандартында Internet-жүйе деп аталады. Шын мәнінде, IPSec-қазіргі кезде толық ядросы бар ашық стандарттардың біріккен жиынтығы, және ол жаңа хаттамалармен, алгоритмдермен және функциялармен айтарлықтай оңай толықтырылуы мүмкін.

IPSec хаттамасының негізгі мақсаты — IP желілері бойынша деректерді қауіпсіз беруді қамтамасыз ету. IPSec пайдалануға мүмкіндік береді:

- тұтастық, яғни деректерді таратқанда сығылған, жойылған немесе ауыстырылған болмауы тиіс;
- сәйкестік, яғни деректер жіберушіге берілетін болады, ол кім екенін растайды;
- құпиялылық, яғни ақпарат рұқсат етілмеген ұсыныстың алдын алу түрінде жіберіледі.

(Классикалық анықтамаға сәйкес, деректер қауіпсіздік түсінігі тағы талап–қарастырылып отырған контексте оларды жеткізу кепілдігі ретінде қарастырылуы мүмкін деректердің қол жетімділігін анықтайды. IPSec хаттамасы TCP транспортты деңгей хаттамасын қалдырып, бұл міндетті орындай алмайды).

2.3.4 Әртүрлі деңгейдегі қорғалған арналар

IPSec жалпы қол жетімді (қорғалмаған) желі бойынша деректерді берудің ең кең тараған және ең қауіпсіз технологияларының бірі болып табылады. Бұл технология үшін ортақ ат-қорғалған арна (secure channel) қолданылады. «Арна» термині деректерді қорғау желінің екі торабы (хост пен шлюз) арасында бірнеше виртуалды желілер бойынша желіге қосылған пакеттерді коммутациялаумен қамтамасыз етіледі.

<table>
<tr><td rowspan="6">Қорғалған қолжетімділік хаттамалары</td><td>Қолданбалы</td><td rowspan="3">Қосымшаларға әсер етеді, желілік технологияға тәуелді емес</td></tr>
<tr><td>Көріністік</td></tr>
<tr><td>Сеанстық</td></tr>
<tr><td>Транспорттық</td><td></td></tr>
<tr><td>Желілік</td><td rowspan="3">Қосымшалар үшін анық, желілік технологияға тәуелді</td></tr>
<tr><td>Арналық</td></tr>
<tr><td>Табиғи</td></tr>
</table>

2.9-сурет – Қорғалған арнаның хаттамалар деңгейі

2.9-суретте қорғалған арна көрсетілген OSI моделінің әртүрлі деңгейінде іске асырылған жүйелі құралдармен құруға болады. Егер қызметтерді қорғау үшін жоғары деңгейдегі (қолданбалы, көріністік не сеанстық) сипаттамалар пайдаланылса, онда қандай қорғаныс әдісі (IP немесе IPX, Ethernet немесе ATM) деректерді тарату үшін пайдалануға байланысты емес, ол бір жағынан, ал жойылған қосымшалар осы уақытта нақты қорғаныс хаттамасына тәуелді, яғни қосымшалар үшін мұндай хаттамалар айқын болып саналмайды.

Арнаның қорғалу деңгейі пайдалану үшін пайдаланылғанына байланысты, ол шектеулі әрекет аймағы бар. Хаттама тек толық белгілі бір қызметті-файлдық, гипермәтіндік немесе пошта қызметін қорғайды. Мысалы, S/MIME хаттамасы тек электрондық пошта хабарын қорғайды. Сондықтан әр бір қызметке хаттаманың тиісті нұсқасын дайындау керек.

Secure Socket Layer (SSL) сонымен қатар оның жаңа ашық іске асырушысы Transport Layer Security (TLS) басқа деңгейде жұмыс істейтін, қорғаныс арналарының аса танымал хаттама болды. Хаттама деңгейін төмендету оны әмбебап қорғаныс құралы етеді. Енді кез келген қосымшалар, қолданбалы деңгейдегі хаттамалар, кез келген және бірыңғай қорғаныс

хаттамаларын пайдалану. Алайда, қолданба бұрынғысынша жазылуға тиіс – оларда қорғалған арна протоколының функциялары анық қоңыраулары орнатылуы тиіс.

Арнаның қорғау құралдары төмен іске асса, оларды қосымша мен қосымша хаттамаға мөлдірлету қиын емес. Желілік сонымен қатар арналық деңгейде қорғау хаттамасынан қосымша тәуелділігі толық жойылады. Алайдамұнда біз нақты желілік технологиялардан қорғау хаттамасы тәуелділігі басқа мәселемен қақтығысамыз. Шынымен, ірі құрамды желі әрі бөлігінде, жалпы айтқанда, әртүрлі арналы хаттамапайдаланылады, сол үшін арналық деңгей бірыңғай хаттама арқылыбұл гетерогенді ортаға қорғалған арнаны орындау мүмкін емес.

Мысалы, арналы деңгейде жұмыс істейтін қорғалған Point-to-Point Tunneling Protocol (PPTP) арнасының протоколын қарастырайық. Ол "нүкте-нүкте" байланысты кеңінен пайдаланатын PPP стандарттарында негізделген, мысалы, айтылған желілермен жұмыс істеу кезінде.

PPTP хаттама қолданбалы деңгейдің қызметі және жүргізу үшін қорғаныс құралдары мөлдірлігін қамтамасыздандырмай, сондай ақ желілік деңгей қабылданатын хаттамаға тәуелді болмайды: көбіне, PPTP хаттама IPX, DECnet не NetBEUI хаттамасының негізінде жұмыс істейтін, желіде және IP желісінде пакеттітарата алады. Бірақ, PPP барлық желіде пайдаланбайтындықтан (көптеген жергілікті желілер арналық деңгейде Ethernet протоколы жұмыс істейді, ал жаһандық - ATM, frame relay протоколдары), онда PPTP әмбебап құрылғы болып саналмайды.

Желілік деңгейде жұмыс істейтін IPSec хаттама ымыралы болып есептелінеді. Бір жағынан, ол қолданба үшін мөлдір, ал екінші жағынан-ол барлық желіде жұмыс істей алады, өйткені ол кең тараған IP протоколына негізделген: қазіргі кезде әлемдегі компьютерлердің тек 1% - ы IP-ді қолдамайды, тұтастай алғанда, қалған 99% оны жалғыз хаттама ретінде немесе бірнеше хаттамалардың бірі ретінде пайдаланады.

2.4 IPSec хаттамалары арасында функциялардың таралуы

IPSec ядро 3 хаттамадан құрылады: идентификация хаттамасы (Authentication Header, AH), шифрлаудың хаттамасы (Encapsulation Security Payload, ESP) және кілттерді алмасу хаттамасы (Internet Key Exchange, IKE). Қорғалған арна қолдау функциялары келесі хаттама арасында қолданылады:

- AH хаттамасы сәйкес деректердің толықтығына кепілдік бере алады
- ESP хаттамасы құпиялыққа кепілдік беріп, берілетін деректерді шифрлайды, бірақ ол сондай-ақ деректерді сәйкестендіруді және толықтығын қолдай алады;
- IKE хаттамасы деректерді идентификациялау және шифрлау хаттамасының жұмысына керекті құпия кілттер арнасы соңғы нүктесін автоматты түрде ұсынудың қосымша мәселесін шешеді.

Құрылымның қысқаша сипаттамасындағыдай, АН сонымен қатар ESP хаттамасының функциялары біртіндеп жабылады. АН хаттамасы тек деректердің сәйкестендірілуіне және толықтығына ғана жауап береді, ESP хаттамасы қуатты, өйткені деректерді шифрлеуге, сондай-ақ АН хаттамасының функцияларын орындауға болады (бірақ біз байқағанындай, идентификация мен толықтық бірнеше қысқартулармен қамтамасыз етіледі). ESP хаттамасы шифрлау және сәйкестендіру/толық функцияларын кез келген комбинацияларда, яғни функциялардың басқа да топтарын немесе тек шифрлауды қолдай алады.

IPSec деректерін шифрлау үшін құпия кодты қолданатын шифрлеудің кез келген симметриялы алгоритм пайдалануы мүмкін. Шифрлау тәсілдерінің бірінде деректерді толық және сәйкестендіруді қамтамасыз ету үшін – дайджест функция (digest function) немесе хэш функция (hash function) деп аталатын бір бағытты функция (one-way function) арқылы шифрлау.

Шифрланған деректер белгілі бір аз байттан тұратын дайджест-шаманың негізінде беріледі. Дайджест IP-пакеттегі шығыс хаттарымен бірге жіберіледі. Алушы дайджесті қалыптастыру үшін қандай да бір шифрлеудің бағыттаушы функциясы қолданылатынын біле отырып, оны бастапқы хабарламаларды пайдаланып қайта есептейді. Егер алынған және есептелген дайджестердің шамасы сәйкес келсе, онда бұл пакеттің құрамы беру кезінде қандай да бір өзгерістерге ұшырамағанын білдіреді. Бұл дайджест бастапқы хабарламаларды қалпына келтіруге мүмкіндік бермейді, сондықтан қорғау үшін пайдалануға болмайды, бірақ деректердің толықтығын тексеруге мүмкіндік береді.

Дайджейст бастапқы хаттарға бақылау сомасы болып табылады. Алайда айтарлықтай айырмашылық бар. Бақылау сомасын пайдалану - бұл сенімсіз байланыс желілері бойынша жіберілетін хаттардың толықтығын тексеру құралы және ол ақыл-ойдың нашар әрекеттерімен күреске бағытталмаған. Негізінен, жіберілетін пакетте бақылау сомасының болуы зиянкестерге бақылау сомасының жаңа мәнін қосып, бастапқы хатты тасымалдауға кедергі келтірмейді. Дейджейсті есептеу кезінде бақылау сомасына қарағанда құпия код пайдаланылады. Егер дейджейсті алу кезінде тек жіберушіге және алушыға белгілі параметрлері бар бір бағытты функция (онда пароль бар) пайдаланса, онда бастапқы хат кез келген модификациясы дереу анықталады.

АН және ESP екі хаттамасы арасында қорғау функцияларын бөлу шифрлау жолымен деректердің құпиялылығын қамтамасыз ету экспорт және/немесе импорт құралдарын шектеуде көптеген елде пайдаланылатын тәжірибеге негізделген. Осы еі хаттамаларының әр қайсысы дербес және басқалармен бір мезгілде пайдаланылуы мүмкін, сондықтан мұндай жағдайларда, яғни шифрлау қолданыста шектеулерден пайдаланылуы мүмкін емес болғандықтан, жүйені тек қана АН хаттамамен қою керек.

Тек АН хаттама арқылыдеректерді қорғау көпжағдайда жеткіліксіз болып кетеді, өйткені бұл кезде қабылдаушы жақ деректер дәл өзі күтелетін түйін арқылы жіберілгеніне, сонымен қатар жібергендежеткендігіне сенімді болып келеді. Рұқсаты жоқ қаралымдардан деректерді қолдану бойынша АН хаттама

оларды қорғамайды, себебі оны шифрлемейді. Деректердің шифрленуіне, олардың толықтығыжәне сәйкестендірілгенін тексеретін, ESP хаттамасын пайдалану керек.

3 Оптималды қорғаныс жүйесін және қорғау критерийлерін жобалау міндеттерінің жалпы шешімі

Жалпы қорғау критерийі ретінде қорғалмаған жүйемен салыстырғандағы қорғалған жүйедегі қауіптің меншікті төмендеуін көрсететін қорғаныс коэффициентін (D) пайдаланады.

$$D\% = (1 - R_{защ} / R_{нез}) \times 100\ \%, \qquad (3.1)$$

мұндағы $R_{защ}$ – қорғалған жүйедегі қауіп;

$R_{нез}$ – қорғалмаған жүйедегі қауіп.

Осыған байланысты, осы жағдайдағы оңтайлардыру міндеттері келесі түрде бейнеленген:

$$\begin{gathered} D(C_{ИНФ} \cdot p_{взл}) \text{—>} \max; \\ Ц_{СЗИ} \text{—>} \min; \\ П_{СЗИ} \text{—>} \max. \end{gathered} \qquad (3.2)$$

Бұл мәселені шешу үшін оны шектеу енгізудегі біркритерийлі сызықпен ұштастырамыз. Нәтижесінде келесі мәліметті аламыз:

$$\begin{gathered} D(C_{ИНФ} \cdot p_{взл}) \text{—>} \max; \\ Ц_{СЗИ} \le Ц_{зад}; \\ П_{СЗИ} \ge П_{зад}., \end{gathered} \qquad (3.3)$$

мұндағы $Ц_{зад}$ және $П_{зад}.$ – қорғаныс жүйесі мен жүйенің өнімділік бағасына қойылған шектеу.

Жалпы функционалдық қорғау жүйесін көрсететін жалпы функцияны - ақпарат қауіпсіздігін қамтитын функция деп атайды.

Қорғаныс коэффициентін қауіп параметрлері бойынша қарастырсақ. Жалпы жағдайда жүйеде бірнеше қауіптің түрлері бар. Осы шарттарға сәйкес келесі өлшемдерді ұсынсақ:

ω – жүйеге әсер ететін қауіп түрлерінің мөлшері;

C_i (i =1,ω) – i – типті бұзудың бағасы (шығын);

λ_i(i = 1,ω) –сәйкесінше, i – типті бұзу ағынының қарқындылығы;

Q_i (i = 1,ω) – жалпы ағында ақпаратқа рұқсат етілмеген әрекет жасаған кездегі

i – типті қауіптің болу ықтималдылығы, егер

$$Q_i = \lambda_i / \Lambda ;$$

p_i (i = 1,ω) –қорғаныс жүйесіндегі i – типті қауіптің болу ықтималдылық көрсеткіші.

