ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Автоматика және ақпараттық технологиялар институты

ӘОЖ 004.732

Қолжазба құқығында

Тузелбаев Максат Джайбергенович

Магистр академиялық дәрежесін алу үшін
МАГИСТРЛІК ДИССЕРТАЦИЯ (ЖОБА)

Диссертацияның атауы — Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу

Дайындау бағыты — 7М06201– Телекоммуникация

Ғылыми
жетекші қауымдастырылған профессор, PhD
_____ Юсупова Г.М.
«30» 05 2024ж.

Рецензент
PhD докторы,
Мирас университеті
кафедра меңгерушісі
_____ Көшкінбаев С. Ж.
«06» 06 2024ж.

Норма бақылаушы
ЭТжҒТ каф. ассистенті
_____ Кенгесбаева С.
«11» 06 2024ж.

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра
меңгерушісі Е. Таштай
ЭТжҒТ кафедрасы
тғк, қауымдастырылған
профессор
_____ Е. Таштай
«___» _____ 2024ж.

Алматы 2024

5. Jangid, M., & Trivedi, P. (2016). Improve Performance of Successive Ratio for Virtual Private Network. 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN). doi:10.1109/cicn.2016.26

магистірлік диссертация дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	**Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі**	**Ескерту**
Байланыс желілерін және олардың сенімділігін зерттеу	23.11.22 - 17.02.23	орындалды
VPN желісінің топологиясын теориялық оңтайландыру	10.02.23 - 20.05.23	орындалды
Эксперименттік бөлім	1.09.23 - 15.02.24	орындалды

Аяқталған магистрлік диссертация үшін, оған қатысты бөлімдердегі диссертациялар кеңесшілері мен норма бақылаушысының қойған **қолтаңбалары**

Бөлімдер атауы	**Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Байланыс желілерін және олардың сенімділігін зерттеу	Юсупова Гульбахар Мадреймовна, қауымдастырылған профессор, PhD	17.02.2023	
VPN желісінің топологиясын теориялық оңтайландыру	Юсупова Гульбахар Мадреймовна, қауымдастырылған профессор, PhD	20.05.2023	
Эксперименттік бөлім	Юсупова Гульбахар Мадреймовна, қауымдастырылған профессор, PhD	15.02.2024	
Норма бақылау	Сара Кенгесбаева, ЭТжҒТ каф. ассистенті	11.06.24	

Ғылыми жетекшісі _____ Юсупова Г.М.

Білім алушы тапсырманы орындауға алды _____ Тузелбаев М.Д

Күні «1» 02 2023 ж

АҢДАТПА

Бұл магистрлік диссертация желідегі өткізу қабілеттілігінің тиімділігін де, қол жетімді өткізу қабілеттілігін ескере отырып, жүктемені бөлу механизмін де ескеретін модификацияланған модельді ұсынады. Сонымен қатар, жұмыс байланысты емес түйін жұптарының санын азайту тұрғысынан оңтайландырылған IP/MPLS негізіндегі vpn графикалық модельдерін зерттеді. Бұл критерий MPLS желілеріндегі сенімділік өлшемі ретінде қарастырылуы мүмкін, әсіресе желі түйіндері арасындағы байланыс желілері істен шыққан жағдайда.

АННОТАЦИЯ

Эта магистерская диссертация предлагает модифицированную модель, которая учитывает как эффективность распределения полосы пропускания в сети, так и механизм распределения нагрузки с учетом доступной полосы пропускания. Кроме того, в работе проведено исследование графовых моделей VPN на основе IP/MPLS, оптимизированных с точки зрения минимизации числа несвязанных пар узлов. Этот критерий может рассматриваться как мера надежности в сетях MPLS, особенно в случае отказа линий связи между узлами сети.

ANNOTATION

This master's thesis proposes a modified model that takes into account both the efficiency of bandwidth allocation in the network and the load balancing mechanism taking into account the available bandwidth. In addition, the paper conducted a study of IP/MPLS-based VPN graph models optimized in terms of minimizing the number of unrelated node pairs. This criterion can be considered as a measure of reliability in MPLS networks, especially in case of failure of communication lines between network nodes.

МАЗМҰНЫ

КІРІСПЕ

Қазіргі заманғы компанияның сәтті жұмыс істеуі бизнес-процестерді қамтамасыз ететін ақпараттың қол жетімділігі мен өзектілігіне тікелей байланысты. Қызметкерлердің жұмысын тиімді ұйымдастыруға мүмкіндік беретін жаңа қызметтерді енгізу ақылды желілер мен деректерді беру жүйелеріне сүйенеді. Қазіргі заманғы желілер бейнеконференция, деректерді беру, телефония және бейне хабар тарату сияқты әртүрлі коммуникациялардың негізі болып табылады. Қазіргі уақытта деректер көбінесе MPLS VPN жапсырмаларын ауыстыру технологиясын қолдана отырып желі арқылы беріледі. Бұл технология жеткізу мекен-жайы мен желілік деңгей класын қамтитын пакет тақырыбындағы белгілерді қолдана отырып, пакеттерді жылдам ауыстыруды қамтамасыз етеді. Мұндай желідегі Трафик ресурстардың максималды жүктемесін және қызмет көрсету сапасының талаптарын ескере отырып таңдалған тізбекті желілік түйіндерді қосатын бір бағытты туннельдер арқылы жіберіледі [1].

Кез-келген желінің негізгі шарттарының бірі-оның сенімділігі, оны бағалау үшін әртүрлі критерийлер бар. Сенімділік критерийін таңдау әдетте белгілі бір желінің ерекшеліктеріне және оның мақсатына байланысты.

Бұл магистрлік жұмыста екі негізгі факторды ескере отырып, ағындық модельге негізделген модификацияланған модель ұсынылған: ВЖЖ әрбір сұранысы үшін өткізу қабілеттілігін тиімді бөлу және пайдаланылмаған өткізу қабілеттілігін ескере отырып, желі жүктемесін теңестіру. Диссертация IP/MPLS негізіндегі ВЖЖ графикалық модельдерін әзірлеуге және зерттеуге арналған, байланыссыз түйін жұптары санының оңтайлы критерийіне назар аударады. Бұл көрсеткіш MPLS желісінің сенімділігін бағалау ретінде қызмет ете алады, өйткені ол түйіндер арасындағы байланыс істен шыққан кезде маршруттың істен шығуының салдарын көрсетеді. Байланыссыз түйін жұптарының саны неғұрлым көп болса, деректер пакеттерін жылдам қайта бағыттау үшін есептеу қуатының қажеттілігі соғұрлым жоғары болады. Осы критерийді қолдана отырып, желінің маңызды нүктелерін анықтауға болады, олардың істен шығуы оның жұмысының айтарлықтай нашарлауына әкелуі мүмкін.

Есептеу техникасының дамуымен желілердің нақты өлшемдерін есептеудің нақты әдістерін қолдануға мүмкіндік туды. Бұл әдістер сенімділік функционалдығын есептеудің шамамен әдістерінің сапасын тексеру үшін қажет [2].

1 Байланыс желілерін және олардың сенімділігін зерттеу

1.1 Виртуалды жеке желілердің негізгі компоненттері

Кездейсоқ графиктер көбінесе байланыс желілері үшін модель ретінде қолданылады. Берілген диссертацияда, әсіресе байланыс желісінің моделінде кездейсоқ мультиграфтар қолданылады, яғни кез-келген шыңдар жұбы арасында бірнеше шеттер болуы мүмкін, олардың әрқайсысы белгілі бір ықтималдықпен, R ықтималдығымен пайда болады. Осылайша, біз кездейсоқ графикке негізделген желілер топологиясымен жұмыс жасаймыз. Байланыс сызықтары кездейсоқ графиктің шеттеріне, ал желі түйіндері оның шыңдарына сәйкес келеді. Маршрутизаторлар, коммутаторлар және басқа да желілік жабдықтар желі түйіндері ретінде қарастырылады.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігін бағалау үшін көптеген шаралар бар. Егер сіз кездейсоқ графиктермен байланыс желілерін модельдейтін болсаңыз, онда осы графиктің сәтсіздігін оның деректері арқылы көрсетуге болады, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. Бастапқы деректер ретінде жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдарды, желінің мақсатын, сондай-ақ желінің жұмысының орташа немесе төтенше жағдайларда көрсетілу қажеттігін қолдану керек. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет, мысалы, барлық элементтердің сенімділігінің үлестірілуін болжау қажет. Таңдалған критерий бойынша сенімділікті бағалау үшін Монте-Карло әдісі, жабын ағаштарының саны немесе бұтақтар мен шекаралар әдісі негізінде сенімділік функциясының жуықталған мәнін есептеу алгоритмдері қолайлы.

Маңызды ерекше жағдай – желінің диаметріне шектеу қою. Диаметрдің шектелуі желіде хабарламаның өмір сүру уақыты белгілі бір шектеулі беріліс санынан аспаған кезде өте маңызды.

Сенімділік критерийлері бойынша байланыс желілерінің құрылымдарын әзірлеу. Таңдалған сенімділік сипаттамасына сәйкес желілерді оңтайландыру міндеті жиі туындайды. Бұл тапсырманың сирек кездесетін жағдайлары – клиенттің қолданыстағы желісіне элемент немесе элементтер тобын қосу, бірнеше дисперсті түйіндердің бір желісіне қосылу, жаңа абоненттерді қосу және т. б. Мұндай жағдайларда желілік топологиялардың кең таралған түрлері, мысалы, тізбек (шина), цикл (сақина) және жұлдыз сияқты шешімдер жалпы түрде кездеседі. Бұл жұмыста екінші тарауда EDR критерийі бойынша осы жалпы топологияларды ерікті топологияға оңтайлы қосу туралы шешімдер ұсынылған, мұндай топологиялардағы арнайы шыңдардың оңтайлы орналасуы және осындай топологияға жиек қосу қарастырылған.

Байланыс ықтималдығының максималды критерийі - кездейсоқ график желісінің моделі ретінде пайдаланылған кезде байланыс желілерінің сенімділігінің ең зерттелген және белгілі критерийлерінің бірі. Мұндай графиктің әр шеті мен шыңына оның сенімділігін сипаттайтын белгілі бір сан берілуі мүмкін: жұмыс күйінде болу ықтималдығы. Бұл жағдайда әр шыңның әрқайсысына қандай ықтималдықпен қосылатындығын есептеу мүмкін болады. Бұл ықтималдық байланыстың жалпы терминалдық ықтималдығы деп аталады. Байланыстың екі терминалды ықтималдығын және k-терминалын есептеу міндеттері де кең таралған.

Берілген шаманың ағынын беру ықтималдығының критерийі. Берілген шама ағынының берілу ықтималдығының критерийі байланыс желілерін жобалау кезінде де маңызды. Көрсеткіш берілген уақыт ішінде бөлінген шыңдар жұбы арасында берілген ақпарат көлемін беру ықтималдығы ретінде анықталады.

EDP критерийі. Естеріңізге сала кетейік, EDP – бұл кездейсоқ графиктің шыңдарының ажыратылған жұптарының санын математикалық күту. Сенімділік өлшемі ретінде кездейсоқ EDP графигінің шыңдарының байланысқан жұптарының санын математикалық күту де қолданылады. Әлбетте, барлық шыңдарының салмағы 1 болатын N-шың графигі үшін (салмақ ұғымы төменде түсіндіріледі), EDP - n(n - 1)/2 - EDP, дегенмен, өрнектер EDP әдетте шағын және қолдануға ыңғайлы.

Алғаш рет EDP көрсеткішін есептеудің нақты әдісі А. С. Родионов пен О. К. Родионованың еңбектерінде ұсынылды. Бұл жұмыстарда әр түрлі шеттердің сенімділігі жағдайында EDP-ді дәл есептеу формулалары, сондай-ақ графиктер топологиясында ерекшеліктер болған кезде, мысалы, аспалы шың, көпір, тізбек және т. б. EDP функционалдығын есептеудің қысқартылған әдістері қарастырылды. Бұл формулалар, сондай-ақ олардың негізінде алынған кейбір жаңа формулалар осы магистрлік диссертацияда жиектердің сенімділігі бірдей болған жағдайда қолданылады. Алайда, жұмыстарда EDP критерийі бойынша желілік құрылым жүйелерін құрылымдық оңтайландыру міндеттері қарастырылмаған, EDP көпмүшелерін есептеуге арналған бағдарламалық алгоритмдер мәселелері де бұрын қарастырылмаған.

Кез-келген ұйым, мейлі ол өндірістік, сауда, қаржы компаниясы болсын, мейлі мемлекеттік мекеме болсын, міндетті түрде өз филиалдары арасында ақпарат беру мәселесімен, сондай-ақ осы ақпаратты қорғау мәселесімен бетпе-бет келеді. Әрбір фирманың жеке қол жеткізу арналарының болуы мүмкіндігі бола бермейді және мұнда VPN технологиясы көмектеседі, оның негізінде барлық бөлімшелер мен филиалдар қосылады, бұл жеткілікті икемділікті және сонымен бірге желінің жоғары қауіпсіздігін, сондай-ақ шығындарды айтарлықтай үнемдеуді қамтамасыз етеді.

Виртуалды жеке желі (Virtual Private Network) Интернет желісінде құрылады және пайдаланылады. Егер интернет арқылы байланыс кейбір кемшіліктерге ие болса, мысалы, ақпаратты көшіруден қорғау және

ақпараттың басқа арналар арқылы таралмауы үшін құпиялылық және оның шабуылға ұшырауы, VPN интернет арқылы жиналған барлық трафиктің жергілікті желі ішіндегі әдеттегі трафикті беру сияқты қорғалатынына кепілдік бере алады. Сонымен қатар, виртуалды жеке желілер жеке ғаламдық желіні сүйемелдеумен салыстырғанда айтарлықтай ақша үнемдей алады.

VPN-ді пайдалану көптеген артықшылықтарды ұсынады, олардың бірі – шығындарды төмендету. Бұл технология серверлердің, модемдердің, коммутациялық желілердің және басқа да техникалық құралдардың санын азайту арқылы қашықтағы пайдаланушыларға ішкі желілерге қол жеткізуді қамтамасыз етуге мүмкіндік береді. Сонымен қатар, виртуалды жеке желілер телефон желілері немесе әдеттегі байланыс желілері арқылы әртүрлі компаниялардағы желілік ресурстарға қашықтан қосылуға мүмкіндік береді, бұл икемділікті арттырады және қауіпсіздікті қамтамасыз етеді.

VPN технологиясының негізгі тұжырымдамасы ұсынылды және оның жалпыланған бағалауы жүргізілді. Қызмет түрін және VPN-нің әртүрлі көмек схемасын қарастыруға болады, сондай-ақ технологияның эволюциясы мен OSI моделінің деңгейіне қатынасы тұрғысынан тиісті хаттамалар тізімделіп, талданды. Бұл технологияның көмегімен барлық бөлімшелер мен филиалдар қосылып, жеткілікті икемділікке, жоғары қауіпсіздікке және шығындарды үнемдеуге қол жеткізуге болады [1].

1.2 Белгілер бойынша көп хаттамалы коммутация

MPLS хаттамасы MPLS IP туннельдері болып табылатын ВЖЖ - жылдамдығына өте жақсы бейімделген. Хаттама жұмыс күйінде болуы үшін оның MP-BGR (RFC-2858) маршруттау хаттамасын қолдауы қажет. Бұл коммутация кез-келген көлік протоколы үшін жұмыс істей алады. Желі конфигурацияланғаннан кейін, қазіргі уақытта ол арқылы бірде-бір сессия болмаса да, желі әрқашан бар. Виртуалды желіде пакет пайда болған кезде оған осы ВЖЖ шегінен шығуға мүмкіндік бермейтін белгі беріледі, MPLS хаттамасы басқа шектеулер қоймайды. Кепілдендірілген MPLS қауіпсіздік деңгейін ешқашан асыра бағалау қажет емес. «ортадағы адам» сияқты шабуылдардың өте жойқын күші бар. Бірақ ATM мүмкіндіктерін пайдалану мүмкіндігі бар, әсіресе егер бұл хаттама желіде қолданылған болса.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ осы бағанның деректері арқылы., нәтиже көрсетілуі керек

пе? желінің жұмысы орташа немесе төтенше жағдайларда. Көбінесе тапсырманы дәл шешу және таңдалған сипаттаманың мәнін табу үшін сенімділік графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдетуі керек, мысалы, р ағындардың құрылымын қамтамасыз ету үшін пакетте әрқайсысының өз ауқымы бар белгілер стегі жасалады. Стекметтердің қалыпты түрінде желі және арна деңгейлері тақырыбымен аралық орналасады. Стектегі әрбір жазба 4 октетті алады.

Сияқты технологияның негізгі плюс MPLS VPN бұл дәстүрлі маршруттау арқылы қолдау көрсетілмейтін қызметтердің жаңа түрлерін ашуға негіз болады. Бұл ұйымдар арасындағы күнделікті қатыгез бәсекелестік жағдайында, провайдерлердің алдында үнемі жаңартылып отыратын қызметтерді пайдаланушыларға ұсыну проблемасы туындаған кезде ерекше қызықты болады. басқа бәсекелестерде. Бірақ Қазақстанда бұл бізге қауіп төндірмейді, өйткені бүгінгі таңда Қазақтелеком компаниясы бүкіл ел бойынша байланыс нарығындағы монополистердің бірі болып табылады. MPLS белгілері бойынша байланыс абоненттерге ұсынылатын байланыс қызметтерінің құнын төмендетуге, сондай-ақ сапасын жақсартуға мүмкіндік береді. MPLS көптеген факторларды ескере отырып, маршруттау мүмкіндіктерін кеңейтеді. А және В хосттары MPLS технологиясын қолдайтын желі арқылы в хостына пакеттерді жібереді делік. Дәстүрлі маршруттау кезінде ең қысқа жол принципі бойынша - А хостынан да, В хостынан да пакеттер IGP құралдарымен ең қысқа ретінде таңдалған №1 жолға бағытталады. Енді желі әкімшісі желіні жүктеу статистикасын талдағаннан кейін LSR 2 маршрутизаторындағы жүктемені азайту үшін трафикті басқару ережелерін орнатуға шешім қабылдады делік. Ол үшін трафиктің бір бөлігін басқа маршруттар бойынша бағыттау керек, айталық, хосттан хостқа трафик в №2 жолға аудару. Дәстүрлі маршруттау арқылы мұндай бөлуді жүзеге асыру мүмкін болмас еді, өйткені ол екі жағдайда да бірдей пакеттің тағайындалған мекен-жайын ғана ескереді. Бірақ біздің мысалда желі ядросындағы маршрутизаторлар MPLS қолдайды, сондықтан мұндай ережелерді орындау өте қарапайым. Ол үшін LSR 1 маршрутизаторы А - дан В-ға дейінгі барлық трафикті №1 жолға, ал Б - дан В - ға №2 жолға бағыттайтындай етіп екі таңбаланған маршрутты конфигурациялау қажет. Трафикті көптеген параметрлер бойынша жіктеу және әр сыныптың трафигін таңдалған және мүмкін арнайы оңтайландырылған жолға бағыттау мүмкіндігі әкімшіге трафик ағындарын дәл басқаруға мүмкіндік береді [2].

Осылайша, маршруттар мен ережелерді дұрыс жоспарлау кезінде MPLS технологиясы желілік провайдерлерге қолданыстағы IP желілері үшін бұрын соңды болмаған трафикті бақылау деңгейін қамтамасыз етеді. Бұл желілердің тиімдірек жұмыс істеуін, қызметтердің болжамды сапасын және пайдаланушылардың өзгеретін қажеттіліктеріне бейімделуге икемділікті білдіреді. Пакеттерді жіктеу үшін MPLS жүйелерінде қолдануға болатын критерийлер жиынтығы өте кең. MPLS-тің алғашқы енгізілімдерінде осы

Критерийлердің тек бір бөлігі ғана қолданылатыны анық, ал қалғандары MPLS басқару компоненті үшін қажетті бағдарламалық жасақтама пайда болған кезде жұмысқа тартылады.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде жеке түйіндердің сенімділігі туралы болжамдар қолданылуы керек. және басқа байланыс, желінің мақсаты, сондай-ақ болжам лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін мен графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдетемін.

Егер провайдер белгілі бір қызметтердің жаңа түрін иіскейтін болса да, бұл жағдайда оған барлық MPLS - үйлесімді инфрақұрылымды ауыстырудың қажеті жоқ, тек жеке пакет санатына арнайы F-класс тағайындау үшін жауапты элементті ауыстыру жеткілікті, содан кейін оны көрсету керек.саналы түрде жасалған LSP бағыты. Мәселен, мысалы, пакеттерді тағайындау ішкі желісі мен қосымшаның түрі немесе бастапқы және тағайындалған желілер, қызмет сапасына қойылатын нақты талаптар (qos), мультикаст IP-тарату тобына жататындығы, виртуалды жеке желі идентификаторы (VPN) бойынша жіктеуге болады. Әрі қарай, желі әкімшісі LSR маршруттарын белгілі бір трафик класының нақты талаптарын қанағаттандыратындай етіп конфигурациялай алады: транзиттік түйіндердің санын азайту, берілген өткізу қабілеттілігін қамтамасыз ету, трафикті белгілі бір түйіндер арқылы бағыттау және т. б.

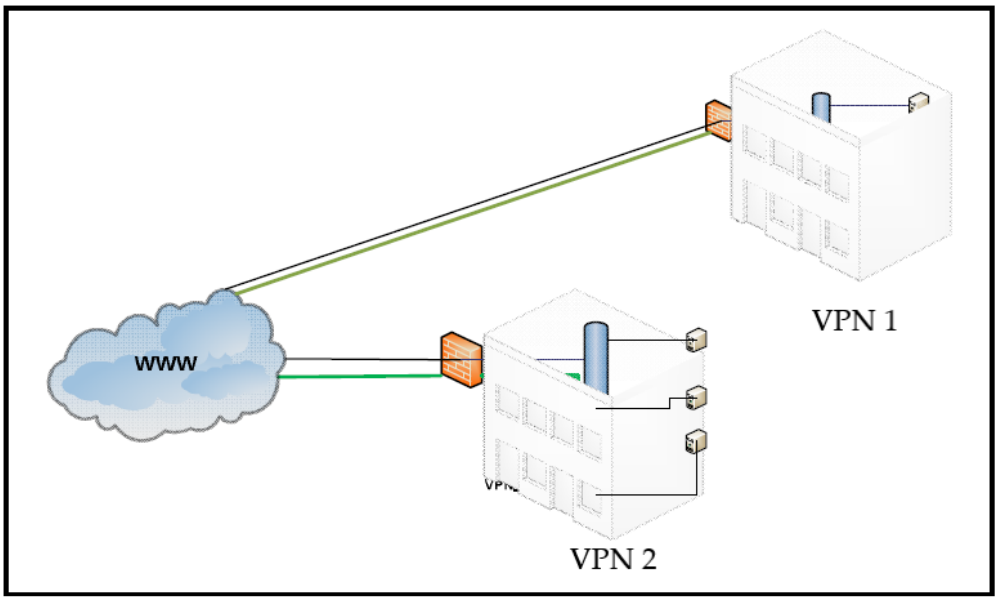
Жаңа қызметті енгізудің соңғы қадамы кіріс LSR маршрутизаторын сәйкесінше конфигурациялау болып табылады. Ол берілген сыныптың анықтамасына сәйкес келетін пакеттерді анықтап, оларды осы сыныптың трафигі үшін арнайы жасалған жолға бағыттауы керек.

1.3 VPN желісінің артықшылықтары және оның кемшіліктері

VPN (виртуалды жеке желілер) - қарапайым жеке желілермен салыстырғанда әртүрлі артықшылықтарға ие. Олардың негізгілері-икемділік, ыңғайлылық және үнемділік.

Барлығы дерлік желіге қосылады және интернет әлемдегі ең үлкен компьютерлік желі болып табылады. Интернет көптеген желілерді қамтиды. Алайда, желілер бір-бірімен қалай байланысады? Бұл мәселенің шешімдерінің бірі - виртуалды жеке желі (VPN). VPN-бұл әртүрлі желілерді байланыстыру

үшін қолданылатын желілік құрылғы немесе құрылғылар сериясы [3]. Қосылудан басқа, VPN икемділік пен қауіпсіздік сияқты артықшылықтарды арзан бағамен ұсынады. Бір жағынан, vpn икемділік, байланыс және қауіпсіздік сияқты көптеген артықшылықтарды арзан бағамен ұсынады. Екінші жағынан, осы артықшылықтарды қамтамасыз ететін есептеу ресурстары желінің жұмысына әсер етуі мүмкін. Бұл әлсіздік бізді vpn желісінің өнімділігіне әсерін зерттеуге итермеледі. 1.1 – суретте VPN арқылы қосылған екі желінің схемасы көрсетілген [4].



1.1 - сурет – VPN арқылы өзара байланысқан екі компьютерлік желі

VPN желілері кәсіпорындарға қашықтағы пайдаланушылардың ішкі желілеріне қол жеткізуін қамтамасыз ету үшін серверлердің, модемдердің, коммутациялық желілердің және басқа да техникалық құралдардың санын азайтуға мүмкіндік береді. Бұл үнемділік қашықтағы пайдаланушыларға өздерінің ішкі желілеріне қол жеткізуді қамтамасыз ету үшін қажетті инфрақұрылымды шектеуге мүмкіндік береді. Сонымен қатар, виртуалды жеке желілер пайдаланушыларға әртүрлі компаниялардағы желілік ресурстарға телефон желілері немесе әдеттегі байланыс желілері арқылы қашықтан қосылуға мүмкіндік береді.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы бағанның бас тартуын осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. Бастапқы деректер ретінде жеке түйіндер мен байланыс желілерінің үстемдігі туралы болжамдар, желінің мақсаты, сондай-ақ осы бағанның деректері туралы болжам қолданылуы

керек. Нәтижелер желінің жұмысы орташа немесе төтенше жағдайларда көрсетілуі керек. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамаларының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет, мысалы, Р болжамы бойынша.

VPN технологиясының негізгі тұжырымдамасы ұсынылды және оның жалпыланған бағалауы жүргізілді. Қызмет түрін және VPN-нің әртүрлі көмек схемасын қарастыруға болады, сондай-ақ технологияның эволюциясы мен OSI моделінің деңгейіне қатынасы тұрғысынан тиісті хаттамалар тізімделіп, талданды.

Содан кейін QoS қамтамасыз етудің арналық және ағындық модельдері қарастырылады. Арна моделін пайдалану кезінде арнайы желі қызметі ыңғайлы және бұл үшін VPN соңғы нүктелерінің әр жұбы арасындағы трафиктің толық матрицасын білу қажет. Әрбір осындай жұп үшін провайдер желіде кепілдендірілген өткізу қабілеттілігі бар жеке маршрутты ұйымдастырады. Ағындық модель үшін элементтері трафиктің максималды жылдамдығының мәндері болып табылатын екі векторды орнату жеткілікті, оны соңғы нүкте барлық басқа соңғы нүктелерге жібере алады және барлық басқа соңғы нүктелерден алады. Провайдер соңғы нүктелердің байланысын жүзеге асыруы керек(мысалы, ағаш түрінде) және берілген векторларға сәйкес келетін кез-келген соңғы нүкте трафигінің берілуіне кепілдік беру үшін қажетті өткізу қабілеттілігін бөлектеуі керек.

Бірінші тарауда ағындық модельдің арнадан артықшылығы көрсетілген, ағындық модельдердің жіктелуі келтірілген және ағындық модель негізінде VPN оңтайлы топологиясын анықтау мәселелері бойынша теориялық жұмыстарға қысқаша шолу берілген. Сондай-ақ, ағаш ағындық моделіне негізделген ең көп таралған және оңай жүзеге асырылатын VPN топологиясы VPN желілік байланыстарының істен шығуына ең осал болып табылатыны көрсетілген. Содан кейін әдебиетте ұсынылған VPN буындарының жалғыз істен шығуынан қорғау стратегиялары талданды-сілтемені қорғау стратегиясы және жолды қорғау стратегиясы, олардың салыстырмалы бағасы берілді және VPN ақауларға төзімділігін қамтамасыз ету міндетінің жалпыланған тұжырымы мыналар туралы ақпаратты қамтиды: VPN технологиясын қолдана отырып, корпоративтік банк желілерін құру және практикалық іске асырудың негізгі принциптері.Қорғалатын аумақтық-бөлінген корпоративтік желіні құру шеңберінде іске асырылатын банк жүйелерінің негізгі функциялары бөлінді: күнделікті банкішілік операцияларды автоматтандыру; есеп жүргізу және жиынтық есептер жасау; филиалдармен және өзге де бөлімшелермен байланыс; банктің барлық қызметін талдаумен автоматтандырылған өзара іс-қимыл жасау және осы жағдайда оңтайлы шешімдерді таңдау; бөлшек операцияларды автоматтандыру; банкоматтар мен кредиттік карточкаларды ауыстыру; банкаралық жарыстарды жүргізу банктің бағалы қағаздар нарығындағы жұмысын автоматтандыру.

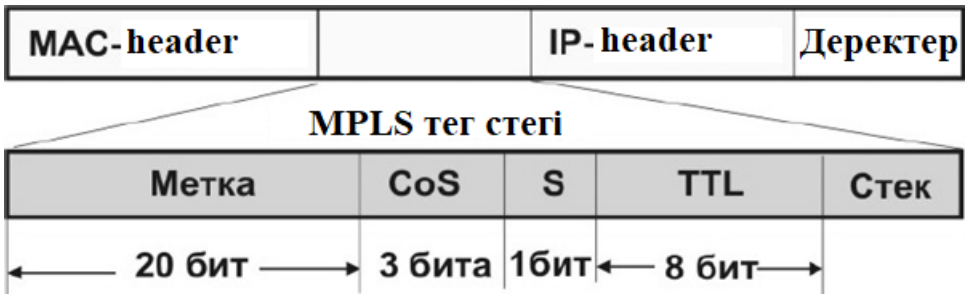
Бұл ретте Банк желісінің негізгі мақсаты филиалдар мен Орталық кеңсе арасындағы үздіксіз байланысты қамтамасыз ету, клиенттердің банк жүйелеріне қол жеткізуін қамтамасыз ету, қосымшалардың штаттық жұмысын қамтамасыз ету, пайдаланушыларға берілген сервистерді ұсыну, деректерді қорғауды қамтамасыз ету болып табылады.

Деректерді қорғау мәселелері, сенімділік пен өнімділіктің болмауы және ашық стандарттардың болмауы виртуалды жеке желілердің кең таралуын қиындатады.Қорғау көптеген интернет технологиялары үшін деректерді беру кезінде қауіпсіздік мәселелері маңызды болып табылады. Виртуалды жеке желілер де ерекшелік емес. Олар үшін басты проблемалар пайдаланушыларды парольдер арқылы аутентификациялау және шифрланған VPN арнасын (туннель) қорғау болып табылады. Сонымен қатар, желі әкімшілері пайдаланушыларға виртуалды жеке желілерге кіруге көмектесетін әдістерді мұқият таңдауы керек.

1.4 Бекітілген ұзындық идентификаторы

Белгі-FEC жіберудің эквиваленттік класын анықтайтын тұрақты ұзындық идентификаторы. Белгілер жергілікті мәнге ие. Затбелгі пакеттерді бір маршрутизатордан екіншісіне жіберу үшін қолданылады, ол кіріс болған жерде ол жолдың келесі бөлігінде жергілікті мәні бар Шығыс затбелгіге ауыстырылады. Жапсырма кез-келген пакеттің құрамында беріледі, ал оның пакеттегі орны қолданылатын арна деңгейінің технологиясына байланысты.