Сәйкесінше, қорғаныс жүйесіндегі бұзулардан келген шығын коэффициентін келесі түрде өрнектейміз:

$$R(p) = \sum_{1}^{\omega} R_i(p) = \sum_{1}^{\omega} C_i \cdot p_{взлі}\,, \qquad (3.4)$$

мұндағы R(p) – i – типті бұзудың шығын коэффициенті; ол бір i – типті бұзу болған кездегі орташа шығын мөлшерін көрсетеді.

Қорғалған жүйе үшін: $p_{угрі} = Q_i$,,

Қорғалмаған жүйе үшін: $p_{угрі} = Q_i$,·(1-p_i) .

Сәйкесінше, қорғаныс жүйесінің бұзудан кезген шығын коэффициентінің уақытқа тәуелділігін келесі түрде көрсетеді:

$$R(\lambda) = \sum_{1}^{\omega} R_i(\lambda) = \sum_{1}^{\omega} C_i \cdot \lambda_{взлі}\,, \qquad (3.10)$$

мұндағы R(λ) –уақыт бірлігіндегі i – типті бұзу коэффициенті.

Қорғалмаған жүйе үшін $\lambda_{угрі} = \lambda_i$, қорғалған жүйе үшін $\lambda_{угрі} = \lambda_i$,·(1-$p_i$).Сәйкесінше, осы екі теңдеуден келесі ортақ теңдеу аламыз:

$$D = 1 - \frac{\sum_{1}^{\omega} C_i \cdot Q_i \cdot (1 - p_i)}{\sum_{1}^{\omega} C_1 \cdot Q_i} = 1 - \frac{\sum_{1}^{\omega} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_{1}^{\omega} C_i \cdot \lambda_i}. \qquad (3.5)$$

Егер бастапқы параметр ретінде қауіп болудың ықтималдылығы Q_i алынса, онда қорғаныс коэффициентін қауіп болу ықтималдылығы арқылы есептеген ыңғайлы болады. Ал егер бастапқы параметр ретінде қауіп ағынының қарқындылығы λ_i алынса, онда, әрине, қорғаныс коэффициентін қарқындылық арқылы есептейміз.

Төменде жүйенің келесі параметрлері көрсетілген.

Статистикалық бағалау әдісі. Әдісті IP-желісіне шабуылдаған үш түрлі шабуыл мысал бойынша қарастырайық: рұқсат етілмеген мүмкіндік (РЕМ), қызмет көрсетуден бас тарту (DoS), абоненттік пунктерге шабуыл.

Бір сағат ішінде рұқсат етілмеген жерлерде болған бұзудан (C_1) пайда болған шығын (бағасы) мен бұзу ағынының қарқындылығын (λ_1) анықтаймыз, шабуыл/сағ, ш.б./шабуыл:

$$\lambda_1 = 5,\ C_1 = 500,\ p_1 = 0.75.$$

Бір сағат ішінде қызмет көрсетуден бас тарту (DoS) кезінде бұзудан (C_2) пайда болған шығын (бағасы) мен бұзу ағынының қарқындылығын (λ_1) анықтаймыз, шабуыл/сағ, ш.б./шабуыл:

$$\lambda_2 = 7,\ C_2 = 800,\ p_2 = 0.8.$$

Бір сағат ішінде абоненттік пунктерге шабуыл жасау кезінде бұзудан(C_3) пайда болған шығын (бағасы) мен бұзу ағынының қарқындылығын (λ_1) анықтаймыз, шабуыл/сағ, ш.б./шабуыл:

$$\lambda_3 = 4,\ C_3 = 200,\ p_3 = 0.55.$$

i – типті қауіптің болу ықтималдылығын есептейміз $Q_i = \lambda_i / \Lambda$;
$\lambda = 20$ – рұқсат етілмеген әрекет кезіндегі ағынның жалпы қарқындылығы

$$Q_1 = \frac{5}{30} = 0.25,\ \ Q_2 = \frac{7}{30} = 0.35,\ \ Q_3 = \frac{4}{30} = 0.2.$$

$p_{угрі} = Q_i$,, ш.б болғандағы қорғалмаған жүйедегі бұзудан келген шығын коэффициентін есептейміз:

$$R(p) = 500\ 0{,}25 + 800 \cdot 0{,}35 + 200 \cdot 0{,}2 = 375$$

Қорғалған жүйеде $p_{угрі} = Q_i,\cdot(1-p_i)$.

$$R(p) = 500\ \ 0{,}0625 + 800\ \ 0{,}07 + 200\ \ 0{,}09 = 93{,}75$$

Енді қорғаныс коэффициентін есептейміз, пайыздық мөлшерде:

$$D = 1 - \frac{93.75}{375} = 0.763 = 76\,\%$$

Оптимистік– пессимистік тәсіл.

Тең қарқындылық әдісі. $\lambda_i = \alpha$, α = const. Бұл әдісте қорғаныс константасын есептеу үшін α ретінде кез келген мәнді алуға болады.Формулада бұл мән жақшада алынып тұрады және соңында өзара қысқартылып кетеді, сондықтан бұл жағдайда қорғаныс тек шығынға ғана тәуелді болады:

$$D = 1 - \frac{\sum_1^{\omega} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_1^{\omega} C_i \cdot \lambda_i} = 1 - \frac{\sum_1^{\omega} C_i \cdot \alpha \cdot (1 - p_i)}{\sum_1^{\omega} C_i \cdot \alpha} = 1 - \frac{\alpha \cdot \sum_1^{\omega} C_i \cdot (1 - p_i)}{\alpha \cdot \sum_1^{\omega} C_i} = 1 - \frac{\sum_1^{\omega} C_i \cdot (1 - p_i)}{\sum_1^{\omega} C_i};$$

$$D = 1 - \frac{500 \cdot 0.25 + 800 \cdot 0.2 + 200 \cdot 0.45}{500 + 800 + 200} = 0.75.$$

Шығынға пропорцианалды болу әдісі. $\lambda_i = \alpha \cdot C_i$, $\alpha = const$. Бұл әдісте бұзудан келген шығын көп болған сайын, осы ақпаратқа рұқсат етілмеген әрекеттер мөлшеріде көп болады деп тұжырымдайды. Яғни, қауіп ағынының қарқындылығы шығынғы тура пропорцианалды. Бұл жағдайда қорғаныс шығынның квадратына байланысты болады:

$$D = 1 - \frac{\sum_1^{\omega} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_1^{\omega} C_i \cdot \lambda_i} = 1 - \frac{\sum_1^{\omega} C_i \cdot \alpha \cdot C_i \cdot (1 - p_i)}{\sum_1^{\omega} C_i \cdot \alpha \cdot C_i} = 1 - \frac{\alpha \cdot \sum_1^{\omega} C^2{}_i \cdot (1 - p_i)}{\alpha \cdot \sum_1^{\omega} C^2{}_i} =$$

$$= 1 - \frac{\sum_1^{\omega} C^2{}_i \cdot (1 - p_i)}{\sum_1^{\omega} C^2{}_i};$$

$$D = 1 - \frac{250000 \cdot 0.25 + 640000 \cdot 0.2 + 40000 \cdot 0.45}{250000 + 640000 + 40000} = 0.75.$$

DoS шабуылдары кезіндегі мысалдарды қарастырайық, осындай шабуылдар кезіндегі пакеттердің жоғалуы мен кідіріп қалу ықтималдылығы. IP-пкеттердің ақпараттық бөлімінің ұзындығы $L_и$ = 700 кбит, қызмет бөлімінің ұзындығы $L_{сл}$ = 250 бит, бағыттаушылар арасындағы жол өткізу қабілеттілігі R_k = 1024 кбит/с.

Пакеттерге қызмет көрсеті кезіндегі жіберу уақыты μ тұрақты шама болып келеді және ол келесі түрде анықталады.

$$\mu = t_{обсл} = (L_и + L_{сл})/R_k; \qquad (3.6)$$

мұндағы: $L_и$ – пакеттегі ақпараттық бөлімнің ұзындығы, бит;

$L_{сл}$ – пакеттің қызметтік биттері (преамбула және концевик), бит;

$_k$ – бағыттаушылар арасындағы жол өткізу қабілеттілігі, бит/с;

$t_{обсл}$ – қызмет көрсету уақыты;

μ – жіберу уақыты.

Қызмет көрсету уақытын келесі формуламен анықтаймыз, с:

$$\mu = t_{обсл} = (L_и + L_{сл})/R_k \; ; \qquad (3.7)$$

$$\mu = t_{обсл} = \frac{700 + 0{,}25}{1024} = 0{,}684.$$

Пайдалану коэффициенті $К_{исп}$, келесі формулада көрсетілген:

$$К_{исп} = \frac{m * R_u}{2 * R_k} * (1 + \frac{L_{сл}}{L_u}). \quad (3.8)$$

мұндағы m – шығушы бағыттаушымен байланыс орнатқан абонеттеің саны;

$R_и$ – терминал арқылы мәліметтерді жіберу жылдамдығы, бит/с.

Сөйлесу пакетінің кешіктірілу уақыты (байланыс арнасындағы кешіктірілу оған қоса жіберу уақыты) келесі формуламен анықталады:

$$m(T) = \frac{L_И + L_{СЛ}}{R_k} \cdot \frac{L_И \cdot (0{,}75 - \frac{mR_И}{4R_К}) - \frac{mR_И}{4R_k} \cdot L_{СЛ}}{L_И \cdot (1 - \frac{mR_И}{2R_k}) - \frac{mR_И}{2R_k} \cdot L_{СЛ}}; \quad (3.15)$$

$$m(T) = \frac{700 + 0.25}{1024} \cdot \frac{700 \cdot \left(0.75 - \frac{10 \cdot 128}{4 \cdot 1024}\right) - \frac{10 \cdot 128}{4 \cdot 1024} \cdot 0.25}{700 \cdot \left(1 - \frac{10 \cdot 128}{2 \cdot 1024}\right) - \frac{10 \cdot 128}{2 \cdot 1024} \cdot 0.25} = 0.798 .$$

Желі арқылы сөйлесуді жіберудің сапалық бағасы білу үшін кезектегі кідіріс, кодектегі және қораптаудағы кідірістердің орташа сомасын анықтайтын жалпы кідірісті білген жөн. Қорытқы кідіріс $m(T_\Sigma)$ кезектігі m(T), қораптаудағы $\delta_з$ және кодерлі сөйлесудегі алгоритмдік кідірістен $\delta_{кодер}$ тұрады:

$$\delta_з = (L_и + L_{сл})/R_и = (700 + 0{,}25)/128 = 1{,}368 ;$$

$$m(T_\Sigma) = m(T) + \delta_з + \delta_{кодер} = m(T) + (L_и + L_{сл})/R_и + \delta_{кодер} \quad (3.9)$$

При $\delta_{кодер}$ = 3мс

$$m(T_\Sigma) = 0.798 + 1.368 + 0.003 = 2.169.$$

3.2 Сәйкестендіру алгоритмдері

АН атауында, MD5 немесе SHA-1 хэштілеудің стандартты криптографиялық алгоритмдерінің негізінде есептеуге болатын, ICV шамалары болады. Бақылаушы суммаларды тікелей есептеудің алгоритмдерін жүзеге асырудың орнына, бұл жағдайда Hashed Message Authentication Code (HMAC) есептеу амалы қолданылады, ол өзіне құпия кілттердің пайдаланылуын, ICV қайта есептелуімен шабуыл мүмкіндігін болдырмас үшін

қолданылады. Бұл жерде тек сәйкестендірудің қысқаша есептеу сұлбасын келтіреміз:

HMAC есептері үшін хэш-функция (оны H ретінде белгілейік) және құпия кілт K қажет болады. H процедураның көмегімен хэштегтеленетін, хэш-функция болып табылады, сәйкесінше бірізді мәліметтер блогында қолданылады. B байттарда осындай блоктардың ұзындығын, ал блоктардың ұзындығын хэштілеу нәтижесінде алынған –L ретінде белгілейміз. Содан кейін, қосымша «құпиялы» шамаларды енгіземіз