MPLS сияқты протокол белгілердің бірнеше түрін қолдайды: бірінші белгі 4 байтты тор болуы мүмкін, ол арна мен желі деңгейлерінің тақырып аралығы арқылы орнатылады. Ол кезде протоколға тәуелсіз болғандықтан, ол желілік деңгейдегі Протокол пакеттерін инкапсуляциялау үшін қолданылады. Екінші белгі виртуалды арна мен виртуалды жол идентификаторларының белгісі болды (VCI / VRI) немесе оны қалай атайды арна деңгейінің қосылым идентификаторының белгісі (DLCI) [2].



1.2- сурет – Тегтің өлшемі

Тегтің өлшемі-4 байт. Тегтің идентификаторы алғашқы 20 битті алады.IP-телефония сапасы 2-3 деңгей бойынша бағаланады, ал бір немесе

басқа IP–телефония провайдері екінші деңгей бойынша жұмыс істейді деп сенімді түрде айтуға болады, өйткені интернет желісіндегі кідірістер өзгереді. Бірақ мен арнайы арналарда жұмыс істейтін IP–телефония провайдерлері 1-2 деңгейлерге дәл сәйкес келеді деп айта аламын. Әрі қарай, дауыстық сигналды кодтау немесе оны декодтау кезінде кідірістерді ескеру қажет.

IP телефониясын пайдаланудың орташа жалпы кідірістері әдетте 160-260 мс аралығында болады. Желіде пакеттің кешігуі жалпы уақытқа байланысты. Пакеттік коммутацияланған желілердегі кідірістер нақты уақыттағы сөйлеу трафигінің берілу сапасына ғана емес, сонымен қатар бұл кідірістер дауыстық шлюздердің коммутацияланатын телефон желілерінің жабдықтарымен түйіскен жеріндегі T1/E1 сандық трактілерінде телефон дабылының дұрыс жұмыс істе аумағын бұзуы мүмкін екенін атап өтуге болмайды.

Ағаш тәрізді қасиет келесіге дейін төмендейді: егер бір LSR-де бірнеше пакет ағындары біріктірілсе, онда бұл LSR сол ағындармен байланысты белгілерді алмастырмайды, бірақ оларды жаңа жапсырманың үстіне қою арқылы қалдырады FEC біріктіру нәтижесінде пайда болатын біріктірілген пакет ағынына сәйкес келеді. Ағаш бірнеше рет тармақталғандықтан, тамырға жақын басқа LSR-де бірнеше біріктірілген ағындардың бірігуі орын алады және стекте тағы бір белгі пайда болады.

Пакеттердің жоғалуы. IP-телефониядағы жоғалған пакеттер сөйлеуді бұзады және тембрдің бұрмалануын тудырады. Қолданыстағы IP желілерінде барлық дауыстық кадрлар деректер ретінде өңделеді. Ең жоғары жүктемелер мен шамадан тыс жүктемелер кезінде дауыстық кадрлар кадрлар сияқты жойылады. Дегенмен, кадрлар уақытпен байланысты емес және жойылған пакеттерді қайталау арқылы сәтті беруге болады. Дауыстық пакеттердің жоғалуы, өз кезегінде, осылайша толтырыла алмайды және нәтижесінде ақпарат Толық берілмейді. Пакеттердің 6% - на дейін жоғалту байқалмайды, ал одан жоғары:

11-16% - қолайсыз. Сонымен қатар, бұл шамалар қысу/декомпрессия алгоритмдеріне байланысты.

Маршрутизатор интерфейстерінің біріне түсетін пакетті қайта бағыттау үшін екі процедураны орындау қажет:

- маршруттаудың келесі қадамын анықтау қажет.

- жапсырмалар стегі үшін қандай операция қажет екенін білу керек. Бұл стектен белгіні алу, стектегі белгіні ауыстыру операциясы болуы мүмкін.

Жапсырмалар стегінен соңғы белгі жойылғаннан кейін, пакеттерді одан әрі өңдеу желі деңгейінің тақырыбы негізінде жүзеге асырылуы керек. Үшінші деңгейдегі хаттаманы айқындау соңғы белгі мен тақырыптың өзі негізінде жүргізіледі. Осылайша, бірінші стекке енгізілген белгі бірегей болуы керек. Сонымен қатар, беру процесінде оны ауыстыратын белгіге бірдей талаптар қойылады. Әйтпесе, Шығыс ler осы пакетте қолданылатын желілік деңгей протоколын анықтай алмайды.

Белгілерді жасау үшін әртүрлі әдістер қолданылады:
- топология негізінде құру әдісі.
- сұраныстар негізінде құру әдісі.
- трафик негізінде құру әдісі.

1.5 Тегті жіберу хаттамасы

LSR жолын әртүрлі жапсырмаларды жіберу хаттамалары арқылы жасауға болады, бұл жағдайда MPLS технологиясы ешқандай шектеулер қоймайды.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Жапсырмаларды жіберу протоколы-бұл бір LSR басқаларды өзі құрған байланыстар туралы, сондай-ақ SR мүмкіндіктері туралы ақпарат алмасу үшін қолданылатын барлық келісімдер туралы хабардар ететін процедуралар мен хабарламалар жиынтығы. Оларға толығырақ тоқталайық.

LSR протоколы, ең алдымен, маршруттау ағаштарын қайталауға және оларды белгілерге негізделген маршруттау ағаштарына айналдыруға арналған. OSPF, BGR және IS-IS хаттамалары кез келген көзден адресатқа ең қысқа жолды таңдау ағашын (SPF) есептейді және таратады. LSR есептелген маршруттау ағашын көшіреді және ағаштағы әрбір арна үшін белгіні бөлектейді. Ағаштың бұтақтары түйісетін нүктелерінде белгілер біріктіріледі.

Маршруттық кестелер ең қысқа жолдар ағашының негізінде құрылады. Бұл кестелерде тағайындалған мекен-жайлардың реттелген жиынтығы және жақын көршілер туралы ақпарат бар.

LSR жолының белгілері бойынша коммутацияланатын жолды қалыптастыру кезінде, ең алдымен, хаттамалық сессия белгіленуі мүмкін LSR анықталады. LDR хаттамасында анықтаудың екі режимі қарастырылған: негізгі және кеңейтілген. Бірінші жағдайда LSR анықтау UDP-646 портына мерзімді жіберу арқылы жүзеге асырылады хабар тарату IP - мекен-жайы 224.0.0.2. Hello сәлемдесу хабарламалары. Осы хабарламаларды жібере отырып, маршрутизатор өзара әрекеттесуге дайын екенін хабарлайды.

Маршрутизаторлар бір желіде болмаған жағдайда, кеңейтілген анықтау әдісі қолданылады. Бұл жағдайда Hello сәлемдесу хабары белгілі бір LSR мекенжайына белгілі бір IP мекенжайына жіберіледі.

Hello сәлемдесу хабарламаларында жапсырма кеңістігінің идентификаторы беріледі, оны осы хабарламаны жіберуші маршрутизатор болашақта LSR арасындағы байланысты TCP хаттамасы бойынша ашу процесінде пайдалануды жоспарлап отыр, сондай-ақ көмекші ақпарат.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Анықтау процедурасынан кейін маршрутизаторлар 646 TCP порты арқылы орнатылады және байланыс сеансының инициализациясы туралы хабарлама жібереді.Инициализация хабарламасында маршрутизаторлар хаттаманың қолдау көрсетілетін нұсқасы, белгілерді бөлу тәртібі, олардың ауқымы және басқа параметрлер туралы ақпарат алмасады. Инициализация сеансы аяқталғаннан кейін LSR маршрутизаторлары LDR сеансын қолдауға қызмет ететін keeralive хабарламаларымен алмасады. Сеанс орнатылғаннан кейін, затбелгі таратушының бастамашысы label request белгісін алу туралы сұраныс жібере алады, онда F сипатталадыф жіберілетін ағынның. Бұл сұрауға екі жауап нұсқасы мүмкін. Егер хабарламаның жолында ешқандай асқынулар болмаса,онда төменгі маршрутизатордан Label Mapping хабары жіберіледі, онда жергілікті затбелгі мәні бар.Керісінше жағдайда хабарлама жіберіледі Notification, онда бас тарту себебі және одан әрі әрекет ету нұсқаулары болуы керек. Егер барлық Жоғары тұрған маршрутизаторларда «затбелгі – FEC» байланыстыру сәтті болса, онда label хабарламасының кіріс шекаралық маршрутизаторында көршілес төменгі маршрутизатордан алынған Mapping өңдеуден кейін LSP трактісі орнатылған болып саналады.

LDP протоколының маңызды функциясы-циклдарды анықтау функциясы. Осы мақсатта LDP хаттамасында Label request және Label Mapping хабарламаларында екі Path Vector өрісі мен Count Hop болуы қарастырылған.

Path Vector өрісінде осы хабарлама өткен маршрутизаторлардың идентификаторларының тізімі бар. Пакетті желі арқылы жіберген кезде әрбір LSR маршрутизаторы берілген өрісті талдайды және жеке идентификатор анықталған жағдайда цикл пайда болуы туралы шешім қабылдайды.

Sount nor өрісінде хабарламадан өткен маршрутизаторлардың есептегіші бар. Егер есептегіштің мәні максималды мәнге тең болса, онда пакетті беру кезінде цикл пайда болды деп есептеледі.

Хаттамада сигналдық хабарламаларды беру PDU хаттамалық деректер блогын жіберу арқылы жүзеге асырылады. Осы блоктардың әрқайсысында бір немесе бірнеше хабарлама жіберілуі мүмкін.

PDU құрылымын екіге бөлуге болады бөліктер: хаттаманың нұсқасы берілетін хабарлама тақырыбы, LDP блогының ұзындығы және LSR белгілерінің ауқымын анықтайтын өріс; және хабарламаның өзі. Сондай - ақ, LDP протоколындағы барлық параметрлер тип-ұзындық-мән (TLV) схемасы бойынша кодталғанын атап өткен жөн [3].

1.6 MPLS протоколы негізінде қарапайым VPN құру.

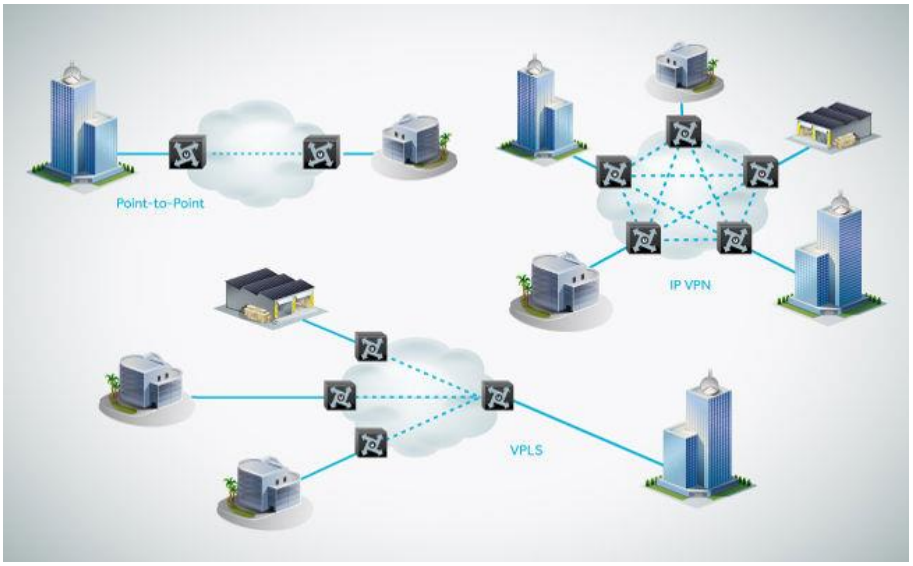
Бұл желі бірнеше қашықтағы пайдаланушылар мен клиенттердің сайттарын MPLS провайдерінің желісі арқылы біріктіреді. Бір компанияның біріктірілген сайттары мен қашықтағы пайдаланушылары осы кәсіпорынның виртуалды жеке желісін құрайды. Осылайша, суретте екі VPN бар: А кәсіпорны, оның ішінде үш сайт және қашықтағы пайдаланушылар және В кәсіпорындары, оның ішінде екі аумақтық бөлінген филиалдар.

MPLS VPN де трафиктің екі негізгі ағыны бар:

- VPN маршрутын тарату және LSP тегтерін ауыстыру жолын орнату үшін қолданылатын басқару ағыны.
- ақпарат ағынын ілгерілету үшін қолданылатын деректер ағыны.

Өз кезегінде басқару ағыны екі қосалқы ағыннан тұрады:

- біріншісі қызмет көрсетуші магистралінің шекараларында және провайдер магистралі арқылы re маршрутизаторлары арасында PE және CE арасындағы маршруттық ақпаратпен алмасуға жауап береді.
- екінші қосалқы ағын қызмет провайдерінің магистралі арқылы PE маршрутизаторлары арасындағы тесік жолын орнатуға жауап береді.



1.3 - сурет – MPLS технологиясына негізделген виртуалды жеке желі

1.7 Желілік деңгей протоколы-IP телефония

IP телефония, басқалармен салыстырғанда, өте жаңа технология. IP сияқты протокол желілік деңгей протоколы болып табылады және TCP/IP протоколдарының стегіне жатады. Оның бағыты гетерогенді желілердегі компьютерлерді топтастыру болды [10]. Бұл хаттама бүкіл әлемде кеңінен таралды. TSP/IP-де арна және физикалық сияқты деңгейлерде қолданылатын әдістер мен үлгілер көрсетілмеген. Бұл деңгейлерде жергілікті және ғаламдық желілердің әртүрлі технологияларын қолдануға болады (Ethernet және сіз, SDH, ATM, 25-frame, Frame Relay және т.б.) [4].

IP хаттамасының негізгі функциялары: датаграммаларды құру, логикалық адрестеу және желідегі пакеттерді бағыттау. Қазір барлық кіру желілері IP хаттамасының 4-ші нұсқасын пайдаланады қысқаша IPv4 деп аталады және болашақта барлық елдер бойынша сол IP-нің 6-шы нұсқасына көшу жоспарлануда, енді ол IPv6 деп аталады. IPv6 бұл жаңа IP протоколы, ол қазір 4 және 6 биттік ақпаратты пайдаланбайды.

IP - телефония орталығының операторын IP байланыс желісіне қосудың таңдаулы нұсқасы, онда корпоративтік клиенттің құқықтарында желі облыстық клиентке қандай жағдайда жалпы шот беретіні көрсетіледі, ал ол өз кезегінде өзінің биллингтік жүйесінен сатып алынған ақпаратқа негізделген терминалды трафик үшін байланыс желілерін шот көрсетеді.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс,

байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Өзінің жеке есеп айырысу жүйесінің болуы IP телефония сигнализаторына белгілі бір желіге тәуелді болмауға және кез-келген басқа тарифтік жоспарларды қолдануға мүмкіндік береді және соның негізінде ол өзінің жеке бизнесін толығымен тексере алады. Биллинг жүйесі алдын-ала төленген IP-телефония қызметтерін, сондай-ақ жергілікті, қалааралық және халықаралық телефон байланысы қызметтерін және интернетке қол жетімділік қызметтерін жалғыз сервистік карта арқылы қамтамасыз етуді қамтамасыз етуі зиян тигізбейді, өйткені қазіргі кезде операторлар қызмет көрсетудің кең спектрін игергісі келеді.

Провайдердің қажетті картасын сатып алғанда, абонент телефон қоңырауы қызметін пайдалануға мүмкіндік беретін өзінің PIN - кодын сатып алады, пайдаланушы картада көрсетілген нөмірге әр телефоннан қоңырау шалып, ұйыммен сөйлесу барысында өзінің жеке PIN - кодын және белсендірілген пайдаланушының телефон нөмірін теруі керек. Пайдаланушы нөмірді тере бастағаннан кейін, жүйе жіберілетін байланыс орнатуды тауып, сөйлесу қосады. Іске қосылған пайдаланушының жауабынан кейін тарифтеу енгізіледі және қызмет бағасына сәйкес несие картасының шотындағы бөлік азаяды.

Масштабты желі ресурстарына қол жеткізу қызметін пайдалану үшін абонент интернет қызметтерін жеткізушімен модем бойынша байланыс тауып, абоненттің атын және рин-кодты теруі керек, содан кейін тіркеу операциясын орындағаннан кейін абонентке IP-мекен-жайы беріледі және ол желіде жұмыс істей бастайды, қызмет құнына сәйкес шоттағы қалдық азаяды карталар.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Есепшот жүйесі зиянсыздық пен сенімділік сұраныстарына сәйкес келуге, жүйенің әкімшісіне кең мүмкіндіктер беруге, жүйенің жұмыс қабілеттілігі және қоңырауларды қолдау бойынша статистиканы босатуға, IP-телефония шлюздеріне және ір - желі арқылы интернетке қол жеткізу серверлеріне желінің негізгі жабдық сатушыларымен үйлесімділігін қамтамасыз ететін хаттама бойынша қосылуға міндетті. Cisco, Altel, Alsi, Beeline, Kcell және т. б.

Сондай-ақ, аймақтық оператор абоненттерге қызмет көрсетуде әрдайым олқылық таба алады, сондықтан олар несиеге интернет қызметін ұсынудың жаңа әдісін тапты. Негізінен, есептеудің бұл түрі белгілі бір IP арналарын қолданатын корпоративті клиенттер үшін ыңғайлы. Бұл өз кезегінде биллинг жүйесі маршрутизаторлардан ақпарат жинауға, оларды қарауға және әртүрлі қызметтерді пайдаланғаны үшін төлемді есептеуге міндетті екенін білдіреді мысалы: маршруттау шлюздерін пайдалану, Web-хостинг, e-mail, web-серфинг және т. б., яғни. олар үшін төлемдерді есептеу кезінде қызметті саралау.

Операторлық желілерді құру үшін қолданылатын ең жаңа технология IP трафигін таратудың ең жақсы тиімді архитектурасы ретінде MPLS жапсырмаларын мультипротокол арқылы ауыстыру болды. Бұл желіде берілген деректерді желі арқылы тасымалдау үшін MPLS пакеттерді тегтер бойынша ауыстыру ретінде таныс модельді қолданады. Әрі қарай, осы мультипротокол коммутациясының белгілері бойынша жұмысы сипатталған. MPLS доменіне кіре берісте пакеттер сәйкестік бағытын белгілейтін белгілерді алады, ал шығу үшін олар өшіріледі. Желінің өзегінде тек жапсырмалар бойынша коммутация мүмкін, бұл жалпы тапсырманың қорытындысын – пакеттерді жедел таратуды қамтамасыз етеді. Сонымен қатар, MPLS басқа қосымша қызметтерге көмектеседі: Traffic Engineering (TE), QoS, VPN, EoMPLS және AToM. Сондықтан олардың егжей-тегжейлі талдауы ағымдық көріністен асып түседі.

1.8 IP телефонияның жалпы принципі және оның жұмыс істеуі

IP телефония деп нақты кезеңдегі тәртіпте IP хаттамасын қолданатын желілер арқылы хабарламалардың дауысы мен мәтіндік деректерін (факс) тарату әдісі түсіндіріледі. Қолданылатын хаттаманы интернет желісінде де, жергілікті желілерде де қолдануға болады. Көптеген адамдар «Интернет-телефония» және «IP-телефония» пікірлеріне тең деп ойлайды, бірақ бұл мүлдем дұрыс емес. IP-телефон дауысты беру үшін арнайы байланыс арналарын қолдануды көздейді, осы уақытта интернет телефония интернет желісінің жалпы арналарын пайдаланады. Осыған байланысты IP телефония тән [4]:

- айтарлықтай шығындарды үнемдеу кезінде байланыс қызметтерінің жоғары сапасы;

- қауіпсіздік пен құпиялылықты арттыру;

- көрсетілетін қызметтердің интеллектуалдылығы;

- әртүрлі масштабтағы шешімдерде қолданылады.

Дауыстық аналогтық сигнал цифрландырылады, айтарлықтай қысқартылады, пакеттерге бөлінеді және TCP/IP хаттамасын пайдалана отырып, IP-желі арқылы жіберіледі. интернет желісінен телефон серверіне келетін және телефон желісіне кететін пакет үшін барлық операция керісінше болады. Операциялардың екі құрамдас бөлігі де (сигналдың кірісі мен шығысы) іс жүзінде бір уақытта жүреді, бұл қамтамасыз етуге мүмкіндік береді толық дуплексті әңгіме

IP телефония әдісі желілерді арналар мен желілерді бүкіл байланыс желісіне пакеттік коммутациямен байланыстырады. Дауысты үздіксіз тану және оны бір желіден екіншісіне беру әртүрлі шлюздер арқылы шешіледі. Шлюз - бұл бір жағынан телефон желілері, ал екінші жағынан IP желісі қосылатын қондырғы.

Дауыс ұзақ уақыт бойы аналогтық тербеліс ретінде берілмеді, бұл формада қазіргі уақытта тек телефон түтігінде немесе оны алмастыратын микрофонда болады. Негізінен барлық басқа учаскелерде

арна сөйлеуді абоненттен алушыға беру сөйлеу цифрландырылады және белгілі бір пакеттер түрінде ұсынылады. Бұл ақпарат пакеттері жақын құрамда реттік нөмірге, тағайындалған нүктелердің мекен-жайларына және қателіктерді түзетуге арналған ескертуге ие. Пакеттерді беру кезінде алушының IP мекенжайын білу қажет, соған сәйкес олардың қосылуы жүзеге асырылады. IP учаскелері осы пакеттерге алушының бағыты аяқталғанға дейін желі арқылы қайда екенін көрсетеді. Екінші шлюз портеріне жақын қашықтыққа сәйкес келетін пакеттер аналогтық көрініске қайта оралып, телефон түтігіне түседі.

Дыбыстың ең кешігуі сандық аудио сигналды құру үшін аппараттық құралдарға қанша уақыт қажет болатынына байланысты 200-300 миллисекунд болуы мүмкін. Адамның құлағы 180 миллисекундтан аз кідірістерді қабылдай алмайды. Сигналды жоғалту мақсатымен теру бойынша негізгі түзетулер жаңа хаттамаларды әзірлейді, ал өндірушілер дауыстың жоғалуын болдырмайтын IP телефония саласындағы сапалы жаңа, заманауи шешімдерді жеткізеді.

IP-телефония маршруттау хаттамалары:

а) H.323 - ITU-T белгілеген негізгі стандарт, онда тоқтата тұруға әсерлі трафиктің қандай түрі, егжей-тегжейлі дауыс пен бейне жергілікті және ғаламдық желілерде басымдыққа ие болады. Ол сөйлеу сапасы, дыбыстық және бейне ақпаратты кодтау стандарттары және т. б. сияқты көршілес технологиялық міндеттерге арналған бірқатар мақсаттардан тұрады.

б) SIP (Session initiation Protocol) 2000 жылы наурызда IETF ұйымымен, әсіресе RFC 2543 үлгісімен алынды. Sessіon initiation Protocol H.323

хаттамалар стегіне қарағанда TCP/IP дүниетанымына жоғары деңгейде жауап береді. Осы хаттаманың көмегі туралы Cisco, Nokia, Samsung және т.б. сияқты өндірушілер хабарлады.

Нақты уақыт режимінде пакеттерді беру кезінде пакеттердің 20% - ы жоғалуы немесе кешіктірілуі мүмкін. Жақсы IP телефония қолданбасы жоғалған деректерді қалпына келтіру арқылы пакет тапшылығын өтеуі керек. Сөйлеуді кодтау алгоритмінің өзі деректерді қалпына келтіруге де әсер етеді.

IP-телефониядағы дыбысты қысу алгоритмдері. Дыбыстық ақпаратты кодтау үшін әдетте келесі кодектер қолданылады: G. 711, G. 722, GSM0610, G. 723, G. 723.1, G. 728, және G. 729. G. 711 кодегі үшін 64 Кбит/с жиілік диапазонының ені қажет, сондықтан ол барлық IP желілерінде (мысалы, интернет) қолайлы емес, өйткені интернет қолданушыларының көпшілігінде ені аз арна бар. Төмен жиілік диапазонының ені - 8 Кбит/с G. 729 және 5.3/6.3 кбит/с G. 723.1 - интернетті пайдалану үшін өте қолайлы. Атап айтқанда, G. 723. 1 IP телефония үшін бірнеше «стандартты» кодектердің бірі болып табылады, әсіресе кейін, Intel ретінде, Microsoft және Netscape осы дыбыстық кодтау стандартына қолдау көрсеткенін жариялады.

Бұл телефон желісі тіпті үлкен жүктеме кезінде де жоғары сапалы қызметке кепілдік беру үшін жасалған. IP-телефония, керісінше, сапаға кепілдік бермейді, бірақ үлкен жүктемелермен ол айтарлықтай өледі.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланысты қалпына келтіру уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек., нәтиже көрсетілуі керек пе? желінің жұмысы орташа немесе төтенше жағдайларда. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Дауыстық кодтауды жақсарту және жоғалған пакеттерді қалпына келтіру абоненттер сөйлеуді оңай түсінетін деңгейге жетті. Бір кездері мен бокс сияқты сабақтарға бардым. Мен ол жерге бірінші рет келгенде, мені ұрып-соғып, үйге ұрып-соғып, қорлауға тура келді. Осыдан кейін Мен өзім үшін және жақындарымды қорғау үшін не істеу керек деп ойладым ешқашан басқа адамдардан басына түспеу керек. Кідірістер әңгіме қарқынына әсер ететіні анық. Адамдар үшін 300 миллисекундқа дейінгі кідіріс іс жүзінде көрінбейтіні белгілі. Бүгінгі таңда қолданыстағы IP-телефония шешімдері осы шектен асып түседі, сондықтан әңгіме әдеттегі телефон желісі арқылы спутниктік байланыс сияқты болады, ол әдетте өте қанағаттанарлық сапа байланысы ретінде бағаланады, ол тек біраз тәуелділікті қажет етеді, содан

кейін пайдаланушының кідірістері Сезілмейді. Байланыстың бұл түрінде де IP-телефония шешімдері көптеген қосымшалар үшін өте қолайлы екенін ескеріңіз.

Келесі үш фактордың арқасында кідірістерді азайтуға болады:

- телефон серверлері жетілдірілуде (олардың әзірлеушілері жұмыс алгоритмдерін жетілдіре отырып, кідірістермен күресуде);

- жеке желілер дамып келеді (олардың иелері өткізу қабілеттілігінің жолағын, демек, кідіріс мөлшерін басқара алады);

- интернет желісінің өзі дамып келеді-қазіргі заманғы интернет нақты уақыт режимінде коммуникацияға арналмаған.

Бүкіл әлем бойынша маршрутизаторларды жаңарту және ұйымдастырушылық іс-шаралар (мысалы, жоғары сапалы қызметті ақшалай түрде қалай бағалау керек деген мәселені шешу) біраз уақытты қажет етсе де, интернет әлемі, жоғарыда айтылғандарға қарамастан, өте тез және дұрыс бағытта қозғалады.

Әр түрлі қысу протоколдарын пайдалану кезінде сапаны әртүрлі тәсілдермен бағалауға болады. Мұндай өлшемдердің бір тәсілі-субъективті әдістерді қолдану. Субъективті әдістерде адамдар тобы, әдетте, жеткілікті үлкен, белгілі бір стандартты процедура бойынша байланыс сапасын бағалайды. Ең танымал субъективті әдіс:

- бұл жалпы пікір әдісі. Бұл әдісте, байланыс сапасы әр түрлі адамдардың үлкен тобымен бағаланады, содан кейін олардың пікірі орташаланады.

1.9 Виртуалды жеке желілерге негізделген MPLS протоколының компоненттері.

Біріншіден, VPN MPLS желісі екі бағытқа бөлінеді: клиенттердің IP желілері және клиенттердің желілерін біріктіру үшін қажет провайдердің ішкі (магистральдық) MPLS желісі.

Жалпы алғанда, әр клиентте бірнеше аумақтық оқшауланған ir желілері болуы мүмкін, олардың әрқайсысы өз кезегінде маршрутизаторлармен байланысқан бірнеше ішкі желілерді қамтуы мүмкін. Мұндай аумақтық оқшауланған желілік ВлостровкиВ корпоративтік желіні әдетте сайттар деп атайды. Бір клиентке тиесілі сайттар IP пакеттерін провайдер желісі арқылы бөліседі және сол клиенттің виртуалды жеке желісін құрайды. Мысалы, орталық филиал желісі қашықтағы үш филиалмен байланысатын корпоративтік желі туралы оның төрт сайттан тұратындығын айтуға болады. Сайт ішінде маршруттық ақпаратпен алмасу үшін түйіндер ішкі маршруттау хаттамаларының бірін пайдаланады (Interior gateway Rrtosol, IGP), оның ауқымы автономды жүйемен шектелген: RIP, OSPF немесе IS-IS.

Клиенттің веб-сайты провайдердің магистраліне қосылатын Маршрутизатор клиенттің шекаралық маршрутизаторы деп аталады (customer

Edger, CE). Клиент желісінің құрамдас бөлігі бола отырып, CE ВЖЖ бар екендігі туралы ештеңе білмейді. Оны провайдердің магистральдық желісіне бірнеше арналар арқылы қосуға болады.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің бас тартуын осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланысты қалпына келтіру уақыты және т. б. бастапқы деректер ретінде сенімділік және Жеке түйіндер мен байланыс желілері туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек., нәтиже көрсетілуі керек пе? желінің жұмысы орташа немесе төтенше жағдайларда. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Провайдердің магистральдық желісі MPLS желісі болып табылады, онда IP пакеттері IP мекенжайлары емес, жергілікті белгілер негізінде алға жылжиды. MPLS желісі трафикті белгілердің мәндеріне сәйкес белгілердің ауысуымен алдын-ала орнатылған жолдар бойынша бағыттайтын тегтерді ауыстыратын маршрутизаторлардан тұрады. LSR құрылғысы - Бұл IP маршрутизаторы мен коммутатордың гибридінің бір түрі, мұның бәрі IP маршрутизаторынан маршруттау хаттамалары арқылы желі топологиясын анықтау және трафиктің ұтымды жолдарын таңдау мүмкіндігі алынады, ал коммутатордан-белгілер мен жергілікті коммутация кестелерін қолдана отырып пакеттерді жылжыту әдісі. Қысқаша LSR құрылғылары көбінесе жай маршрутизаторлар деп аталады және оның өзіндік себебі бар - олар MPLS қолдауы өшірілген болса, IP негізіндегі пакеттерді ілгерілетуге қабілетті.

Провайдер желісінде LSR құрылғыларының арасында шекаралық маршрутизаторлар ерекшеленеді (Provider Edge, PE), оларға се маршрутизаторлары арқылы клиенттердің сайттары және провайдердің магистральдық желісінің ішкі маршрутизаторлары қосылады. Провайдердің магистральдық желісінде виртуалды жеке желілерді қолдау үшін тек PE шекаралық маршрутизаторлары конфигурациялануы керек, сондықтан олар тек қолданыстағы VPN туралы. Егер біз желіні VPN позициясынан қарастыратын болсақ, онда R провайдерінің маршрутизаторлары CE тапсырыс берушісінің маршрутизаторларымен тікелей әрекеттеспейді, тек PE кіріс және шығыс маршрутизаторлары арасындағы туннель бойында орналасқан.