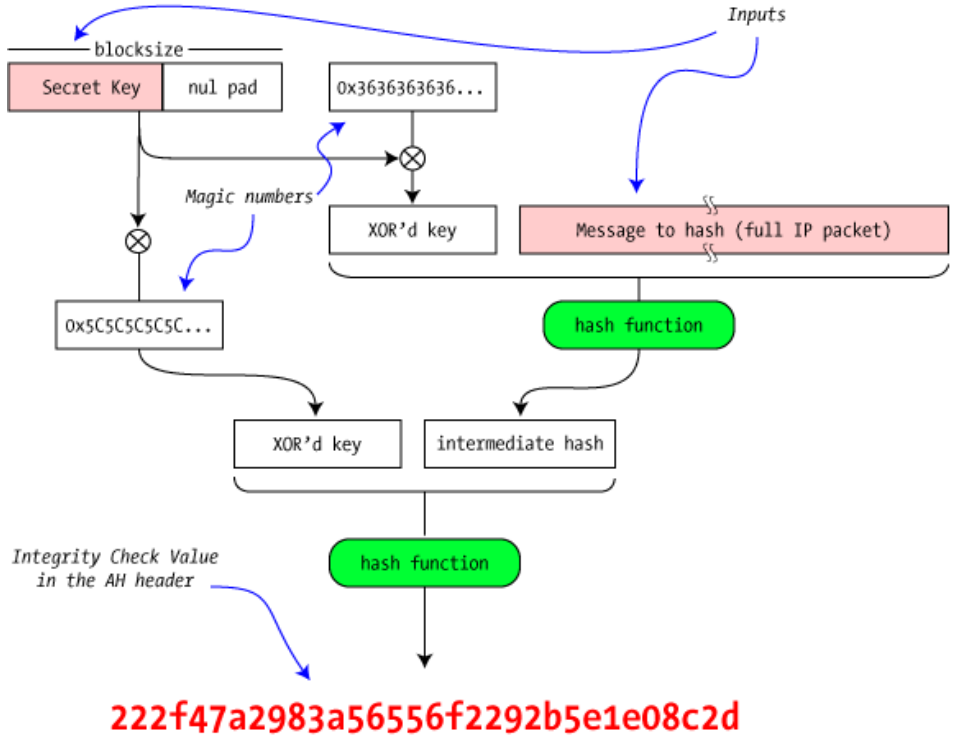
ipad = байт 0x36, B рет қайталанған

opad = байт 0x5C, B рет қайталанған

'text' ретінде көрсетілген, пайдаланушылық мәліметтерден HMAC есетеу үшін келесідей операцияларды орындау керек:

ICV = H (K XOR opad, H (K XOR ipad, text))

ICVесептеудің бұл сұлбасы мына суретте көрсетілген:



3.1-сурет – HMAC

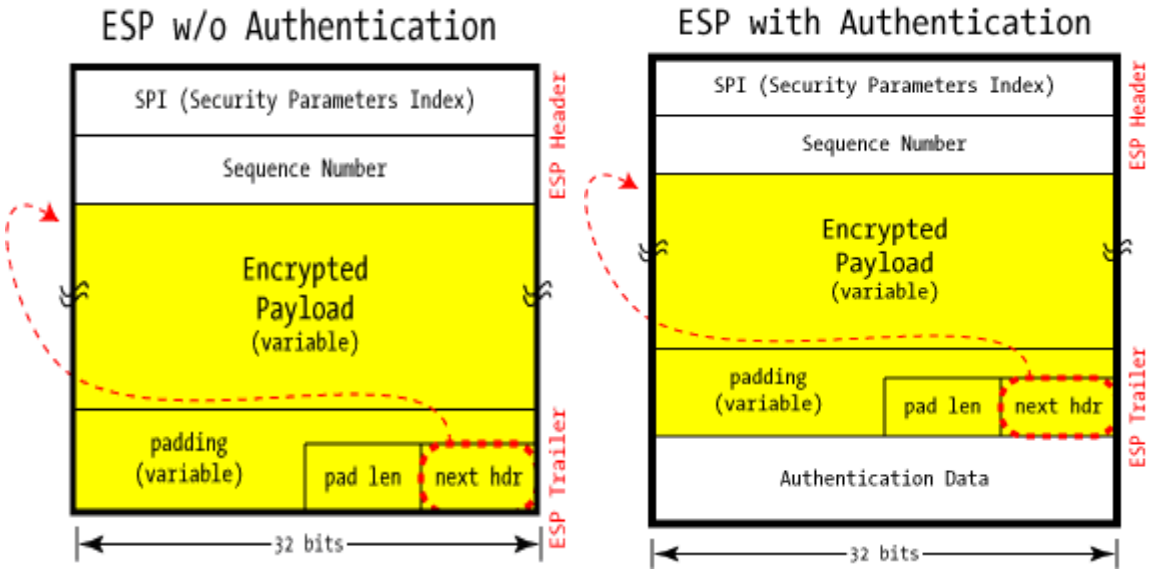
Еске салатын жағдай, IPsec белгіленген алгоритмдердің пайдалануын болжайды, тек ақпараттардың алмасуына қатысатын, олардың екі жақтан келісімдері қажет. Сондықтан сәйкестендірудің басқа қызметтері үшін мүмкіндіктер сақталады.

3.2.1 ESP хаттамасы

ESP (Encapsulating Security Payload) – жіберіліетін ақпараттардың құпиялылығын сақтау үшін шифрлеу алгоритмін пайдаланатын хаттама,

сондықтан ол күрделірек. ESP стандартты жүзеге асырылуында, мәліметтердің шифрленуі үшін DES қолданылады. Бұл алгоритмде қолданылатын құпия сөздің ұзындығы 56 бит, сондықтан ол бүгінгі стандарттар бойынша жеткілікті берік болып табылады. Осы мәселеге орай көптеген өндірушілер өздерінің имплеметацияларында 3DES-ке, ал кейбіреулері AES-ке өтті.

ESPның AH басты айырмашылығы, ESP шифрленген мәліметтерді қапшықтандырады, яғни өзіне атаулар мен аяқтағыштарды қосады. ESP негізіг қызметі рұқсат етілмеген көрілімнен трафиктің қорғалуы, сол уақытта сәйкестендіру салдарынан қорғаныс өзгерісі опционды болып табылады. Бірақ ESP тек пайдалы жүктемені және ESP атауы сәйкестендіреді, сол уақытта стандартты IP-атауда көптеген өрістерді AH сәйкестендіреді. Суретте әртүрлі опциондармен ESP-пакеттің екі пішіні көрсетілген: таритің сәйкестендірілуінсіз және сәйкестендірілуімен



3.2–– сурет - ESP

SPI және Sequense Number, nexthdr өрістері AH өрісіне ұқсас сәйкес келетін, шамаларға ие.

Encrypted Payload – жоғарғы деңгейлер хаттамасының шифрленген мәліметтері (TCP, UDPжәне т.б.)

padding – мәліметтер блогының ұзындығын түзулеу үшін қызмет ететін өріс

pad len –padding өрісінің ұзыныдығы

ESP, AH секілді, тунелльді сияқты тасымалдаушы режімде де жұмыс жасай алады.

ESP қызмет жасауының екі режімін бөлек қарастырамыз.

3.3 Қауіпсіз қауымдастық

Мәліметтердің берілісін қорғау бойынша AH және ESP хаттамалары өздерінің жұмыстарын орындау алуы үшін, IKE хаттамасы екі соңғы нүктелер арасында, IPSec стандартында «қауіпсіз қауымдастық» (Security Association, SA) деген атауға ие, логикалық байланысты орнатады. SA орнату өзара сәйкестендіруден басталады, себебі егер де барлық мәліметтер басқамен берілсе немесе басқамен қабылданса, қауіпсіздік шаралары міндетін жоғалтады. SA келесіде таңдалынатын параметрлері, AH немесе ESP екі хаттамасының қайсысы, мәліметтерді қорғау үшін, қандай қызметтер хаттаманы орындайтынын анықтайды: мысалы, тек сәйкестендірілуді немесе толықтылықты тексеру ма, немесе сонымен қатар, жалған қойылымдардан қорғаныстыма. Қауіпсіз қауымдастықтың аса маңызды параметрі криптографиялық материял болып табылады, яғни AH және ESP хаттамаларының жұмысы кезінде қолданылатын, құпия кілттер.

IPSec жүйесі қауіпсіз қауымдастықтың қолмен орнату амалын қолдануға рұқсат береді, онда әкімшілік құпия кілттерді қосқанда, қауымдастықтың келісілген параметрлерін олардың қолдауы үшін, әрбір соңғы тұйінді конфигурациялайды.

AH немесе ESP хаттамасы орнатылған SA логикалыұ байланыстың аясында жұмыс істейді, оның көмегімен таңдалынған параметрлерді пайдаланумен жіберілетін мәліметтердің қажет етілген қорғанысы жүзеге асырылады.

Қауіпсіз қауымдастықтың параметрлері қорғалған арнаның екі соңғы нүктелерін орнату керек. Сондықтан IKE хаттамасының SA орнатудың автоматты процедурасын пайдалану кезінде, арнаның іртүрлі жақтарында жұмыс жасайтындар, келісімді үдерістің жолы кезіндегі параметрлерді таңдайды, оған ұқсастары, алмасу жылдамдығының екі жақ үшін де макисмалды қолайлысын анықтайды. AH және ESP хаттамаларымен шешілетін, әрбір міндеттер үшін сәйкестендіру мен шифрлеудің бірнеше сұлбалары ұсынылады – бұл IPSec өте икемді құрал жасайды. (Байқағанымыздай, сәйкестендірілу мәселесін шешу үшін дайджест қабылдау функциясын таңдау мәліметтерді ширлеу үшін алгоримтді таңдауға еш әсер етпейді.)

IPsec стандартты нұсқасында үйлесімділікті қамтамасыз ету үшін кейбір міндетті «құрал-саймандық» жиынтықтар анықталған: көбінесе, мәліметтердің сәйкестендірілуі үшін SHA-1 немесе MD5 бір жақты шифрлеудің бір функциясы пайдаланылуы мүмкін, ал шифрлеу алгоритмінің саны міндетті түрде DES кіреді. Сонымен қатар IPSec қосатын, өнімді өндірушілер, шифрлеу мен сәйкестендірудің басқа алгоритмдерінің есебінен хаттаманы кеңейту керек, олар оны сәтті жасауда. Мысалы, IPSec көптеген жүзеге асырушылары Triple DES атақты алгоритмін, сонымен қатар салыстырмалы жаңа — Blowfish, Cast, CDMF, Idea, RC5 қолдайды.

IPSec стандарттары Internet хосттары арқылы барлық өзара әрекеттесетін трафиктердің берілісі үшін SA бір қауымдастығын шлюздерге пайлануға

мүмкіндік береді, сонымен осы мақсат үшін SA еркін санын құра алады, мысалы әрбір TCP байланысқа біреуі беріледі. SA қауіпсіз қауымдастық өзімен IPSec логикалық байланысты ұсынады, сондықтан мәліметтердің екі жақты ауысым кезінде SA екі қауымдастықты ұсынады.

3.4 Cisco Packet Tracer бағдарламасы арқылы моделді жобалау

Tracer бағдарламасы тәуелсіз визуальды интерактивті бағдарлама болып келеді және компьютерлік желіліерді жобалау үшін ең маңызды ақпарраттармен қамтамасыз ететін оқыту бағдарламасы болып табылады [15]. Студенттер мен мұғалімдер арасындағы қарым-қатынасты күшейтеді және студенттерге мәліметтерді қарапайым жолмен жеткізеді. Студент оқу және нұсқаушы презентациялар арттыру керек. Ол шынайы модельдеу бірегей комбинациясын ұсынады және визуализация, кешенді бағалау мүмкіндіктері, авторлық құқық қызметі бірнеше ынтымақтастық және бәсекелестік үшін мүмкіндіктер көрсетіледі.

Пакеттік Tracer күрделі желілерін зерттеу үшін пайдаланылуы мүмкін және зертханалық жабдықтар толықтырулар керек. Мұндай маршрутизаторлар сияқты түрлі желілік құрылғылар арасындағы, қосқыштар, сымсыз кіру нүктелері, компьютерлер, байланыс және бағдарламаларды қажет етеді. Студенттер көп оңай функционалдық түсінуге болады. Түрлі желілік құрылғылар және желілік протоколдар «Үлкен экранды» нақты желілерде орын алады.

Ең маңызды үйрету және үйренудің атрибуттардың бірі әртүрлі функцилардың қабылдануы болып табылады [15]:

- көптеген желілік протоколдар;
- бірнеше платформаларды қабылдау;
- логикалық және физикалық жұмыс жасау орны;
- шынайы уақыттағы симмуляция ;
- қолайлы CLI;
- ғаламдық дестелер;
- LAN, TCP/IP, коммутация, машрутизация және WAN протоколдары;
- қызметі жіктеу зертхана деңгейі;
- көптеген тілдерді қабылдау;
- енгізілген ақпарат;
- жаң-жақты мүмкіншілік;
- интерфейс.