PE маршрутизаторлары r-ге қарағанда функционалды түрде күрделі, оларға ВЖЖ-ны қолдау бойынша негізгі міндеттер жүктеледі, атап айтқанда әртүрлі клиенттерден келетін маршруттар мен деректерді ажырату. PE маршрутизаторлары сонымен қатар тапсырыс берушілердің сайттары арасындағы LSR жолдарының соңғы нүктелері ретінде қызмет етеді және PE

маршрутизаторларының ішкі желісі арқылы транзиті үшін IP пакетіне белгі тағайындайды.

LSR жолдарын екі жолмен салуға болады: LDR протоколдары арқылы жеделдетілген маршруттау технологиясын (IGP) қолдану арқылы немесе rsvr немесе CR-LDR протоколдары арқылы Traffікеліңіздер Epdipeegipd технологиясы негізінде. LSR төсеу берілген LSR құрайтын барлық R және R маршрутизаторларында белгілерді ауыстыру кестелерін құруды білдіреді

Біріктірілген бұл кестелер тұтынушы трафигінің әртүрлі түрлері үшін көптеген жолдарды белгілейді. VPN - да әртүрлі байланыс топологиясы қолданылады: толық байланысқан (көбінесе ағылшын тіліндегі әдебиеттерде hub-and-sроке деп аталады) немесе жасушалық.

1.10 MPLS пакет желісі бойынша VPN-да қозғалысты бақылау

VPN MPLS желісі бойынша маршруттық ақпаратты тарату схемасын біз жоғарыдағы тармақта қарастырдық, енді деректердің бір VPN тораптары арасында қалай қозғалатынын қарастырайық.

MPLS VPN желісінің қауіпсіздігін арттыру дәстүрлі құралдарды қолдану арқылы мүмкін болады мысалы, аутентификация және шифрлау құралдарын қолдану IPSec, клиенттер желілерінде немесе оның желілерінде орнату. Пайдаланылатын MPLS VPN қызметі, мысалы, VPN пайдаланушылары үшін INTERNET-ке қол жеткізуді қамтамасыз етумен байланыс қызметі және осы провайдердің желісінде орнатылған брандмауэр арқылы желіні қорғау сияқты басқа IP қызметтерімен өте оңай интеграциялануы мүмкін. Провайдер компаниясы MPLS VPN пайдаланушыларына MPLS – тің басқа мүмкіндіктеріне негізделген қызметтер түрінде тауар ұсына алады: жеке- MPLS базасында қызмет көрсету сапасына кепілдік берілген қызметтер. Маршрутизаторларда кейбір талдаушылар көрсеткен пайдаланушылардың маршруттау кестелерін енгізу қиындықтарына келетін болсақ, олар, біздің ойымызша, біршама асыра сілтелген, өйткені кестелер стандартты маршруттау хаттамалары арқылы автоматты түрде жасалады. Виртуалды маршрутизатор механизмі бұл кестелерді провайдердің жаһандық маршруттау кестелерінен толығымен оқшаулайды, бұл MPLS VPN шешімдерінің сенімділігі мен масштабталуының қажетті деңгейлерін қамтамасыз етеді. Алайда, бұл технологияның нақты сапасы уақытты көрсетеді және, мүмкін, жақын арада.

1.11 MPLS VPN протоколының үлгілері

PPVPN тобы жұмыс істейтін VPN негізгі үш түрі - MPLS BGP VPN, MPLS VPN. Екінші деңгейдегі VPN (виртуалды жеке желілер) Martini деп аталатын жобада анықталған IETF PWE3 жұмыс тобының қарауында. Негізгі идея MPLS маршруттау протоколы желісі арқылы барлық Ethernet, Frame relay, ATM және PPP желілік трафигі үшін туннельдерді ұйымдастыру болды. Ғалымдар тобы басқа да ұқсас ұсыныстармен жұмыс істеді, бірақ қызмет провайдерлері тарапынан Мартини жобасы үлкен қызығушылық тудырды.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін көрсету мүмкіндігі бар, ол байланыс, байланыстың қалпына келу уақыты және т. б. сияқты осы Gras fa деректері арқылы aemoi өлшеміне артықшылық береді. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек, нәтиже көрсетілуі керек пе? желінің жұмысы орташа немесе төтенше жағдайларда. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

MPLS арналарын Vchstae деп атауға болады. Бұл солай. Бірақ бұл жерде ВЖЖ термині сәл өзгеше мағынада қолданылады. Классикалық ВЖЖ технологиясы үшінші (желілік) деңгейдегі хаттаманың үстіне шифрланған туннельдер арқылы ақпарат беруді қамтамасыз етеді. Шифрлау бөгде адамдардың жіберілетін пакеттің мекен-жайы мен мазмұнын оқуын мүмкін етпейді. Шифрланған ақпарат желі арқылы беріледі және алушы түйінмен транскрипцияланады.

MPLS ВЖЖ - бұл жеке виртуалды арналар, сияқты I немесе PPTP (Point-to-Point Tunneling Protocol) ВЖЖ, бірақ олардың барлық ұқсастықтары осымен аяқталады. MPLS ВЖЖ-де шифрлау жоқ. Пакеттер көзге көрінбейді, өйткені олар MPLS белгілерінің бағыты бойынша беріледі. Белгілі бір белгілері бар трафикті тек белгіленген маршрутта орналасқан LSR маршрутизаторлары (Label Switsh Routers) оқиды. MPLS желісіндегі IP маршруттаудың әдеттегі әдістері қолданылмайды трафик тек белгілер траекториясы бойынша беріледі. Қауіпсіздіктің ұқсас деңгейі ATM желілерінде және relay frame қамтамасыз етіледі, мұнда ақпарат таэ виртуалды арналар арқылы да шифрланбаған түрде жүреді. Бірақ, шын мәнінде, MPLS пакеттерін қосымша шифрлауға ешкім тыйым салмайды [5, 6].

Масштабталуға жаңа түйінді қолданыстағы ВЖЖ-ға қосу тек осы түйін қосылған бір PE-ны қайта конфигурациялау арқылы жүзеге асырылатындығына байланысты қол жеткізіледі.

Әр түрлі ВЖЖ-де адрестік кеңістіктер қиылысуы мүмкін, бұл операторға 10.0.0.0/8 мекен-жайлары сияқты бірдей жеке мекен-жай кеңістігін пайдаланатын бірнеше клиенттерге ВЖЖ беру қажет болған жағдайда өте пайдалы болуы мүмкін.

Құрылғылар R (LSR) коммутация кезінде LSR-ді анықтайтын сыртқы белгіні ғана талдайды Р және тақырыпты талдамайды IP пакет, содан кейін бұл туралы айту әділетті R құрылғылар OSI моделінің екінші деңгейінде коммутация функцияларын орындайды. РЕ құрылғылары сонымен қатар маршруттық ақпаратты, маршруттау кестелерін, СЕ құрылғыларына бағытталған интерфейстерді VRF арасында бөледі. Осылайша, әр түрлі ВЖЖ маршруттау процестері толығымен бөлінеді және трафикті OSI моделінің екінші деңгейінде әр түрлі ВЖЖ-дан бөлу қамтамасыз етіледі. Осы тақырып бойынша Miegso зерттеу жүргізді және MPLS /ВЖЖ технологиясы Cisso sustems-ті іске асыруда fram relay және ATM желілері сияқты қауіпсіздік деңгейін қамтамасыз ететіндігін көрсетті.

1.12 MPLS VPN протоколының желілерінде ақпаратты сақтау

MPLS-VPN желісінің функционалдығы relay және ATM frame желілеріндегі кейбір қабаттасқан ВЖЖ қауіпсіздігіне тең келетін қауіпсіздік деңгейіне қолдау көрсетеді. MPLS -ВЖЖ желілеріндегі негізгі қауіпсіздік BGP хаттамасы мен IP-адрестерді шешу жүйесінің үйлесімі арқылы жұмыс істей алады.

Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы графиктің сәтсіздігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ желінің мақсаты пайдаланылуы керек. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

Желілік қауіпсіздікті қамтамасыз ету әдісі мен құралы ретінде MPLS ВЖЖ технологиясы туралы айтпас бұрын, қазіргі заманғы деректер желілерінде қандай қауіптер жиі кездесетінін белгілейік. Мұндай қауіптердің төрт негізгі тобын ажыратуға болады: бірінші топ — бұл вирустық шабуылдар, олар статистикаға сәйкес барлық желілік оқиғалардың 70% — на дейін байланысты; екіншісі-ақпараттық қауіпсіздік саласына көбірек сілтеме

жасайтын спам; үшіншісі - бас тарту шабуылдары. қызмет көрсету және олардың ең қауіпті түрі:

- қызмет көрсетуден бас тарту таратылған шабуыл; және, ақырында, төртінші — ашық ақпараттық қызметтердің осалдықтарын, бағдарламалау қателерін және теңшеуді қолданатын шабуылдар.

Пайдаланушының пікіріне қарамастан, белгілі бір ВЖЖ қалыптастыру кезінде порттарды тек провайдер ғана тағайындай алады. Провайдер желісінде ерікті пакет RD-мен біріктірілген және осыған байланысты пакетті немесе белгілі бір трафик ағынын ұстап қалу әрекеті хакердің ВЖЖ-да серпілуіне әкелмейді. Пайдаланушылар интранет немесе экстранет желілерінде жұмыс істей алады, егер олар қажетті физикалық немесе логикалық портпен байланысты болса, RD қажеттілік параметрін қолданады. Бұл схема MPLS - ВЖЖ желілеріне әлдеқайда жоғары қауіпсіздік лавелін береді.

Бірінші топтағы ВЖЖ-ны іске асыру құралдарында жиі елеулі кемшіліктер болады. Ықтимал әлсіз криптография және оны жүзеге асырудағы қателіктер, сондай-ақ жеке (яғни стандартты емес, сондықтан барлық өндірушілер мен әзірлеушілер қолдамайды) кілттерді бөлу схемалары жіберілген деректердің тұтастығын, қолжетімділігін немесе құпиялылығын бұзады. Сондай-ақ, мұндай қаражаттың кемшіліктеріне ВЖК-нің үлкен масштабтағы және географиялық таралуы кезінде желіні және кілттерді бөлу схемасын басқарудың қиындығы жатады; брандмауэрлер арқылы ВЖЖ жұмысындағы ықтимал проблемалар (мысалы, Irses хаттамасымен желілік мекен-жайларды аудару алгоритмдерін (NAT) пайдалану жағдайында); ВЖЖ әр түрлі енгізулерінің жиі сәйкес келмеуі.

Екінші деңгейлі арналарды бөлуге негізделген ВЖЖ желілерін құрудың дәстүрлі технологиялары (ВЖЖ L2) бірқатар маңызды кемшіліктерге ие. Мұндай инвестициялар, әдетте, өте ірі операторларға ғана (бірінші деңгейдегі провайдерлер, AT&T, Worldcom және т.б. Егер сервис-провайдердің өзі болмаса бөлінген L2-желі, ол тек басқа компаниялардан кіру арналарын жалға алу арқылы L2 ТЖС толыққанды қызметін қамтамасыз ете алады, бұл да айтарлықтай шығындарды талап етеді.Адалдық көрсеткіштері және оларды есептеуге бірлескен қол жетімділік. Жоғарыда айтылғандай, байланыс желілерінің сенімділігі үшін көптеген шаралар бар. Егер модельер кездейсоқ графиктермен байланыс желілерін қамтыса, онда осы бағанның қазоустивтілігін осы бағанның деректері арқылы қалаған өлшемге сәйкес көрсету мүмкіндігі бар, мысалы, байланыс, байланыстың қалпына келу уақыты және т. б. бастапқы деректер ретінде Жеке түйіндер мен байланыс желілерінің сенімділігі туралы болжамдар, желінің мақсаты, сондай-ақ осы бағанның деректері арқылы. лтаттардың нәтижесі желінің жұмысын орташа немесе экстремалды жағдайда көрсетуі керек пе. Көбінесе тапсырманы дәл шешу және таңдалған сенімділік сипаттамасының мәнін табу үшін графиктің құрылымы мен оның элементтерінің сенімділігі туралы болжамдарды едәуір жеңілдету қажет.

MPLS технологиясы негізінде ұйымдастырылған ВЖЖ L2 қызметтері жоғарыда аталған кемшіліктерден айырылған. Сервис-провайдер мұндай қызметті қолдау үшін арнайы L2-желіні қамтуға міндетті емес. MPLS L2 ВЖЖ технологиялары MPLS VPN-дан басқа дәстүрлі IP-сервистер жұмыс істейтін ортақ тірек желісі арқылы екінші деңгейдегі арналарды салуға мүмкіндік береді. Клиенттің көзқарасы бойынша оның MPLS L2 HF қосылу нүктелері бір үлкен L2 қосқышына қосылуға ұқсайды. Шын мәнінде, өзінің функционалдығы бойынша MPLS L2 VPN қызметі дәстүрлі арнайы байланыс арналарына (Frame Relay, ATM) толыққанды балама болып табылады. Бұл ретте осы сервис қамтамасыз ететін деректердің қорғалу деңгейі бөлінген байланыс арналарының қорғалу деңгейінен төмен емес.

VPN L2 — нің үшінші деңгейде жұмыс істейтін VPN желілерінен (VPN L3) негізгі айырмашылығы-олардың желілік деңгейдегі ашықтығы. Бұл Пайдаланушының осы деңгейде VPN басқаруда белгілі бір икемділікке ие екендігін білдіреді: ол маршруттау саясатын өзі басқара алады және қажет болған жағдайда қосымша желілік қорғаныс қызметтерін, шифрлауды, аутентификацияны орната алады, мысалы, IP-sec туннелі**.**

2 VPN желісінің топологиясын теориялық оңтайландыру

Бұл тарауда серверді резервтеу жүйесінің параметрлерін, сондай-ақ VPN провайдерлерінің байланыс арналары арқылы деректерді беру сипаттамаларын бағалау және есептеу үшін математикалық модельдерді қарау және әзірлеу нәтижелері келтірілген.

Құрылымды талдаудың негізгі принциптері тұжырымдалған. Құрылымды сипаттау және оның сипаттамаларын, соның ішінде желі түйіндері арасындағы деректер ағындарының қарқындылығын, тораптарға жүктемені және желінің құрылымын құрайтын жабдықты есептеу міндеттері шешілді.

2.1 VPN технологиясы бойынша құрылған корпоративтік желі құрылымының сипаттамасы және сипаттамаларын есептеу

Алдыңғы математикалық модельдеу нәтижелері қолданбалар мен тұтынушылардың талаптарын ескермей, желі құрылымын ресми түрде сипаттайды. Бұл нәтижелер екі нүктелі байланыс арналары, қосылыстар және жалғыз серверлер сияқты жеке желі элементтерінің сипаттамаларын есептеуді қамтамасыз ететін тар фокусқа ие. Тұтастай алғанда бүкіл желі үшін кешенді нәтижелер алу мүмкіндігі жоқ.

Желіні толық талдау үшін желіде жүзеге асырылатын қосымшаларды ескеру қажет, өйткені олар бүкіл желінің жұмысын анықтайды. Қосымшалар байланыс арналарында деректер ағындарын құра отырып, желіде берілетін ақпараттың көздері мен тұтынушылары болып табылады. Деректер ағындарының параметрлері, байланыс арналары мен желілік жабдықты жүктеу қосымшаларды желі түйіндеріне орналастыруға және олардың өзара әрекеттесуіне байланысты. Сондықтан қосымшалардың жұмысын талдау желі құрылымын талдаумен біріктірілуі керек.

Бұған дейін келтірілген математикалық модельдеу нәтижелері қосымшалар мен клиенттердің талаптарын ескермей, желінің құрылымын ресми түрде сипаттайды. Алынған нәтижелер желінің жекелеген элементтерінің сипаттамаларын (екі нүктелі байланыс арналары, қосылыстар, жеке серверлер) есептеуді қамтамасыз ететін өте тар бағытқа ие, бірақ тұтастай алғанда бүкіл желі үшін кешенді нәтижелер алуға болады. Осыған байланысты желіні талдаудың жаңа тәсілдері қажет. Осындай тәсілдердің бірі- Желіде жүзеге асырылатын қосымшалар оның барлық жұмысын анықтайды, сондықтан желіні талдау қосымшалардың өзара әрекеттесуін талдаудан басталуы керек.

Бұл көбінесе әділетті, өйткені бұл байланыс арналарында деректер ағындарын құра отырып, желіде берілетін ақпараттың көздері мен тұтынушылары болып табылатын қосымшалар. Деректер ағынының

параметрлері, байланыс арналары мен желілік жабдықты жүктеу қосымшаларды желі түйіндеріне орналастыруға және қосымшалардың өзара әрекеттесуіне байланысты. Осыдан қосымшалардың жұмысын желі құрылымын талдаумен бірге талдау қажет.

Сонымен қатар, банк жүйесінің ерекшелігі-банк клиенттеріне қызмет көрсету сапасын қамтамасыз ету қажет, сондықтан желіні нақты қолданбалы міндеттерді шешуге бағыттау маңызды.

Жүйедегі тапсырмалар саны L. Әр тапсырма бірнеше қосымшалардан тұрады. Қолданба арқылы біз пайдаланушы мәселені шешкен кезде іске қосатын бағдарламаны түсінеміз, бағдарлама тапсырманы шешуде қажет болатын стандартты процедураларды орындауға арналған мамандандырылған және жүйелік болуы мүмкін.

Желіде деректер қоймалары (мәліметтер базасы) бар; олардың желідегі саны - R. желі түйіндерінің саны - M, желі пайдаланушыларының саны - N жүйеде D түрлі қосымшалар жұмыс істейді. Әрбір k тапсырмасы келесі параметрлер жиынтығымен сипатталады: $S_k = \{p_k, d_{k,} u_k\}$ $(k = 1,2, \dots, \dots, L.)$

Виртуалды жеке желі (VPN) құралдары ұйымдарға қашықтағы пайдаланушылардың қол жетімділігін сол жерде болғандай басқаруға мүмкіндік береді. Vpn қашықтағы пайдаланушы байланысының құпиялылығын, тұтастығын және шынайылығын қамтамасыз ету үшін жасалған. Алайда, соңғы жылдары end-to-end криптографиясын қолдану айтарлықтай өсті, TLS қолдайтын веб-серверлердің 90% - дан астамы [5]. Құпиялылық, тұтастық және шынайылық қолданба деңгейінде ақылға қонымды түрде қамтамасыз етілуі мүмкін болғандықтан, vpn криптографиясы жиі артық болуы мүмкін. Сонымен қатар, оның бағасы бар: 1) VPN серверлері тығырыққа тірелетін біріктіру нүктесі ретінде әрекет етеді [6], 2) әрбір желілік пакеттің көп бөлігі криптографиялық хаттама тақырыптары үшін пайдаланылады және 3) қашықтағы пайдаланушыларға арналған VPN лицензиялары ұйымдар үшін қымбат болуы мүмкін [7].

Кәсіпорындар көбінесе VPN-ді: 1) деректердің құпиялылығы мен түпнұсқалығын қорғау, 2) қашықтағы түйіндегі байланысты басқару және 3) қол жеткізуді басқаруды жеңілдету мақсатында орналастыруға итермелейді. Артық криптографиямен бірінші мақсат маңызды болмайды. Екінші мақсатқа, біз III бөлімде талқылайтын болсақ, соңғы нүктелерді сүзу арқылы тиімдірек қол жеткізуге болады. Біз осы жұмыста қалған мақсатты - қол жетімділікті бақылауды егжей - тегжейлі қарастырамыз.

Желі шеңберінде ұйым хосттар мен құрылғыларға жеке, шешілмейтін мекен-жайларды тағайындау үшін желілік мекен-жай трансляциясын (NAT) қолдана алады, сондықтан Инфрақұрылым NAT құрылғылары арқылы өтпестен бөгде адамдарға қол жетімді болмайды [8]. Мұндай желілік мекенжайларды веб-серверлер, электрондық пошта және брандмауэрлер сияқты ішкі қызметтерді басқаруға рұқсат етілген тізімдерде пайдалануға болады [9, 10]. Алайда, мұндай мекен-жайларды сүзу қашықтағы

пайдаланушылар үшін практикалық емес, өйткені интернет-провайдерлер (ISP) өз клиенттері үшін динамикалық мекен-жайларды жиі пайдаланады. Кейбір жеткізушілер IPv4 мекенжайларының шектеулі кеңістігін динамикалық түрде тарату үшін тасымалдаушы деңгейіндегі желілік мекенжай трансляциясын (тасымалдаушы деңгейіндегі желілік мекенжай трансляциясы немесе CGN) енгізді. CGN ұялы байланыс желілерінің 92% - в қолданылды [11] 2016 жылға қарай. Кейбір жеткізушілер 5G желілерін орналастырумен 30 миллион үй желісіне CGN әсер етеді деп есептейді.

Ұйымдар мекен-жайға негізделген сүзу мүмкіндігі үшін VPN серверлерімен NAT-ты пайдаланғысы келуі мүмкін, бірақ VPN үстеме ақысы қиын болуы мүмкін. Егер ұйымдарда қашықтағы қосылатын соңғы пайдаланушының түпнұсқалығын тез және оңай тексеруге мүмкіндік беретін желі деңгейіндегі идентификатор болса, өте жақсы болар еді. Мұндай идентификаторлар қосылатын машинаның немесе желінің ықтимал заңдылығын дәлелдейтін аутентификатордың бірінші деңгейлі факторы ретінде қызмет ете алады. Содан кейін бұл факторды сервердің соңғы нүктесінде қолданба деңгейіндегі тіркелгі деректері сияқты басқа сенімді аутентификация факторларымен біріктіруге болады. Соңғы пайдаланушы да, ұйым да теріс пайдаланудың алдын алу үшін идентификаторды пайдалануға келісуі маңызды.

2.2 Қашықтан қол жеткізу VPN

Қашықтан қол жеткізу VPN. Бұл желі түрі пайдаланушыға жеке желіге қосылуға және барлық ресурстарға қол жеткізуге көмектеседі. Бұл желіге қол жеткізу түрі қауіпсіз әрі желі арқылы деректерді беру үшін кеңінен қолданылады. Қашықтан қол жеткізу VPN жалпыға қолжетімді орындарда пайдаланушылар арасында маршрутизация әдістерін пайдалана отырып, маршрутизаторлар арасында жасырын туннель құру арқылы жасалады. Қазіргі кезде технологиялар маршрутизациялық хаттамалардан бұлтқа негізделген жүйелерге ауысты. Бұлттық технологияларды пайдалану арқылы пайдаланушыларға деректерге қашықтан қол жеткізу VPN арқылы қосылудың қажеті жоқ. Бұлттық технологиялар бұлттық инфрақұрылым арқылы желіге қауіпсіз қосылуға мүмкіндік береді, бұл желі ішінде тең-теңімен қосылуды қамтамасыз етеді. VPN деректердің жоғалуына және қауіпсіздіктің жетіспеушілігіне байланысты қауіпсіздік және құпиялылық мәселелерін туғызады. Бұл мәселенің заманауи тәсілі ретінде Secure Access Service (Қауіпсіз қол жеткізу қызметі) қолданылады. Бұл қызметті пайдалану қашықтан қол жеткізу желісі арқылы қауіпсіздік пен VPN үшін жеке жол жасауды қажет етпейді. Ол пайдаланушыларға бұлттық қызметтер мен деректер орталықтарына интернет арқылы тұрақты қауіпсіздік пен құпиялылықты қамтамасыз ете отырып қол жеткізуді ұсынады.

Сайттан сайтқа қол жеткізу VPN. Сайттан сайтқа қол жеткізу VPN, сондай-ақ маршрутизатордан маршрутизаторға VPN деп аталады, үлкен желілерде маршрутизаторлар арқылы қол жеткізуге болатын биттік ақпаратты қамтиды және көбінесе ірі компаниялар мен ұйымдарда қолданылады. Бұл желілер әлемнің әртүрлі бөліктерінде орналасқан және сайттан сайтқа қол жеткізу VPN бір желі орнынан басқа желіге компьютерлерді қосу үшін желіге қол жеткізуді қамтамасыз етеді. Бұл қол жеткізу түрі негізінен екі түрлі болады: интернетке негізделген VPN, ол бір компанияның кеңселерін байланыстыру үшін қолданылады және сыртқы VPN, ол әртүрлі ұйымдардың кеңселерін қосу үшін қолданылады. Сайттан сайтқа қол жеткізу VPN арқылы компания өз қашықтағы кеңселерімен қауіпсіз желілік байланыс орнатып, ресурстарды бір желі арқылы бөлісе алады. Бұл қол жеткізу түрі жұлдыз және шұқығыш топологиясын пайдаланады. Бұл тәсіл компанияның немесе ұйымның өз деректер орталығы бар болғанда жоғары сезімтал деректер мен қолданбаларды қорғауға көмектеседі.

RIP маршрутизациясы.RIP (Routing Information Protocol) - бұл көзден алушыға дейін қорғалған арналарды орнату үшін ең кеңінен қолданылатын хаттама. Маршрутизаторлар арасында қосылымды орнату үшін маршрутизация әдістері қолданылады. RIP деректерді көзден межелі орынға беру үшін ең жақсы жолды анықтау үшін хоп санын пайдаланады. Хоп саны - бұл бастапқы және соңғы нүктелер арасындағы құрылғылар саны. RIP үшін әкімшілік мән 120-ға тең. RIP-те бір желіде ең көп дегенде 15 маршрутизаторды пайдалануға болады. Әрбір маршрутизатор желідегі басқа маршрутизаторлар арасындағы қашықтықты көрсететін маршрутизация кестесін ұстайды. RIP деректерді көзден қабылдаушыға жіберу үшін жасырын туннель құрайды, бұл деректердің ұрлануын болдырмайды.

VPN хаттамаларының төрт негізгі түрі бар:

Нүктеден нүктеге туннельдік хаттама (PPTP): PPTP - бұл қосылымды орнату үшін ең ескі тәсіл. Бұл хаттама заманауи жаңа хаттамалармен салыстырғанда көптеген қауіпсіздік мәселелеріне ие, бірақ ол сенімді әрі кеңінен қолданылады.

Екінші деңгейлі туннельдік хаттама (L2TP): L2TP PPTP-нің орнын басады. Бұл хаттама жүйеден тыс шифрлау мен құпиялылықты қамтамасыз етпейді, бірақ қауіпсіздікті арттыру үшін жиі IPsec-пен бірге қолданылады. Ол кеңінен қолданылады, жақсы жылдамдыққа ие, бірақ бір портта жұмыс істегендіктен оны оңай бұғаттауға болады.

Ашық VPN (Open VPN): Бұл ашық хаттама, ол әзірлеушілерге 2048 биттік RSA шифрлау кілті және 160 биттік SHA1 хэш алгоритмімен іске асыруға мүмкіндік береді. Ашық VPN күшті шифрлауға ие, бірақ жылдамдық жағынан баяу.

Қауіпсіз сокет туннельдік хаттама (SSTP): SSTP Microsoft операциялық жүйелерімен біріктірілгендіктен танымал. Ол 2048 биттік SSL кілтімен аутентификацияны және 256 биттік SAL кілтімен шифрлауды қолданады.

SSTP басқа VPN хаттамаларымен салыстырғанда жақсы қауіпсіздікті қамтамасыз етеді және үшінші тараптармен бұғаттау, жою немесе бұзу қиын.

VPN желісі деректерді қажетті арна арқылы тасымалдау үшін бастапқы және межелі маршрутизаторлар арасында жасырын туннель құру үшін жасырын жолды қамтиды. Алдымен біз маршрутизаторды ашамыз және командалық жолда VPN конфигурациясын орнатамыз. Бірінші командалық жол терминалы маршрутизаторды оның әдепкі IP мекенжайымен конфигурациялайды. Алдымен біз (int tunnel) командасын пайдаланып туннель құрамыз. Енді біз маршрутизаторға пайдаланушыға ғана белгілі бірегей IP мекенжайын бердік, ол VPN үшін виртуалды интерфейс жасайды. Бұл IP мекенжайлары әзірлеуші тарапынан белгілі (мысалы, 100.0.0.1 255.0.0.0), бұл бірегей IP мекенжайы. Орындау мекенжайы деректерді бастапқы нүктеден межелі нүктеге жасырын қабат арқылы өткізу үшін жеке жол жасайды. Енді біз бірінші маршрутизатор үшін se0/3/3 туннель көзін және деректер алынуы керек межелі нүктені жасадық, содан кейін терминалды жаптық. Бірегей IP мекенжайларын беру арқылы бірдей конфигурациялар екінші маршрутизаторға да қолданылады. Маршрутизатор техникасы VPN-ді интернетте бірегей IP мекенжайын пайдаланып, жасырын туннель жолы арқылы қауіпсіз қызмет провайдері ретінде жасауға көмектеседі. Бұл екі бірегей IP мекенжайы жасырын туннель арқылы виртуалды орта жасайды және деректер пакеттері, веб-шолу, HTTP және FTP барлығы осы жасырын туннель арқылы деректерді байланысты құрылғыларға бермей немесе шығармай орындалады. Егер біз мұны жасамасақ, ақпарат терминалмен байланысты барлық компьютерлерге соңғы нүктеден соңғы нүктеге дейін жіберіледі. Осылайша, Виртуалды Жеке Желі деректерді бастапқы маршрутизатордан межелі маршрутизаторға дейін жасырын туннель құру арқылы деректердің қауіпсіздігін және деректердің алдын алуды қамтамасыз етеді. Жасырын жол VPN туннелі смартфон құрылғыларын, ноутбуктерді, компьютерлерді және барлық деректерді қосады және оларды шифрлайды. Архитектура пайдаланушыға VPN қызметтеріне кіруге мүмкіндік береді. Бұл пайдаланушының IP мекенжайын жасырып, сервердегі басқалармен арадағы кедергі рөлін атқарады. (Жасырын қабат жоқ болса) деректер бір нүктеден екінші нүктеге дейін барлық межелі нүктелерге беріледі. Егер біз VPN-ді жасырын жол жасау үшін Маршрутизация ақпарат хаттамасын (RIP) пайдаланып іске асырсақ, бірегей IP мекенжайының қажетті компьютерден басқа ақпаратты жібермей деректерді беруге мүмкіндік беретінін көреміз. RIP маршрутизациясы деректерді жасырын жолмен виртуалды ортада орнатылған құрылғыларға береді. Бұл суреттер VPN-ді желіде және VPN-сыз пайдаланғандағы қажетті нәтижені көрсетеді. Әрбір нәтиже бір маршрутизатордан екінші маршрутизаторға ақпаратты VPN арқылы және VPN-сыз жібергендегі айырмашылықты көрсетеді [12].

EDP көпмүшелерінің коэффициенттерінің нақты мәнін есептеудің үш әдісі бар. Толық шамадан тыс әдістер. EDP есептеудің бірінші әдісі-кездейсоқ графиктің орындалуының толық шектелуі

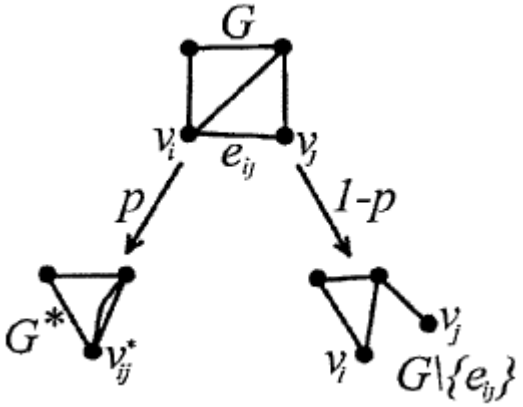
$$N(G) = \sum_{i=0}^{m} p^i (1-p)^{m-i} \sum_{j=1}^{C_m^i} N * (G_{ij}) \qquad (2.1)$$

мұндағы G_{ij}, j–G графигінен дәл I жиектерді алып тастау опциясы (ықтималдықпен жүзеге асырылады) $p_i(1-p)_{m-i}$, $N^*(G_{ij})$ - G_{ij} -дегі шыңдардың байланыссыз жұптарының саны. Негізінде, бұл формула кездейсоқ шаманың ықтималдығына көбейтілген кездейсоқ шаманың мәндерінің қосындысы ретінде анықтамасы бойынша дискретті жағдайда математикалық күтуді есептеу болып табылады.осындай мәндерді қабылдау. Әлбетте, барлық жиектердің сенімділігінің теңдігі туралы біздің болжамымызда N (G) көпмүшенің көрінісі бар p.