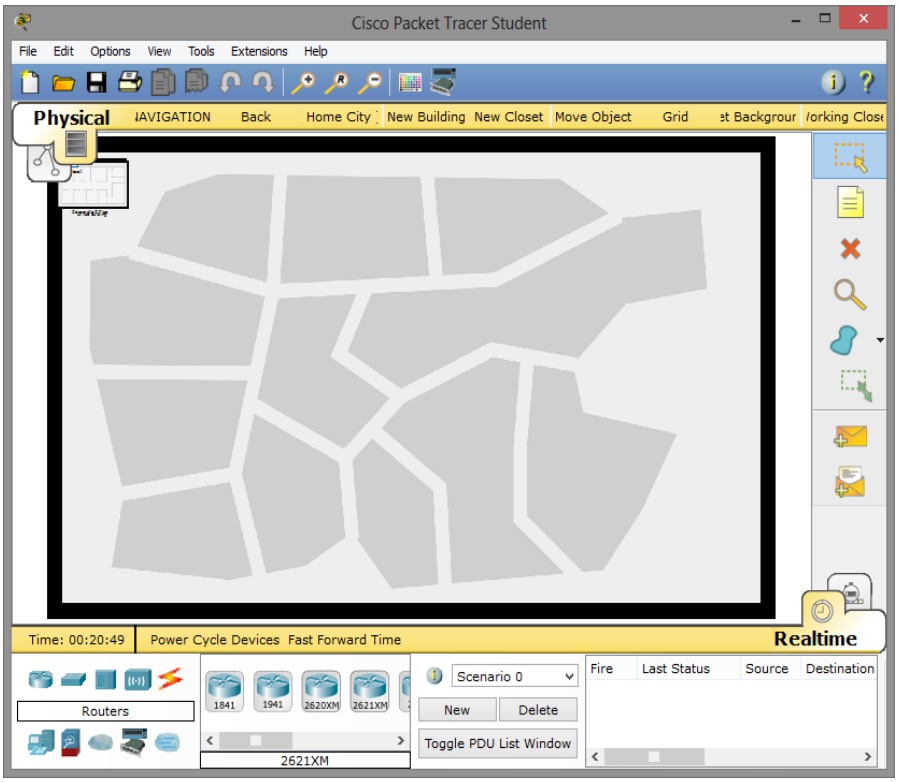
Tracer бағдарламасы келесі келесі протоколдарды қабылдайды:

- жаңа қауіпсіздік протоколдары: IPsec және GRE VPNs, IPS және IRS, AAA, сымсыз байланысты қауіпсіздік, SNMP, syslog, NTP;
- Quality of service (L2 және L3);
- L7: HTTP, DNS, TFTP, DHCP, Telnet,SSH;
- L4: TCP және UDP;

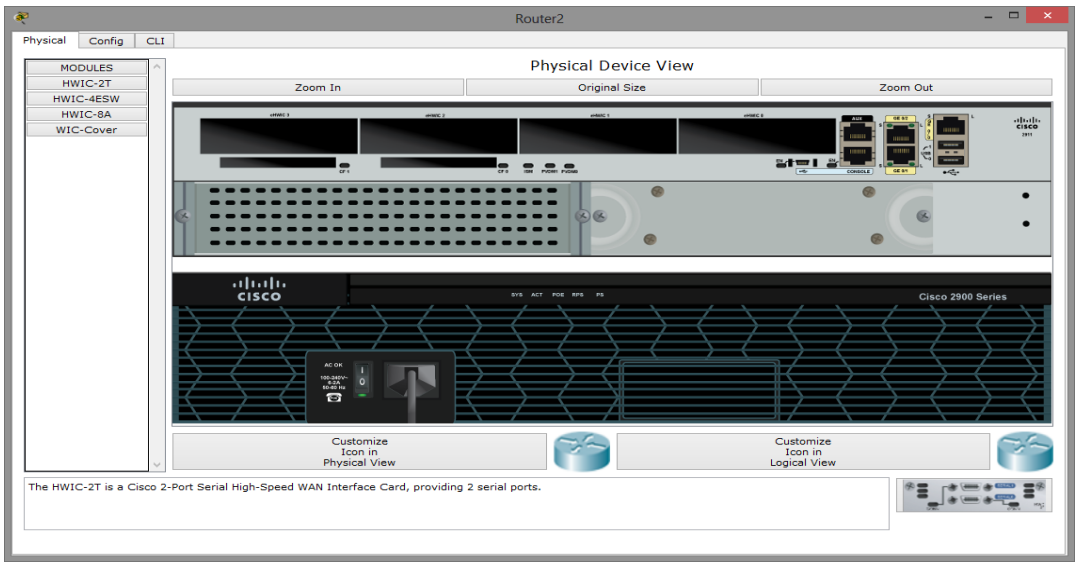
- L3: IPv4, IPv6, ICMPv4, ICVPv6, ARP, статистикалық маршрутизация RIPv1/v26 EIGRP, OSPF;

- L2/L1: Ethernet, 802.11a/b/g/n, HDLC, PPP, Frame Relay, SLARP, CDP, STP, RSTP, VTP, DTP, LACP, PAgp.

3.3 - суретте физикалық және логикалық жұмыс істеу орны көрсетілген. Физикалық және логикалық жұмыс кеңістіктері бар. «Логикалық және физикалық жұмыс кеңістіктері «желілік жабдықтардың түрлі көрсетеді және құрылғы және олардың арасындағы қарым-қатынастары көрсетілген. Түрлі физикалық жерлерде бөлінген желінің құрылғылар сияқты көрінетін (Географиялық аймақтардың, қалалар, ғимараттар, үй-жайлар, және т.б.), немесе олар логикалық топологиясы арқылы қосылған. Физикалық және логикалық топология арасындағы айырмашылықтарды зерттеп, қашан олар әр түрлі физикалық немесе логикалық құрылғылар арасында жылжыту орындары тағайындалған.

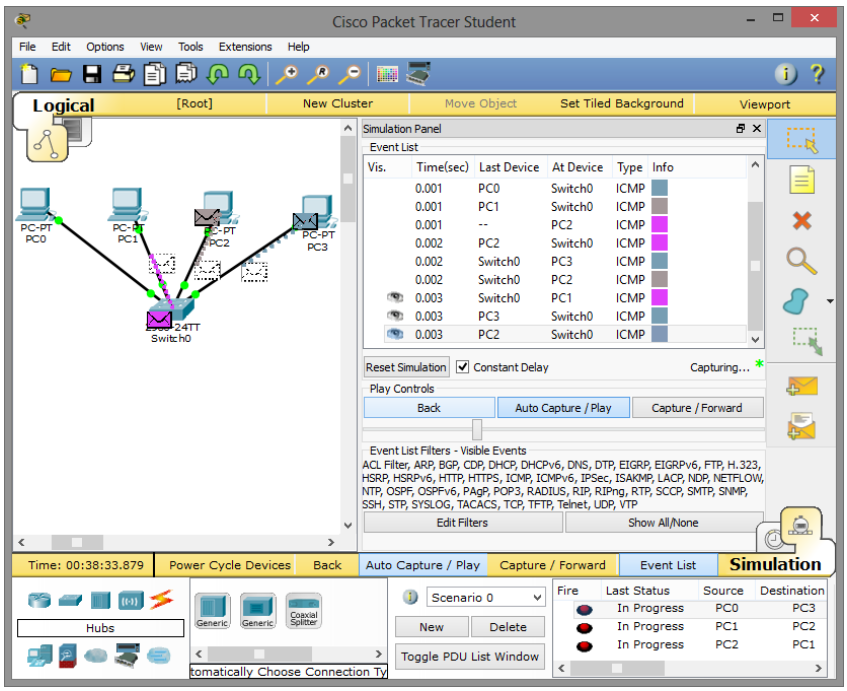


3.3-сурет – Кәсіпорын ішіндегі желінің физикалық топологиясы

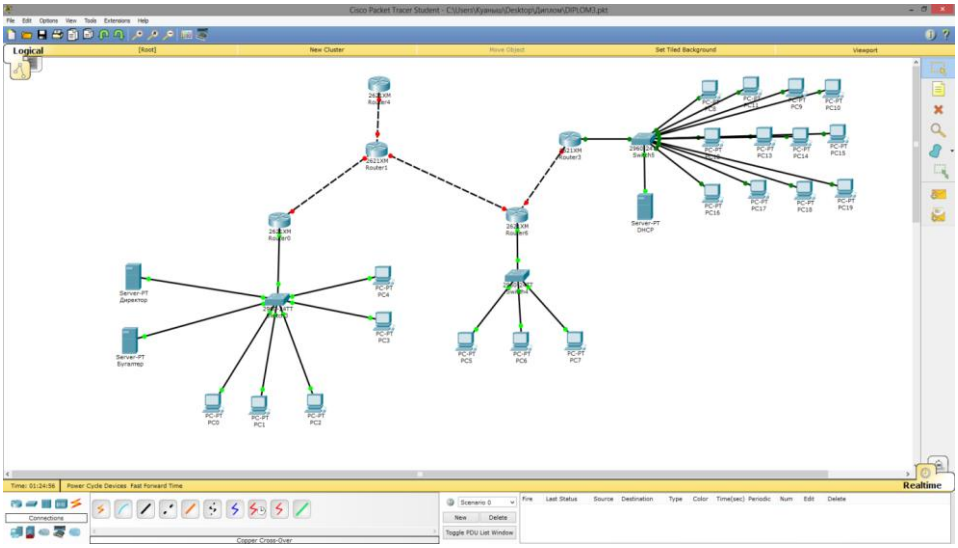


3.4-сурет – Маршрутизатордың физикалық интерфейсі

Нақты уақыттағы режим және имитациялық режим. Нақты режимі уақыт немесе модельдеу режимі желісін құру үшін пайдаланылады, құрылған топологиясы ішіндегі топологиялары және модельдеу процестері бар. Нақты уақыт режиміндегі симуляцияда желілерін нақты ортасын модельдеу және сол жылдамдықпен, ал нақты жағдайларда хаттамалар. Егер қандайда бір операция Tracer бағдарламысында нақты уақытта 30 секунд алатын болса, тура осындай уақытты алады моделденген Tracer бағдарламасында. Жаңа құрылғылар оңай нақты уақыт режиміне қосыла алады және логикалық топологияда нақты режим уақыты қала алады. Құрылғылар панелі әртүрлі құрылғылардан тұрады және бірнеше группаларға бөлінеді: маршрутизаторлар, коммутаторлар, ақырғы құрылғылар және т. б. Қосылғандарын нақтылап тестілеу үшін қарапайым пинг арқылы байқаймыз, ақырғы құрылғылардың арасындағы байланысты PDU бағдарламасы арқылы біз байланыстың қаншалықты дұрыстын байқаймыз және осы PDU бізге керекті жолмен істеуі қажет. Керекті моделдеу режимға қосылған жағдайда, Tracer бағдарламасында деректер құрылғылар арасындағы алмасуы нақты түрде байқалады. Деректерді тасымалдайтын кадрлар мен дестелер конверт ретінде көрсетіледі және құрылғылар арасында қозғалады. Tracer бағдарламасында осы конверттердің әрбір құрылғыға жеткен кездегі моменттерді қадағалайды. ISO/OSI деңгелер арасындағы қарым-қатынасты студенттер еркін бақылай алады және ақпараттың қай жерде өтпей қалғандарын көрсетеді. Фильтр арқылы тек протоколдардың қарым қатынастары бақылайтын режимге қойып қойсақ болады және қолданушыға моделдеу кезінде өте қажет болуы мүмкін.