Тармақталу әдісі. Кеңінен танымал тармақталу әдісі (факторизация әдісі). Шын мәнінде, бұл әдіс балама ретінде tij шетінің болуы туралы гипотезаны және оның болмауы туралы гипотезаны қолданған кезде толық ықтималдық формуласын қолданудан тұрады,

$$N(G) = pN\left(G * \left(e_{ij}\right)\right) + (1-p)N(g\{e_{ij}\}) \qquad (2.2)$$

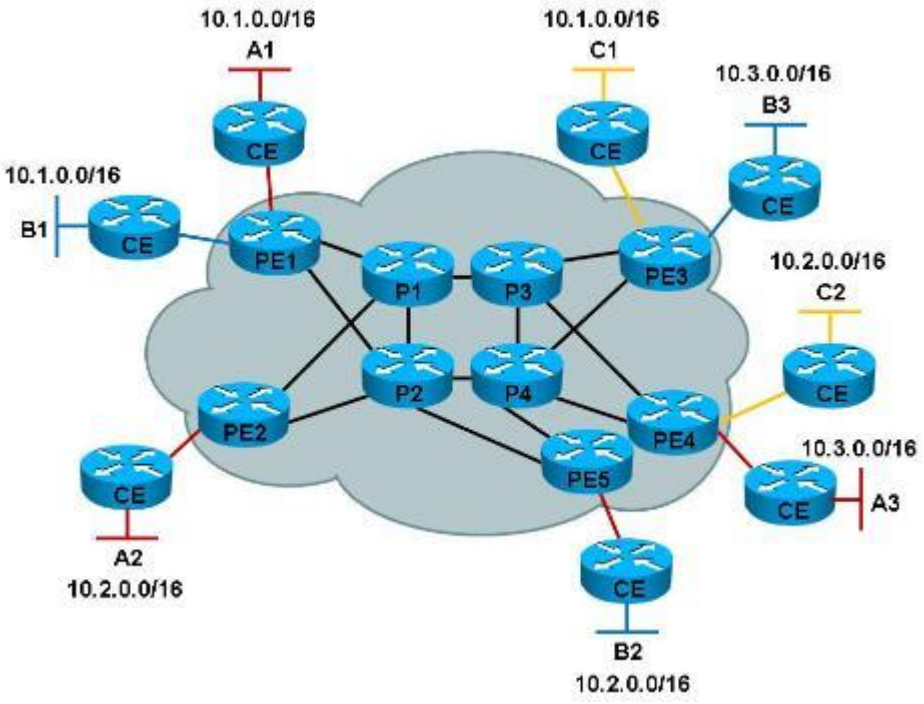
мұндағы G * (eij) - eij жиегіне тартылған график, оның іске қосылу ықтималдығы бар R, онда V * ij біріктірілген шыңының салмағы wi + wj, a G \ {eij} – Eij жиегін алып тастау арқылы G-ден алынған график. Осылайша, егер әр жиектің сенімділігі бірдей және тең болса p, онда функционалдылық (G) көпмүшеге ұқсайды p. Шыңдарды қатайту ұғымын түсіндірейік: бұл vi және VJ екі шыңының сәйкестендірілуі: бұл шыңдарды байланыстыратын ei шеті графиктен алынып тасталады, 29 VI және VJ екі шыңының орнына графикте v*i j біріктірілген шыңы пайда болады және Vi және VJ шыңдарына қатысты барлық шеттер осы шыңға айналады. Тармақталу әдісінің схемасы 2.1-суретте көрсетілген



2.1- сурет – Тармақталу әдісінің схемасы

2.3 VPN желілісінің топологиясының түрлері

VPN желісінің топологиясы (виртуалды жеке желі) деректер маршруттары мен түйіндерді бір-біріне қосу тәсілдерін қамтитын желі түйіндері арасындағы байланыстың физикалық немесе логикалық құрылымын анықтайды. Желінің өнімділігін, қауіпсіздігін және сенімділігін қамтамасыз ету үшін дұрыс топологияны таңдау өте маңызды. Технологияның дамуымен және киберкеңістіктегі қауіптердің көбеюімен VPN желісінің топологиясын оңтайландыру міндеті барған сайын маңызды бола түсуде.



2.2 - сурет – MPLS VPN топологиясы

VPN желісінің топологиясы желінің негізгі сипаттамаларына тікелей әсер етеді:өнімділік: топологияны таңдау деректер жылдамдығына және желінің жалпы өткізу қабілеттілігіне айтарлықтай әсер етуі мүмкін.

Сенімділік: жақсы жобаланған топология жоғары ақауларға төзімділікті қамтамасыз етеді және ықтимал сәтсіздік нүктелерін азайтады.

Қауіпсіздік: оңтайлы топология деректерді рұқсатсыз кіруден қорғауға көмектеседі және қол жеткізуді тиімді басқаруды қамтамасыз етеді.

Шығындар: әр түрлі топологиялар әр түрлі ресурстар мен инвестицияларды қажет етуі мүмкін, бұл желіні орналастыру мен пайдаланудың жалпы құнына әсер етеді.

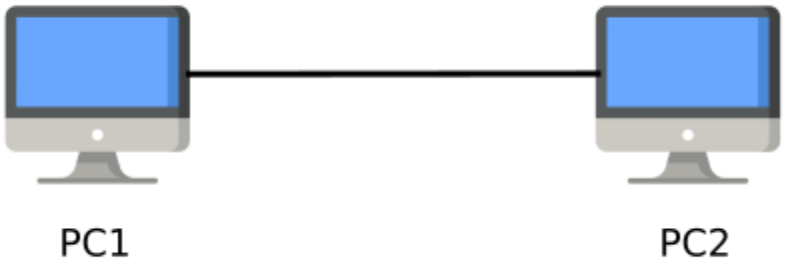
VPN топологиясының дамуы 1990 жылдары туннельдеу және деректерді шифрлау технологияларының пайда болуымен басталды. VPN желілері бастапқыда ірі компаниялардың қашықтағы кеңселерін қосу үшін пайдаланылды, бұл интернет арқылы корпоративтік ресурстарға қауіпсіз қол

жеткізуге мүмкіндік берді. Уақыт өте келе vpn топологиялары жаңа талаптар мен қиындықтарға бейімделу арқылы дамыды.Ерте шешімдер: алғашқы VPN желілері екі кеңсені қосу үшін қарапайым нүкте-нүкте топологияларын жиі қолданды.Желілердің өсуі және күрделілігі: бизнестің дамуымен және қашықтағы кеңселер мен филиалдардың көбеюімен толық байланысқан желі немесе жартылай торлы топология сияқты күрделі топологиялар қажет болды.Қазіргі гибридті шешімдер: бүгінгі таңда икемділік, өнімділік және экономикалық тиімділікті қамтамасыз ету үшін әртүрлі тәсілдердің элементтерін біріктіретін гибридті топологиялар танымал.

2.4 Нүктеден-нүктеге дейін топологиясы (Point-to-Point)

Нүкте-нүкте топологиясы (нүктеден нүктеге дейін) Виртуалды жеке желіні (VPN) ұйымдастырудың ең қарапайым және кең таралған шешімдерінің бірі болып табылады. Топологияның бұл түрі қорғалған деректерді беруді және ең аз кідірістерді қамтамасыз ететін желінің екі түйіні арасындағы тікелей байланыспен сипатталады. Бұл бөлімде біз ерекшеліктерді, артықшылықтар мен кемшіліктерді, сондай-ақ нүкте-нүкте топологиясын пайдалану мысалдары мен оңтайландыру мүмкіндіктерін егжей-тегжейлі қарастырамыз.

Нүкте-нүкте топологиясында желінің әрбір түйіні vpn туннелі арқылы басқа түйінге тікелей қосылады. Бұл туннель байланысы рұқсатсыз кіру мен ұстап қалудан қорғау үшін шифрлау мен аутентификацияны қолдана отырып, деректерді қауіпсіз тасымалдауды қамтамасыз етеді. Туннельді IPsec, SSL, L2TP және басқалары сияқты әртүрлі хаттамалар арқылы орнатуға болады.



2.3 - сурет – Нүктеден-нүктеге дейін топологиясы

Тікелей байланыс: деректер аралық түйіндер мен маршрутизаторларды айналып өтіп, екі түйін арасында тікелей тасымалданады, бұл жоғары жылдамдықты және ең аз кідірістерді қамтамасыз етеді.

Туннельді пайдалану: туннель интернет сияқты жалпыға ортақ желілер арқылы берілетін деректерді шифрлауды және қорғауды қамтамасыз етеді.

Басқарудың артықшылығы: қарапайым құрылымның арқасында желі оңай басқарылады және қызмет көрсетіледі, бұл әсіресе кішігірім ұйымдар мен пайдаланушылар үшін өте маңызды.

Орнату және басқарудың қарапайымдылығы: нүктеден нүктеге дейінгі желі күрделі конфигурацияны қажет етпейді және оны тез орналастыруға болады. Мұндай қосылысты басқару да көп күш жұмсамайды, бұл топологияны шағын және орта бизнес үшін тартымды етеді.

Жоғары жылдамдық және төмен кідірістер: түйіндер арасындағы тікелей байланыстың арқасында деректер ең аз кідірістермен беріледі, бұл әсіресе жауап беру уақытына сезімтал қолданбалар үшін маңызды.

Қауіпсіздік: VPN туннельдерін пайдалану деректерді ұстап қалудан және рұқсатсыз кіруден қорғаудың жоғары деңгейін қамтамасыз етеді, бұл құпия ақпаратты қорғау үшін маңызды.

Инфрақұрылымның минималды шығындары: нүктеден нүктеге дейінгі желіні құру үшін жабдықтар мен параметрлердің минималды мөлшері қажет, бұл орналастыру мен пайдалану шығындарын азайтады.

Шектеулі масштабтау: желідегі түйіндердің санын көбейту кезінде басқару мен конфигурацияда қиындықтар туындайды, өйткені әрбір жаңа қосылым жеке туннельді орнатуды қажет етеді.

Брондаудың болмауы: түйіндердің бірі немесе байланыс арнасы істен шыққан жағдайда, барлық байланыс жоғалады, өйткені деректерді берудің балама маршруттары жоқ.

Үлкен желілер үшін жарамсыз нұсқа: көптеген түйіндері бар үлкен желілер үшін көптеген туннельдерді орнату және басқару қиындықтарына байланысты нүкте-нүкте топологиясы тиімсіз болады.Нүкте-нүкте топологиясы қашықтағы кеңселерді немесе филиалдарды орталық кеңсеге қосу үшін корпоративтік желілерде кеңінен қолданылады. Мысалы, бас кеңседе кәсіпорын ресурстары мен қолданбаларына қауіпсіз қол жетімділікті қамтамасыз ету үшін қашықтағы кеңсемен тікелей байланыс болуы мүмкін.

А компаниясының Нью-Йоркте орталық кеңсесі және Лос-Анджелесте филиалы бар. Филиал қызметкерлерінің корпоративтік желіге қауіпсіз қол жеткізуін қамтамасыз ету үшін Нью-Йоркте нүкте-нүкте топологиясы қолданылады. Бұл интернет арқылы берілетін деректерді қорғауға және кеңселер арасында ақпараттың жылдам берілуін қамтамасыз етуге мүмкіндік береді.Жеке пайдаланушылар компьютер мен қашықтағы сервер арасында қауіпсіз байланыс жасау үшін нүктеден нүктеге дейінгі VPN қолдана алады. Бұл жеке деректерді қорғауға және интернетте жұмыс істеу кезінде құпиялылықты қамтамасыз етуге мүмкіндік береді.

2-мысал: деректерді қорғау: В пайдаланушысы Интернетке қоғамдық Wi-Fi желілері арқылы кірген кезде өз деректерін қорғағысы келеді. Ол ноутбук пен үй сервері арасында VPN нүкте-нүкте байланысын орнатады, бұл

трафикті шифрлауды және деректерді ұстап қалудан қорғауды қамтамасыз етеді.Екі сервер арасында қауіпсіз деректер алмасуды қамтамасыз ету үшін нүкте-нүкте топологиясын да пайдалануға болады. Бұл әртүрлі географиялық аймақтарда таратылған серверлері бар компанияларға қатысты.

3-мысал: серверлер арасында деректер алмасу: В компаниясында әртүрлі елдерде Екі деректер орталығы бар. Бұл орталықтардағы серверлер арасында деректерді қауіпсіз бөлісу үшін нүктеден нүктеге дейінгі VPN қолданылады, бұл деректерді ұстап қалудан қорғауға және ақпаратты берудің жоғары жылдамдығын қамтамасыз етуге мүмкіндік береді.

Хаттамалар мен технологиялар:IPsec (Internet Protocol Security): деректерді шифрлау мен аутентификациялауды қамтамасыз ететін қорғалған VPN туннельдерін жасау үшін кеңінен қолданылатын протокол.SSL (Secure Sockets Layer): клиент пен сервер арасында Қауіпсіз қосылыстар жасау үшін қолданылады, көбінесе веб-трафиктің қауіпсіздігін қамтамасыз ету үшін қолданылады.

L2TP (Layer 2 Tunneling Protocol): деректерді беру қауіпсіздігін қамтамасыз ету үшін IPsec-пен бірге жиі қолданылатын туннельдеу протоколы.Аппараттық шешімдер: VPN хабтары және vpn қолдайтын маршрутизаторлар сияқты арнайы құрылғылар қорғалған нүктеден нүктеге қосылуға мүмкіндік береді.

Бағдарламалық шешімдер: әртүрлі операциялық жүйелерде жұмыс істейтін VPN клиенттері мен серверлері арнайы жабдықты қажет етпестен VPN туннельдерін орнатуды және басқаруды қамтамасыз етеді.

Күшті шифрлауды қолдану: деректерді қорғау үшін AES-256 сияқты заманауи шифрлау алгоритмдерін қолдану.Көп факторлы аутентификация: қосылым қауіпсіздігін жақсарту үшін пайдаланушының аутентификациясының қосымша деңгейлерін қосу.Маршруттарды оңтайландыру: кідірістерді азайту және желінің өткізу қабілеттілігін жақсарту үшін оңтайлы маршруттарды орнату.QoS (қызмет сапасы) пайдалану: маңызды трафиктің басымдылығын қамтамасыз ету және желі өнімділігін арттыру үшін трафикті басқару технологияларын қолдану.