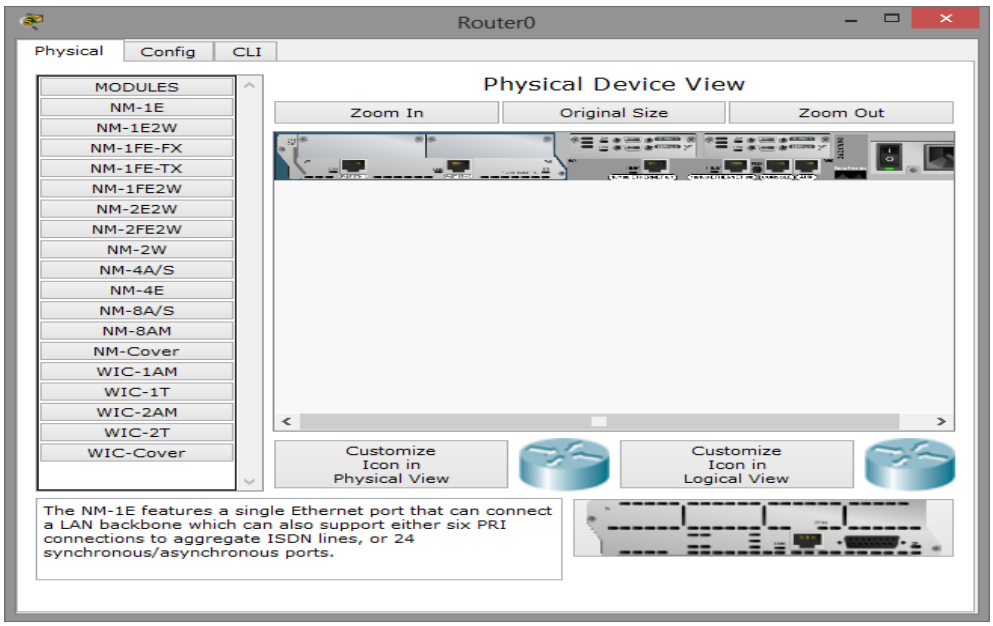


3.5-сурет – Деректердің компьютерлар арасындағы хаттар түрінде көрсетілуі

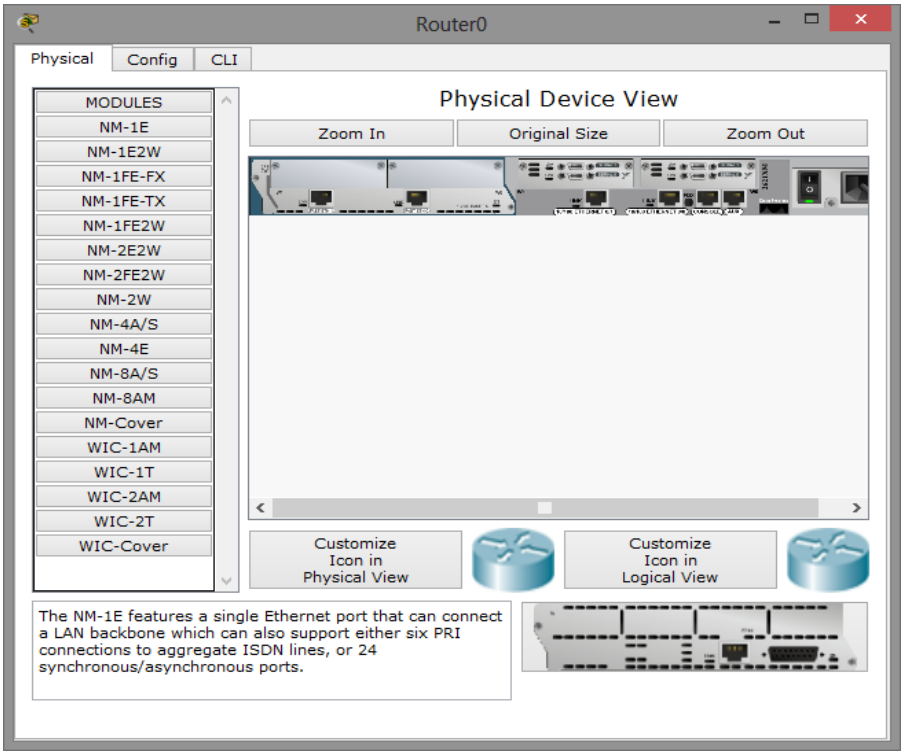


3.6-сурет – Желінің логикалық топологиясы

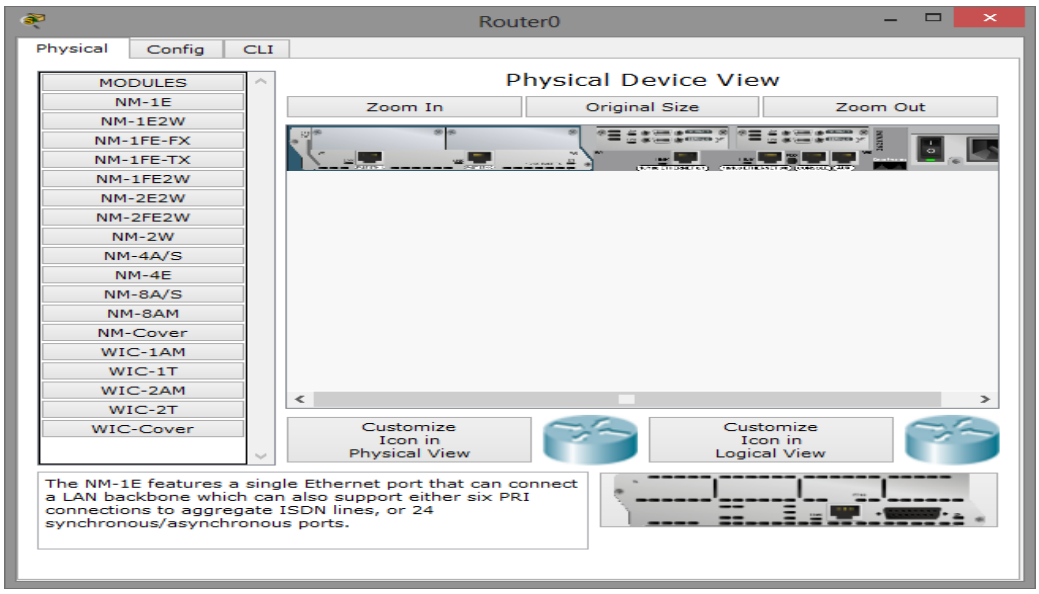
Жобалық LAN үш маршрутизаторлар тұрады: директор, бухгалтер, инженерлер, қарапайым жұмыскерлер үшін маршрутизатор үшін байланысты компьютерлер директоры және оның хатшысы арқылы басшысы 24 порттарының тұратын Cisco 2950-24 қосқыш. Жылы маршрутизаторлар үшін үш коммутаторға қосылған энергетика және климаттың жабдықтарды Департаменттер масштабталатын желілік және қызметкерлердің көп санын қосыңыз. Логикалық желі топологиясы А қосымшасынан сурет А.1 көрсетілген.



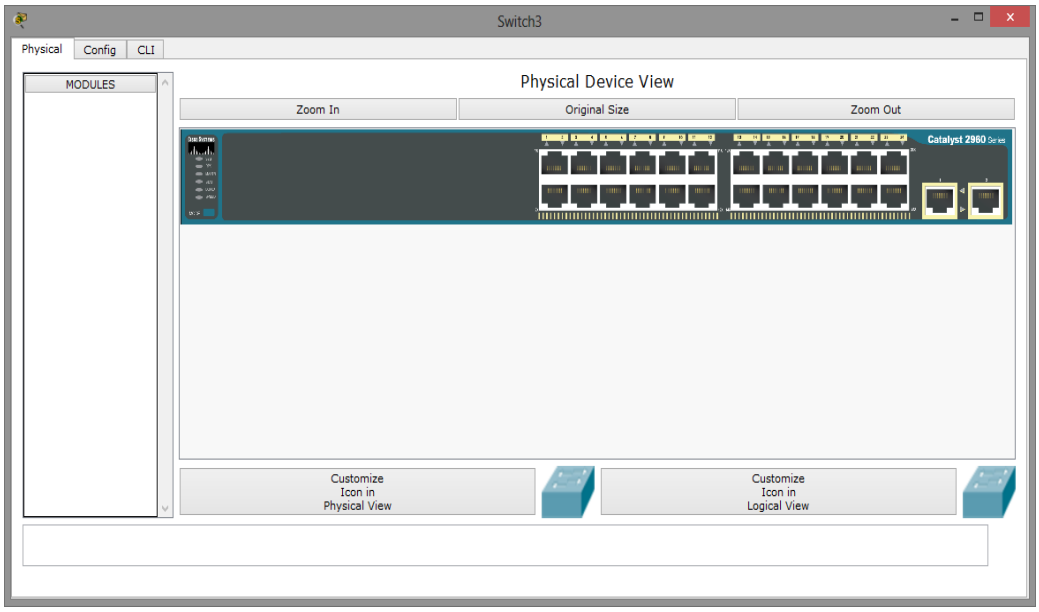
3.7-сурет – Директорлар мен бухгалтерлердегі маршрутизатордың физикалық интерфейсі



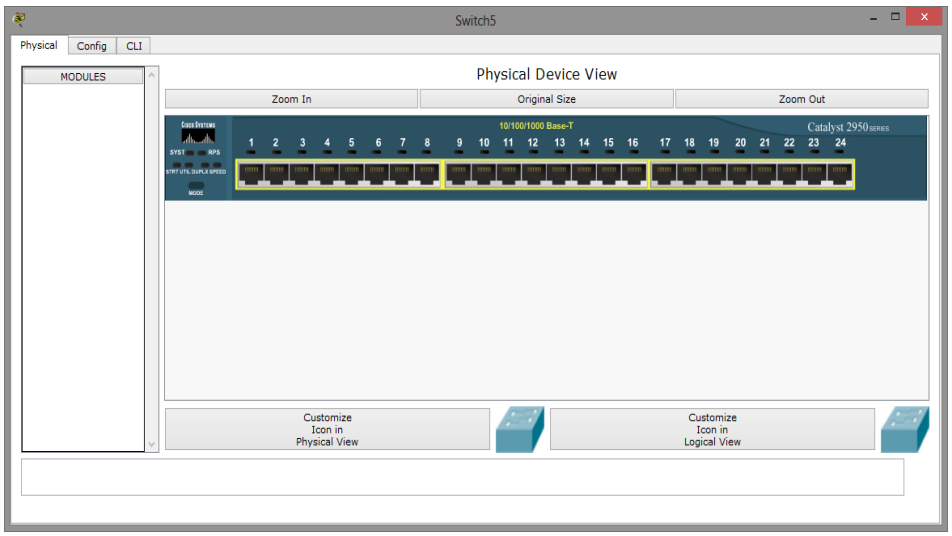
3.8-сурет – Қарапайым жұмысшылардың маршрутизаторының физикалық интерфейсі



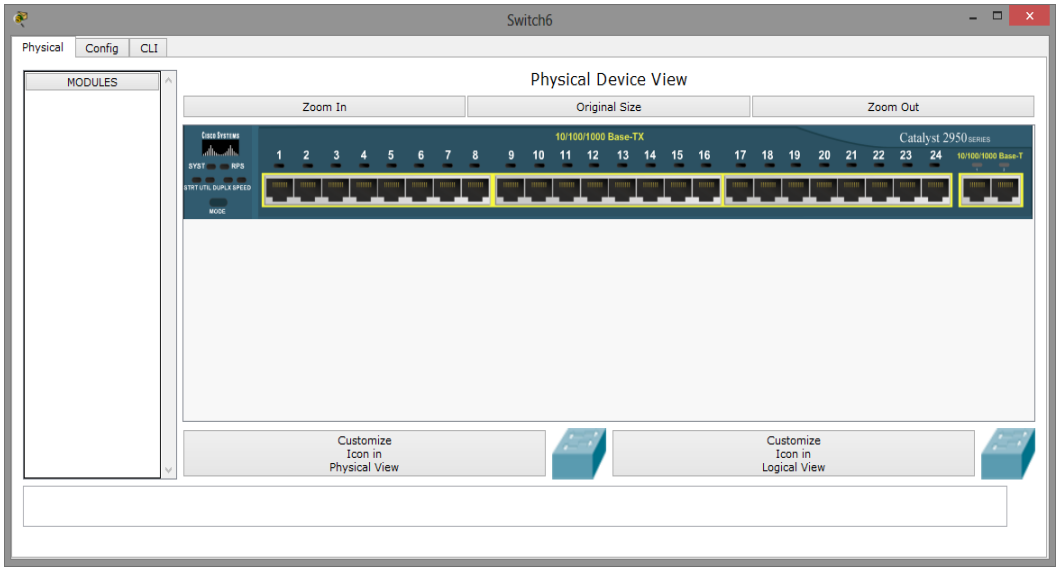
3.9-сурет – Инженерлік бөлімнің маршрутизаторының физикалық интерфейсі



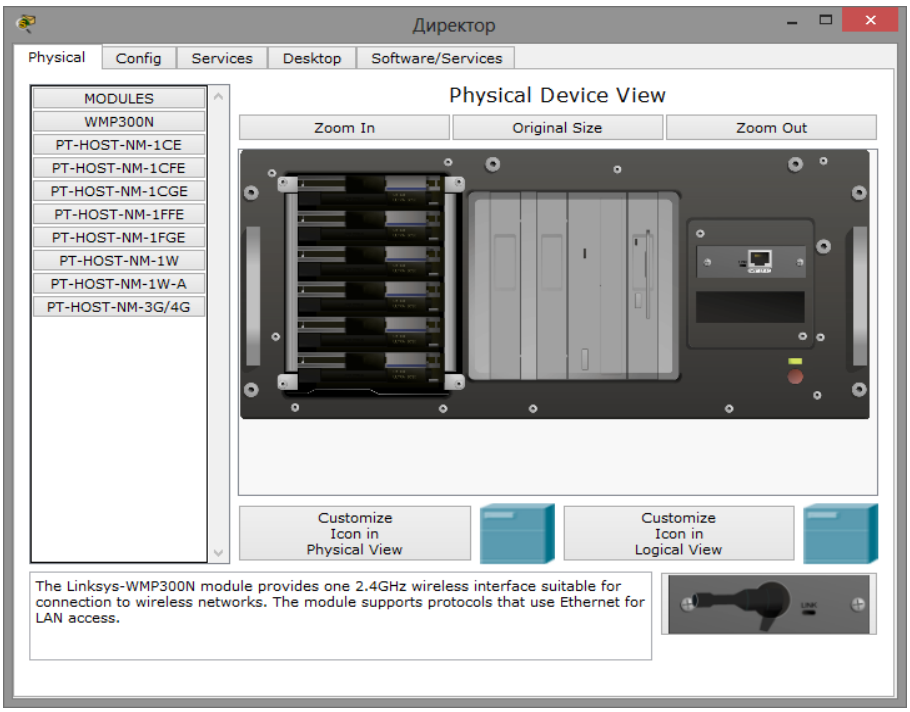
3.10-сурет – Директорлар мен бухгалтерлер бөлімі үшін қолданылатын коммутатордың физикалық интерфейсі



3.11-сурет – Қарапайым жұмысшылар бөлімі үшін қолданылатын коммутатордың физикалық интерфейсі

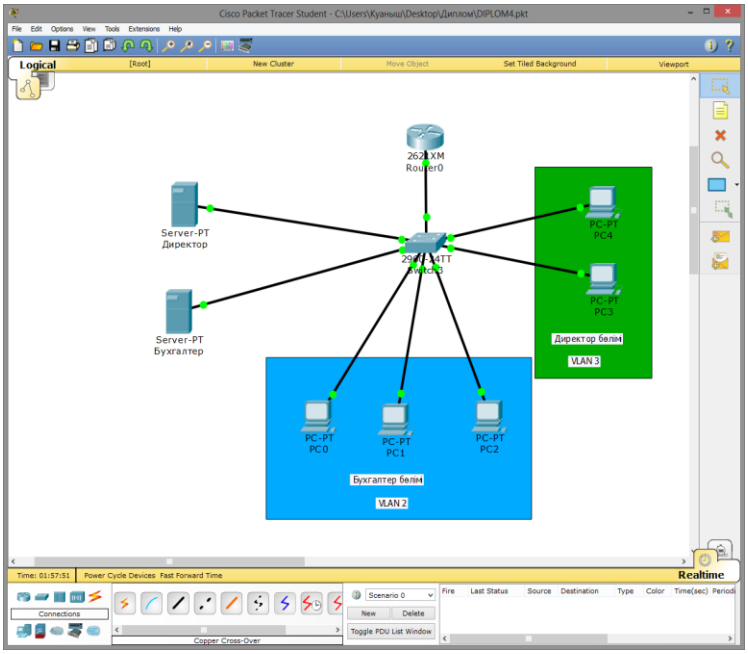


3.12 -сурет – Инженерлік бөлім үшін қолданылатын коммутатордың физикалық интерфейсі



3.13-сурет – Осы топологояда қолданылған сервердің физикалық интерфесі

Ақпараттың сақталуы маңызды болған себептерден бухгалтерлық бөлімнің деректердің бөлімінің арасындағы ешқандай ақпараттардың өтпеуін қамтамасыз ету үшін VLAN көмегімен екі сегментке бөлдім.



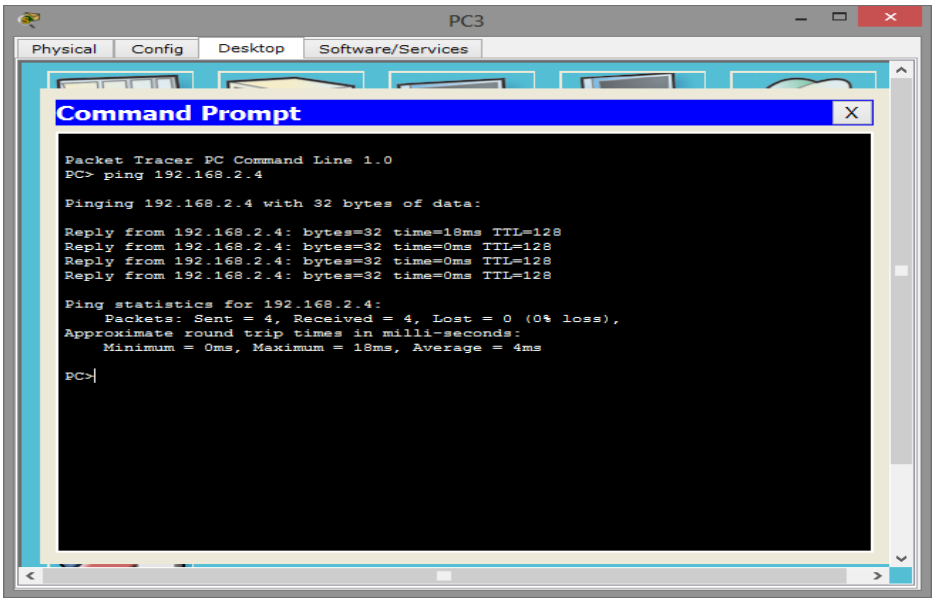
3.14-сурет – Директор мен бухгалтер бөлімдерінің екі сегментке бөлінуі

Директор мен бухгалтер бөлімінде өздерінің ақпараттарды сақтайтын қолданылатын серверлары болады және олар бір бірінің сервера қол жеткізе алмайды.

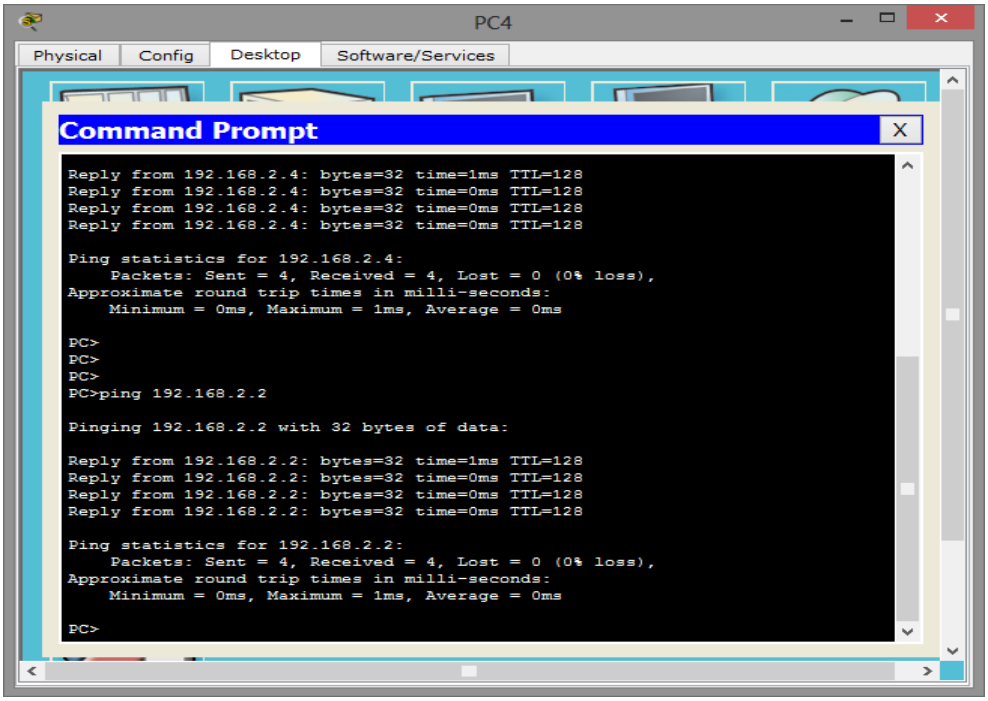
Өзара байланыс болуы үшін коммутартордағы келесі параметлерді қарастырдық:

3.15, 3.16, 3.17, 3.18 –суреттер коммутаторда орындалған командалар.

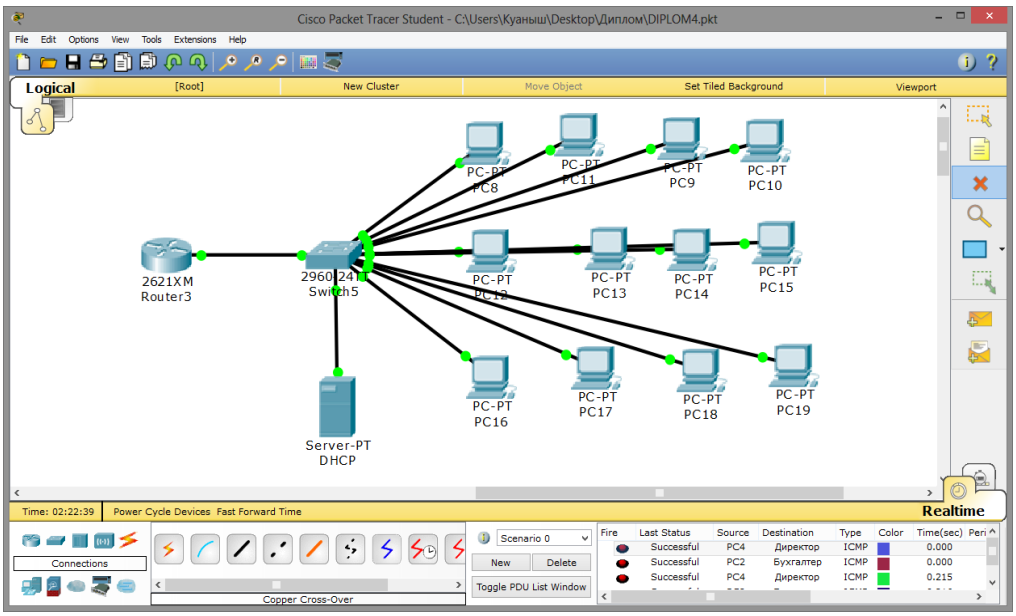
Әрбір компьютерге және серверлерге өзінің статикалық IP-адрестерін орнаттым:



3.15-сурет – PC3-тен серверга пингтау кезіндегі ақпараттың жетуі

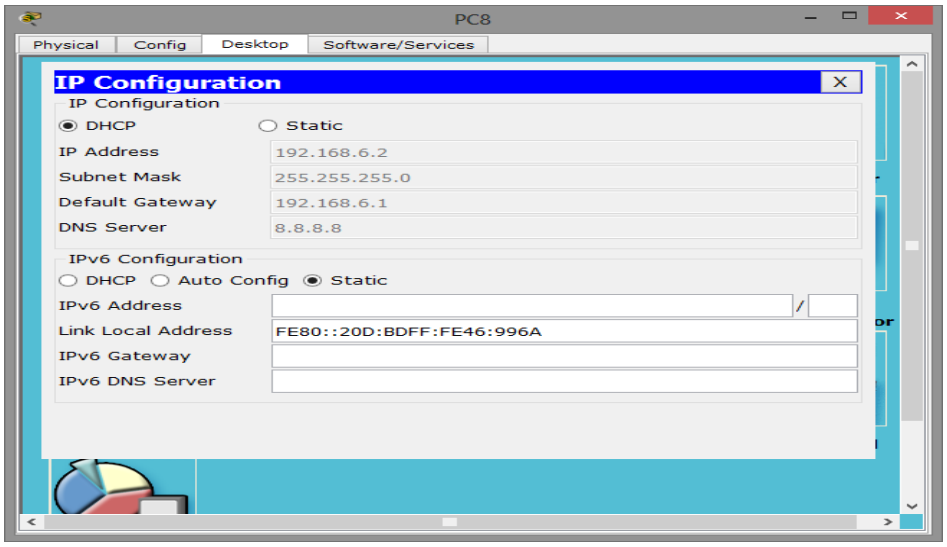


3.16-сурет – Директор бөліміндегі компьютерлардың өзара пингтелуі



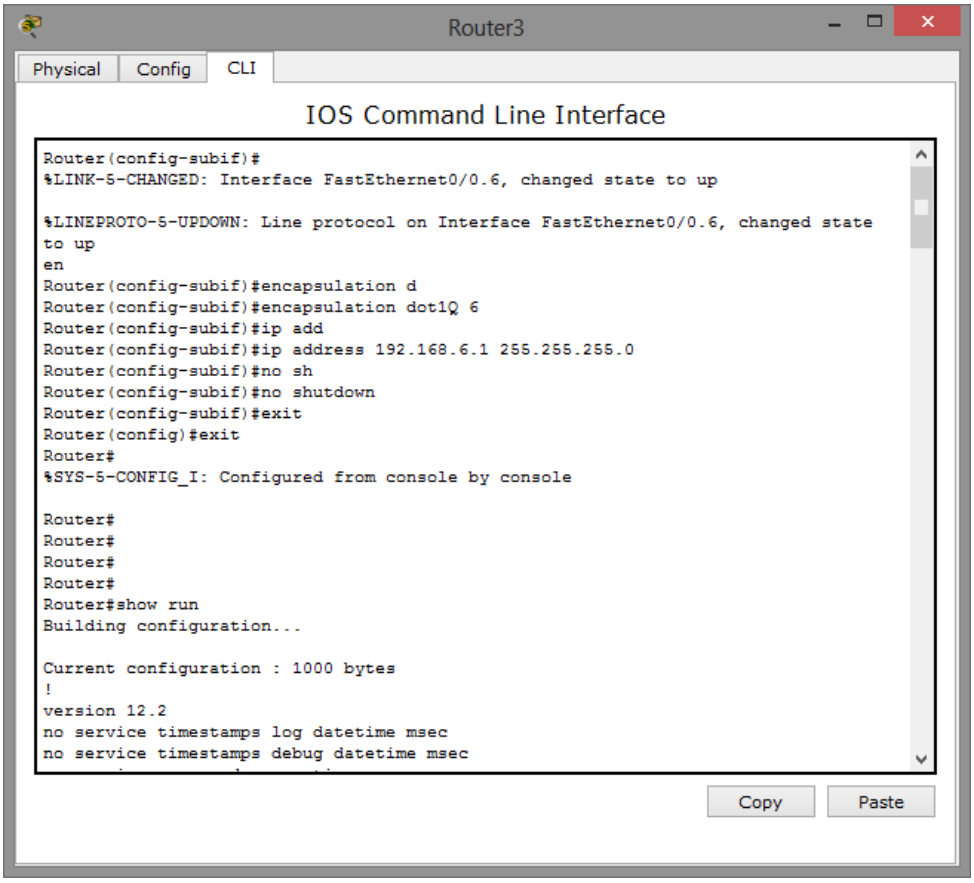
3.17-сурет – DHCP протоколы арқылы қарапайым жұмысшылар бөліміндегі желіні қолдану

IPSec протоколы арқылы біз көптеген компьютерлер үшін IP-адресті автоматты түрде бере аламыз. Сұрау қабылдау функциясы жүреді бұл кезде: коммутаторға қосылған компьютер ең алдымен коммутатор арқылы маршрутизаторға жіберіледі содан сон маршрутизатор IP адресі жоқ болған себептен оны DHCP-серверіне жібереді. DHCP-сервері оған автоматты түрде IP-адресін береді және сол компьютер қабылдайды. DHCP-сервері өте қолайлы болып келеді, егер компанияда өте көп компьютерлер болған жағдайда.

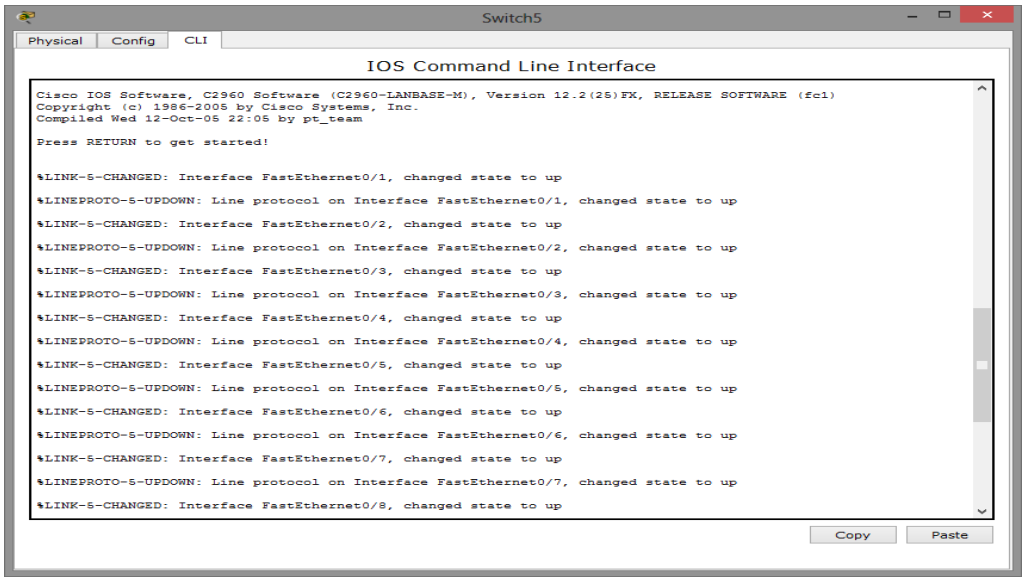


3.18-сурет – PC8 компьютері үшін DHCP-серверінен берілген IP-адрес

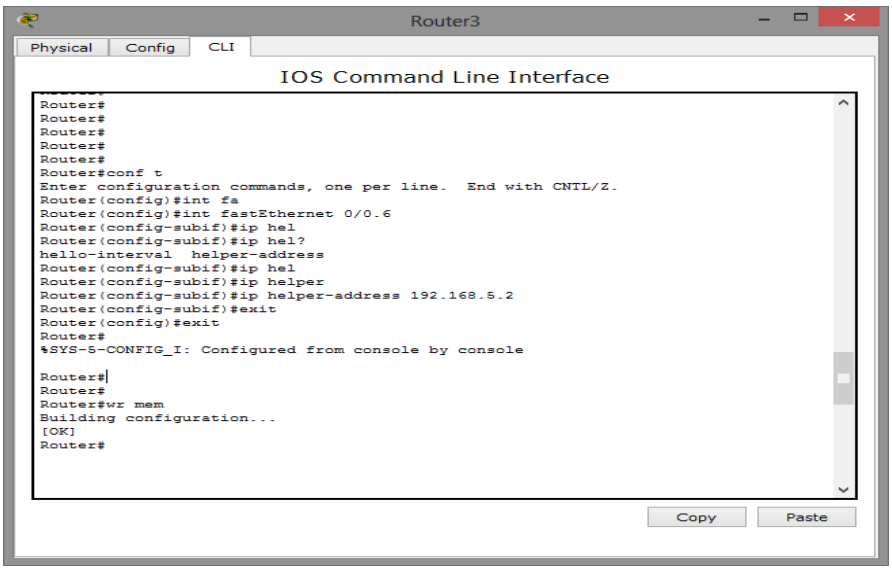
Маршрутизаторлар мен компьютер арасындағы байланыс орнату үшін әрбір VLAN үшін маршрутизатордаса б-интерфейсін жасаймыз.



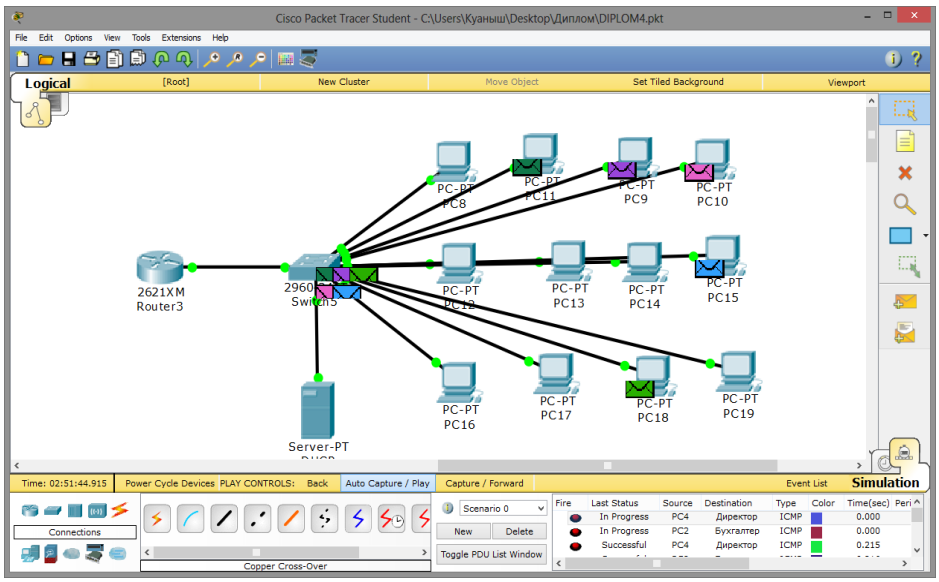
3.19-сурет – Саб-интерфейсті жасау командалары



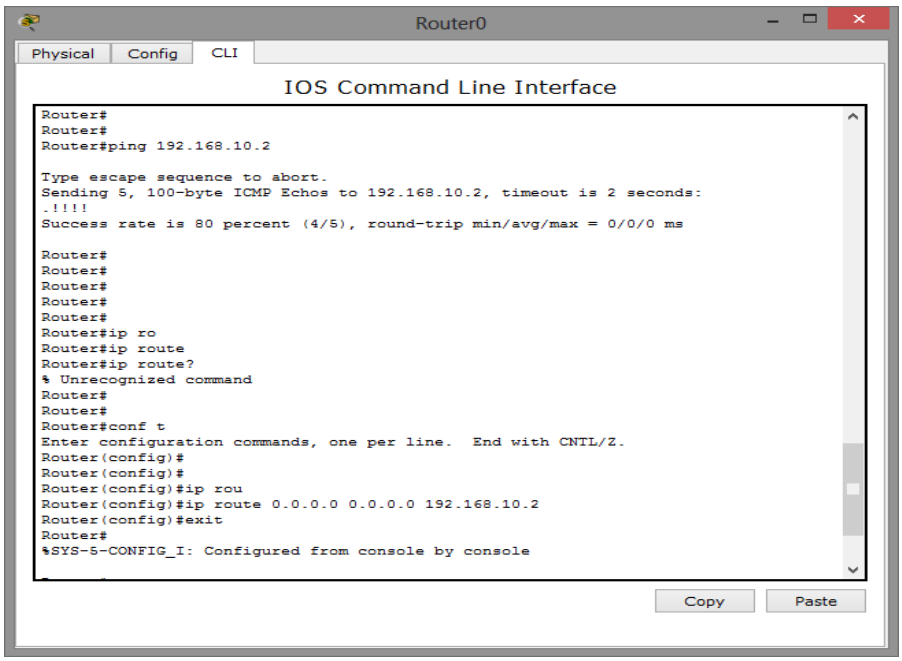
3.20 сурет – Коммутатордағы FastEthernet интерфейстерінің көтерілуі



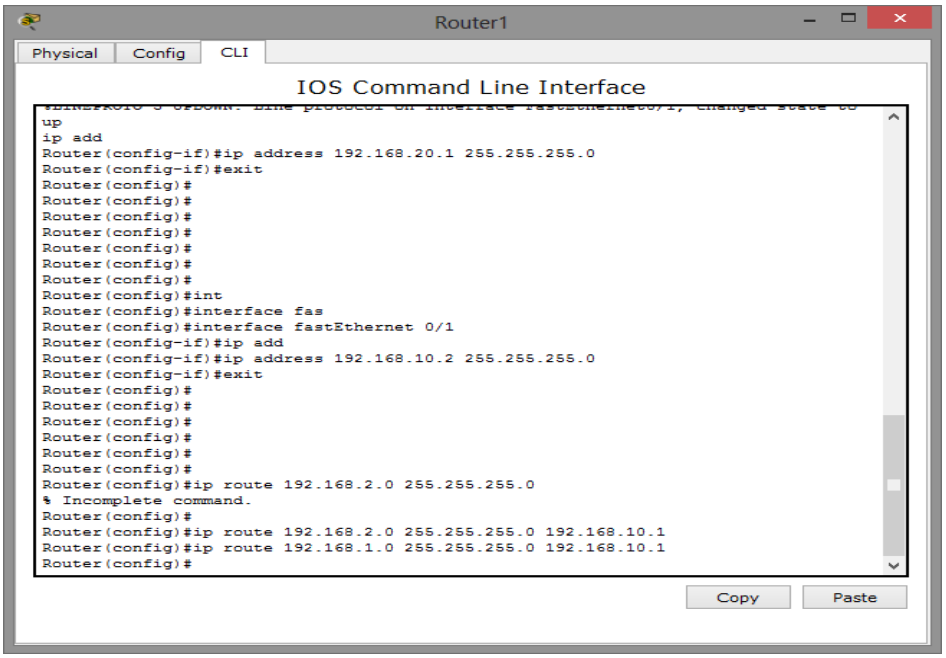
3.21 -сурет – Компьютерлердің IP-адрес сұраған кезіндегі маршрутизатордың DHCP-серверіне бағыттау үшін орындалған командалар



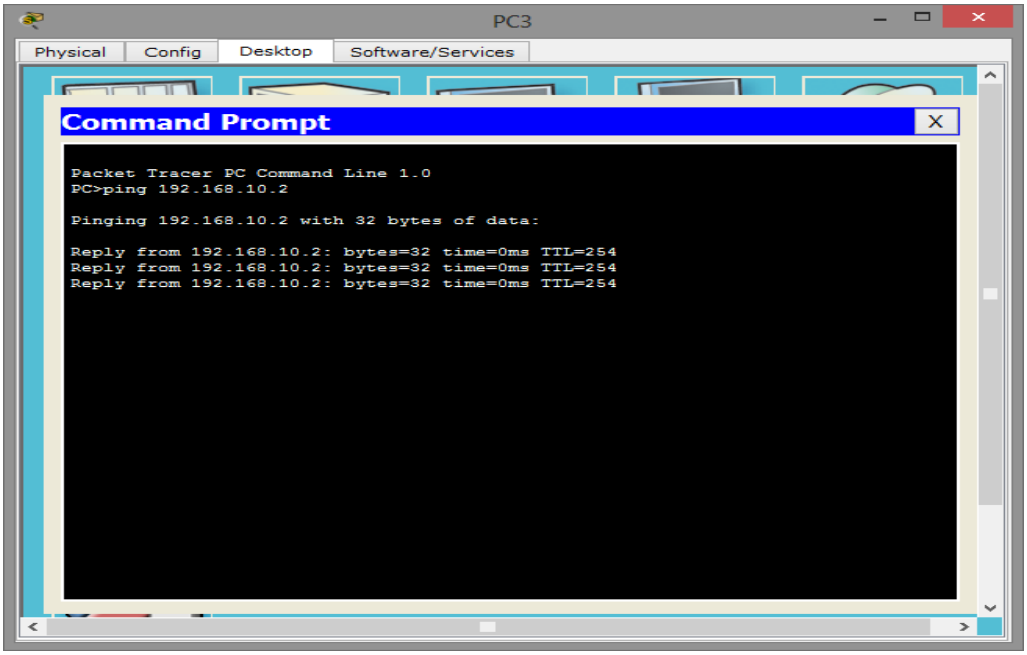
3.22 - сурет – Ақпараттың коммутаторға ешқандай қиындықсыз жетуі



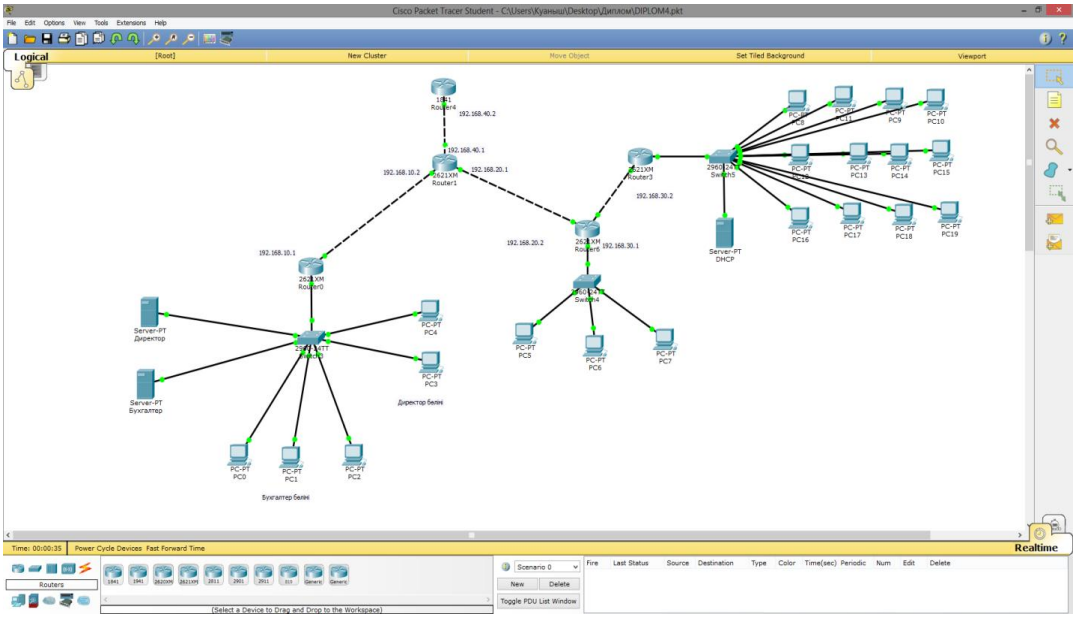
3.23-сурет – Router0 және Router1 арасындағы статикалық маршрутизация орнату үшін Router0 орындалатын командалар



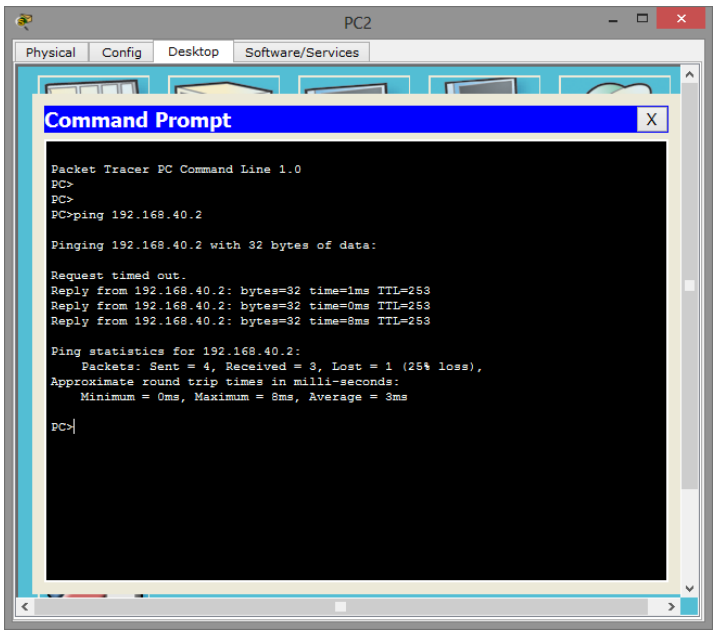
3.24-сурет – Router0 және Router1 арасындағы статикалық маршрутизация орнату үшін Router1 орындалатын командалар



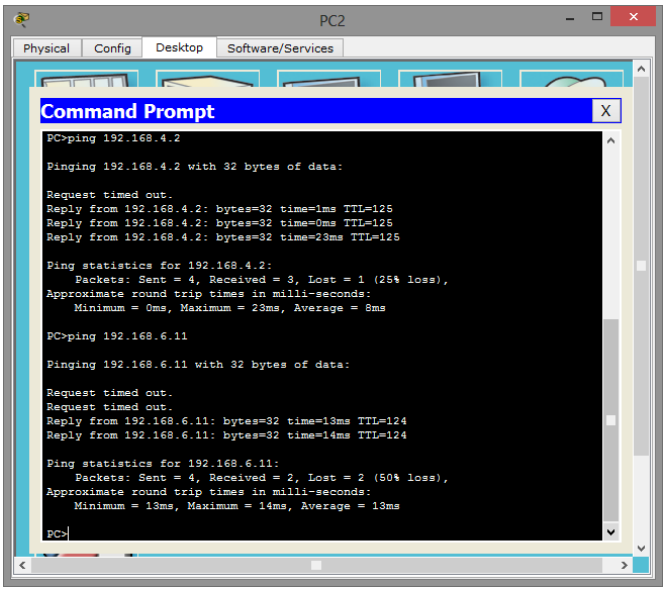
3.25-сурет – Директор бөлімшесінен Router 1 машрутизаторнының пингталуы



3.26-сурет – Желінің линктарының көтерілуі



3. 27-сурет – PC2-ден интернетті пингтау



3. 28-сурет – PC2-ден 4-ші және 5-ші сегменттердің пингталуы

Осы топологияны cisco packet tracer бағдарламасы арқылы құрып желінінің қаншалықты жұмыс істейтінің көрдік және әртүрлі сигменттерінің бір-бірімен қарым-қатынас байқадық. Бұл сигменттерде пингтер ешбір кедергісіз өтті, яғни байланыс жоғарғы деңгейде тұрғанын айқындайды және Router 4 (192.168.40.2) арқылы интернетке қол жеткізуге мүмкіндік береді.

ҚОРЫТЫНДЫ

IP-телефониясы инфроқұрылымының компоненттеріне төнген қауіпті білу керек және де олардан қорғау әдістерін, сонымен қатар ақпараттық қауіпсіздік жағы бойынша VoIP- стандарттарының мүмкіндіктерін жетік білуі керек.

IP-телефониядағы қауіпсіздік бойынша басты мәселе оның тым ашықтығында және оның компонеттеріне зиянкестердің оңай түрде шабуылдайтындығы болып табылады. Осындай шабуылдар белгісіз болғандығына қарамастан олар қажет болса іске асыруы мүмкін, себебі қарапайым IP-желілеріне түскен шабуыл сандық дыбыстар жіберетін желіге бағытталуы мүмкін. Екінші жағынан, IP-желісі мен IP-телефония желісінің ұқсастығы олардың қорғаныс жолдарының бірдей екендігін көрсетеді.

Осыған дейін айтып кеткендей, IP-телефония желісіндегі байланыс қауіпсіздігін қамтамасыз етудің екі мәселесі бар: бұл қызмет көрсету желісіне рұқсат құқығын тексеру және трафик желісі арқылы жіберіліп жатқан мәліметтердің үздіксіз қауіпсіздігі.

IP-телефонияның қауіпсіздігін қамтамасыз ету механизмінің бірі виртуалды жеке желілерді (Virtual Private Network, VPN) пайдалану.

Қорытындылай келе SoftSwitch сигналды ақпаратты өңдеуде желілер арасында арна коммутациясы мен дестелік желі арасында делдал болып, MG (MediaGateway) шлюзі шақыру қызметін өңдейді және басқарып, лектерді басқаруды, мультисервистік желілерде дауысты және деректерді тасымалдауды іске асыратындығы анықталды. SoftSwitch дегеніміз «бағдарламалық коммутатор» дегенді білдіруіне қарамастан, шын мәнінде, бұл құрылғы ешқандай коммутаторлық міндеттер орындамайды. Шақыру қызметтерін басқару типтік жағдайларда шақыру бағдарлауын, пайдаланушы аутентификациясын, байланыс пен дабылды орналастыру мен бөлуді қосады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Гольдштейн Б.С., IP- телефония. Москва, Радио и Связь, 2003. 35-78 бет.
2. Баскаков С.И. Радиотехнические цепи и сигналы. Москва, Высшая школа, 1988. 302 бет.
3. Гольдштейн Б.С., Галышко А.С., История Softswitch продолжается. Москва, Connect, 2005. 148бет.
4. Нұрманов М.Ш. Микросхемотехника негіздері. Астана, Фолиант баспасы, 2008. 244 бет.
5. Нұрманов М.Ш. ОӘК. Радиотехника негіздері. Алматы, ҚазҰТУ баспасы, 2011. 100 бет.
6. Шнепс-Шнеппе М.А., NGN: SoftSwitch умирает. Москва, Connect. Мир связи, 2003. 47-54.
7. Гольдштейн А.Б., Устройства управления мультисервисными сетями: SoftSwitch. Москва, Вестник Связи, 2002. 111бет.
8. www.softswitch.org – электронды ресурс International SoftSwitch Consortium.
9. Нефедов В.И. Основы радиоэлектроники и связи., Москва, Высш.шк., 2002. - 510.
10. www.lucent.ru – электронды ресурс.
11. www.osp.ru – электронды ресурс.
12. Олифер В.Г., Олифер Н.А., Основы компьютерных сетей, Санкт-Петербург, Питер, 2009. 520 бет.
13. Доспаев М., Жандаулетова Ф.Р. Еңбекті қорғау және өміртіршілік қауіпсіздігі негіздері. Алматы, 2008, 17,34,53 бет.
14. Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д., Охрана труда на предприятиях связи иохрана окружающей среды. Москва, Радио и связь, 2001, 161бет.
15. Скала В.И., Охрана труда и техники безопасности в практической деятельности субъектов Республики Казахстан. - Алматы, 2002, 71бет.
16. Закон РК «О труде в Республике Казахстан». - Алматы, ЛЕМ, 2004
17. Чаадаев В.К., Бизнес-процесы в компаниях связи. Эко-Тренз. Москва, 2004, 45бет.

Қ.И. СӘТБАЕВ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

дипломдық жұмысқа

Әбіләкимова Әдемі

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: IPSec протоколын қолдана отырып кәсіпорын желісін жобалау

Бұл дипломдық жұмыста, IPSec протоколын қолдана отырып кәсіпорын желісін жобалау қарастырылды. VPN технологиясын қолдана отырып, IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифры шешілген және шифрланған пакеттердің санын тексеріп, телекоммуникация жүйелерінде ақпаратты қорғау мәселелерін зерттелген.

Дипломдық жұмыс барысында бірінші бөлімде компьютерлік корпоративтік желілердің қазіргі жағдайы мен даму тенденцияларын талданды.

Екінші бөлімде IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифрланған пакеттердің санын тексерілген.

Үшінші бөлімде корпоративтік қорғалған желінің топологиясын жобалау және CiscoPacketTracer бағдарламасында жұмыс істейтін корпоративтік желі модельденген.

IPSec протоколын қолдана отырып кәсіпорын желісіндегі ақпаратты қорғауды ұйымдастыру, иілгіш бағдарламалық коммутатор Softwich-ті IP-телефония желілеріндегі қауіпсіздікті қамтамасыз ету қарастырылған. Сонымен қатар, негізгі түсініктемелер, функциялар, қолдану облысы және қолдану артықшылықтары қарастырылған.

Студент, Әбіләкимова Әдемі, дипломдық жұмысты жазу барысында жетекші нұсқаулығымен өз бетінше жұмыс істеу қабілетін көрсетті. Дипломдық жұмыс "90/А/ өте жақсы" деп бағаланды, ал Әбіләкимова Әдеміні 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша «техника және технологиялар» бакалавры академиялық дәрежесіне ұсынамын.

Ғылыми жетекші
техника ғылымдарының магистрі
ЭТжЕТ каф. аға оқытушы,
_____ Марксұлы С.
«31» 05 2023 ж.

HR Қызметі

Қ.И. СӘТБАЕВ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ
дипломдық жобаға

СЫН – ПІКІР

Әбіләкимова Әдемі

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: «IPSec протоколын қолдана отырып кәсіпорын желісін жобалау »

а) графикалық бөлімі 57 бет;
б) түсіндірме жазбасы 5 бет.

ЖҰМЫСҚА ЕСКЕРТУ ЖАСАУ

Дипломдық жобада IPSec протоколын қолдана отырып кәсіпорын желісін жобалау қарастырылған. VPN технологиясын қолдана отырып, IPSec хаттамасын пайдалану үшін Cisco Packet Tracer бағдарламасы арқылы шифры шешілген және шифрланған пакеттердің санын тексеру, телекоммуникация жүйелерінде ақпаратты қорғау мәселелерін зерттеуге арналған.

IPSec протоколын қолдана отырып кәсіпорын желісіндегі ақпаратты қорғауды ұйымдастыру иілгіш бағдарламалық коммутатор Softwich-ті IP-телефония желілеріндегі қауіпсіздікті қамтамасыз ету қарастырылған. Сонымен қатар, негізгі түсініктемелер, функциялар, қолдану облысы және қолдану артықшылықтары қарастырылды.

IPSec деректерін шифрлау үшін құпия кодты қолданатын шифрлеудің кез келген симметриялы алгоритм пайдалануы мүмкін. Шифрлау тәсілдерінің бірінде деректерді толық және сәйкестендіруді қамтамасыз ету үшін – дайджест функция (digest function) немесе хэш функция (hash function) деп аталатын бір бағытты функция (one-way function) арқылы шифрлау.

Бұл дипломдық жоба жоғарғы оқу орындарының талаптарына сай жеткілікті жоғары дәрежеде жазылған, алынған нәтижелер ақпаратты өңдеп тарату технологиялардағы ғылыми бағытқа жауап береді.

Жұмыс бағасы

Жалпы, дипломдық жұмыс «95/A/ өте жақсы» деген бағаға, ал Әбіләкимова Әдемі 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша техника және технологиялар «бакалавр» академиялық дәрежесіне ұсынылады.

Сын пікір беруші
Халықаралық ақпараттық
технологиялар университеті
т.ғ.к., кафедра меңгерушісі
__________ Бахтиярова Е.А
«02» 06 2023 ж

Подпись указанного лица удостоверяю
Менеджер по персоналу
Мусамин М.К.

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Әбіләкимова Әдемі

Тақырыбы: IPSec протоколын қолдана отырып кәсіпорын желісін жобалау

Жетекшісі: Сұңғат Марксұлы

1-ұқсастық коэффициенті (30): 11.9

2-ұқсастық коэффициенті (5): 5

Дәйексөз (35): 1.3

Әріптерді ауыстыру: 33

Аралықтар: 0

Шағын кеңістіктер: 3

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☑ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

1.06.2023 ж.
Күні

Кафедра меңгерушісі

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Әбіләкимова Әдемі

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: IPSec протоколын қолдана отырып кәсіпорын желісін жобалау

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 11.9

Коэффициент Подобия 2: 5

Микропробелы: 3

Знаки из здругих алфавитов: 33

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

1.06.2023г.
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Әбіләкимова Әдемі

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: IPSec протоколын қолдана отырып кәсіпорын желісін жобалау

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 11.9

Коэффициент Подобия 2: 5

Микропробелы: 3

Знаки из здругих алфавитов: 33

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

1.06.2023
Дата

Марксұлы С.
проверяющий эксперт