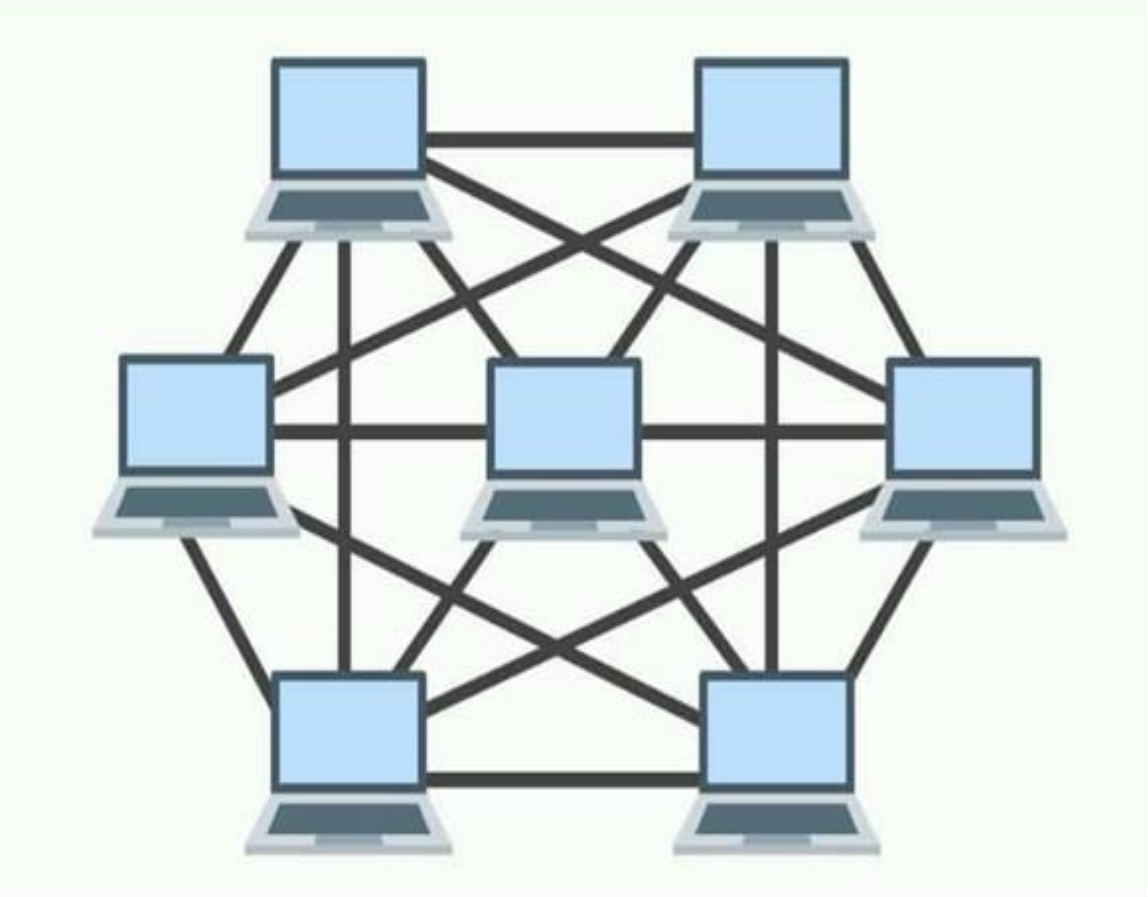
Байланыс арналарын резервтеу: негізгі арна істен шыққан жағдайда желінің үздіксіздігін қамтамасыз ету үшін резервтік арналарды пайдалану.Мониторинг және басқару: ықтимал проблемаларды анықтау және жою үшін желінің күйін үнемі бақылау және жедел басқару.

Нүкте-нүкте топологиясы vpn ұйымы үшін қарапайым және тиімді шешім болып табылады, ол ең аз шығынмен жоғары қауіпсіздік пен өнімділікті қамтамасыз етеді. Бұл түйіндердің аз санын қосу үшін өте қолайлы және деректердің сенімді берілуін қамтамасыз етеді. Алайда, түйіндер санының ұлғаюымен және желінің күрделенуімен масштабталуға және брондаудың болмауына байланысты шектеулер туындауы мүмкін. Мұндай жағдайларда оңтайлы нәтижеге жету үшін басқа, күрделі топологияларды қарастыру немесе әртүрлі тәсілдерді біріктіру қажет.

2.5 VPN-дегі «толық байланыс желісі» (толық тор) топологиясы

«Толық байланыс желісі» топологиясы (Full Mesh) виртуалды жеке желілерді (VPN) қоса алғанда, ең сенімді және өнімділігі жоғары желі құру шешімдерінің бірі болып табылады. Бұл топологияда желінің әрбір түйіні барлық басқа түйіндерге тікелей қосылған, бұл деректердің максималды қолжетімділігі мен ең аз кідірістерін қамтамасыз етеді. Бұл бөлімде Full Mesh топологиясының қалай жұмыс істейтіні, оның артықшылықтары мен кемшіліктері, сондай-ақ қолдану мысалдары мен оңтайландыру мүмкіндіктері егжей-тегжейлі қарастырылады.

Full Mesh топологиясында желінің әрбір түйіні әрбір басқа түйінмен тікелей байланысқа ие, бұл деректердің аралық түйіндер арқылы өтуін қажет етпестен ең қысқа жолмен өтуіне мүмкіндік береді. Бұл желіні өте сенімді етеді және өнімділіктің жоғары деңгейін қамтамасыз етеді, өйткені деректер аралық түйіндерде қалмайды және қосымша маршруттаудың қажеті жоқ.



2.4 - сурет – VPN-дегі «толық байланыс желісі» (толық тор) топологиясы

Максималды байланыс: әрбір түйіннің әрбір басқа түйінмен тікелей байланысы бар, бұл кідірістерді азайтады және деректер жылдамдығын арттырады.Жоғары сенімділік пен ақауларға төзімділік: бір немесе бірнеше түйіндер істен шықса да, қалған түйіндер балама маршруттарды қолдана отырып жұмысын жалғастыра алады.Аралық маршруттаудың болмауы: деректер түйіндер арасында тікелей тасымалданады, бұл маршрутизаторларға жүктемені азайтады және желінің жалпы өнімділігін арттырады.Сенімділік және ақауларға төзімділік: толық тор топологиясы түйіндер арасындағы бірнеше жолдар арқылы максималды ақауларға төзімділікті қамтамасыз етеді. Бұл бірнеше түйіндер немесе байланыс арналары істен шыққан жағдайда да желіні жалғастыруға мүмкіндік береді.Минималды кідірістер: желінің барлық түйіндері арасындағы тікелей байланыс аралық түйіндер арқылы маршруттауға байланысты кідірістерді жояды, бұл желінің жұмысын жақсартады және деректерді беруді тездетеді.Оңтайлы өткізу қабілеттілігі: әр түйіннің деректерді беру мүмкіндігі бар, бұл желінің шамадан тыс жүктелу мүмкіндігін азайтады және ақпарат алмасудың жоғары жылдамдығын қамтамасыз етеді.

Басқарудың қарапайымдылығы: жоғары ақауларға төзімділік жағдайында және күрделі маршруттаудың қажеті жоқ, мұндай желіні басқару көптеген байланыстарға қарамастан салыстырмалы түрде қарапайым болады. Орналастырудың жоғары құны: толық байланыс желісін құру үшін көптеген байланыс арналары мен жабдықтары қажет, бұл орналастыру мен пайдалану шығындарын арттырады.Орнату мен басқарудың күрделілігі: көптеген түйіндермен желіні конфигурациялау мен басқарудың күрделілігі артады, өйткені көптеген қосылымдарды конфигурациялау және қолдау қажет.Масштабтау мәселелері: түйіндердің көбеюімен қажетті қосылыстардың саны экспоненциалды түрде артады, бұл үлкен желілерді орналастыру кезінде қиындық тудыруы мүмкін.Full Mesh топологиясы жоғары сенімділік пен өнімділікті қажет ететін ірі кәсіпорын желілерінде кеңінен қолданылады. Мысалы, банктерде, сақтандыру компанияларында және үлестірілген құрылымы бар басқа ұйымдарда жұмыс үздіксіздігін қамтамасыз ету және деректердің жоғалу қаупін азайту қажет.А Банкінің әртүрлі қалаларда бірнеше ірі кеңселері бар. Full Mesh топологиясын пайдалану кеңселер арасындағы сенімді байланысты қамтамасыз етуге және қаржылық деректерді берудегі кідірістерді азайтуға мүмкіндік береді, бұл банктің жұмысы үшін өте маңызды.Деректер орталықтары (Docs) желілерінің жоғары қолжетімділігі мен сенімділігін қамтамасыз ету үшін Full Mesh топологиясын жиі пайдаланады. Бұл түйіндердің бірі істен шыққан жағдайда жүктемені тиімді бөлуге және бос уақытты азайтуға мүмкіндік береді.

2-мысал: деректер орталығы:DCD B серверлері мен сақтау түйіндерін қосу үшін толық тор топологиясын пайдаланады. Бұл бұлттық қызметтер мен виртуализацияны қолдау үшін маңызды инфрақұрылымның барлық элементтері арасында сенімді және жылдам байланыс орнатуға мүмкіндік

береді.Телекоммуникациялық компаниялар Full Mesh топологиясын өз желілерінің, әсіресе халықаралық байланыстар мен магистральдық желілерді ұйымдастыруда қол жетімділігі мен сенімділігінің жоғары деңгейін қамтамасыз ету үшін пайдаланады.В компаниясы бірнеше елдерде байланыс және Интернетке қол жеткізу қызметтерін ұсынады. Full Mesh топологиясын пайдалану клиенттерге сапалы қызмет көрсету үшін маңызды болып табылатын қызмет көрсету орталықтары арасында сенімді және жоғары жылдамдықты байланыс орнатуға мүмкіндік береді.

MPLS (Multiprotocol Label Switching): толық тор сияқты қосылым тығыздығы жоғары желілерде тиімді маршруттау мен трафикті басқаруды қамтамасыз ететін Протокол.BGP (border Gateway Protocol): маршруттарды басқаруға және ірі желілердегі түйіндер арасында ақпарат алмасуға мүмкіндік беретін маршруттау хаттамасы.OSPF (Open Shortest Path First): маршруттық ақпараттың жылдам алмасуын қамтамасыз ететін және бірнеше қосылымы бар желілерде динамикалық маршруттауды қолдайтын маршруттау протоколы.

Аппараттық маршрутизаторлар: толық торлы желілерде сенімді және тиімді трафикті бағыттауды қамтамасыз ету үшін MPLS және басқа протоколдарды қолдайтын жоғары өнімді маршрутизаторлар мен қосқыштарды пайдалану.Бағдарламалық жасақтамамен анықталған желілер (SDN): Sdn технологиялары желіні икемді басқаруға және нақты уақыттағы трафикті бағыттауды оңтайландыруға мүмкіндік береді, бұл әсіресе күрделі және ауқымды Full Mesh желілері үшін өте маңызды.QoS технологияларын пайдалану: қызмет көрсету сапасын (QoS) қолдану маңызды трафикке басымдық беруге және желіге жоғары жүктеме кезінде де жоғары сапалы қызмет көрсетуге мүмкіндік береді.Маршрутты оңтайландыру: деректер маршруттарын үнемі оңтайландыру кідірістерді азайтуға және желі өнімділігін жақсартуға мүмкіндік береді.Байланыс арналарын резервтеу: бір немесе бірнеше түйіндер істен шыққан жағдайда желінің үздіксіздігін қамтамасыз ету үшін резервтік байланыс арналары мен маршруттарын пайдалану.Бақылау және басқару: желінің күйін үнемі бақылау және жедел басқару желінің жоғары ақауларға төзімділігін сақтай отырып, мүмкін болатын мәселелерді тез анықтауға және жоюға мүмкіндік береді.Бұлтты шешімдерді қолдану: бұлтты технологияларды қолдану өнімділік пен сенімділіктің жоғары деңгейін қамтамасыз ете отырып, жабдық пен желіге техникалық қызмет көрсету шығындарын азайтуға мүмкіндік береді.Ресурстарды пайдалануды оңтайландыру: ресурстарды тиімді басқару және жабдықты пайдалануды оңтайландыру желіні орналастыру және пайдалану шығындарын азайтуға көмектеседіFull Mesh топологиясы көптеген филиалдары мен кеңселері бар ірі корпорациялар үшін өте қолайлы, олар деректермен алмасу және жұмыс үздіксіздігін қамтамасыз ету үшін сенімді және жоғары өнімді қосылымды қажет етеді.Халықаралық корпорация Г әртүрлі елдерде кеңселері бар және жаһандық операцияларды тиімді басқаруға

және деректердің жоғалу қаупін азайтуға мүмкіндік беретін бөлімшелері арасында сенімді байланыс орнату үшін Full Mesh топологиясын пайдаланады.

Телекоммуникациялық компаниялар өз клиенттеріне жоғары қол жетімділік пен деректерді беру жылдамдығын қамтамасыз ететін сенімді магистральдық желілерді құру үшін Full Mesh топологиясын жиі пайдаланады.

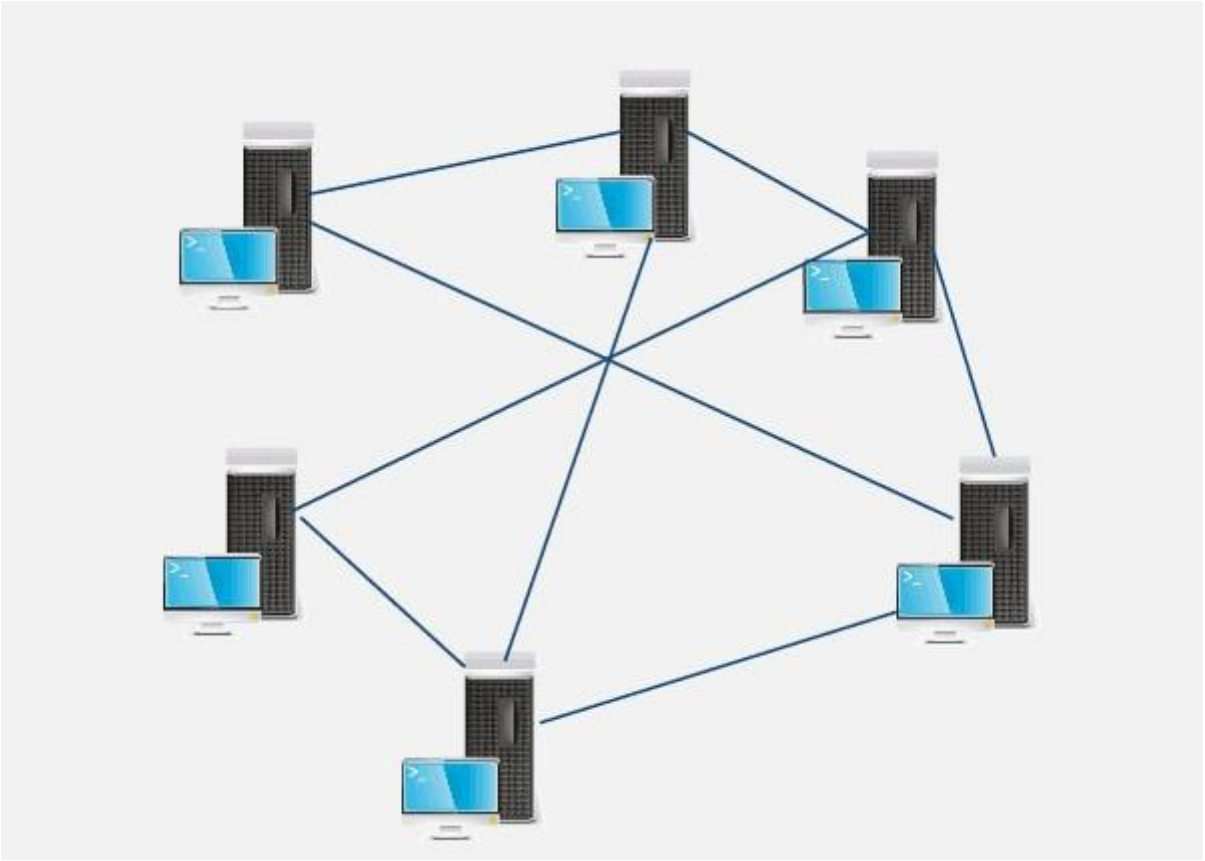
Байланыс провайдері Д өзінің халықаралық деректер орталықтары арасындағы байланысты қамтамасыз ету үшін Full Mesh топологиясын пайдаланады, бұл бүкіл әлем бойынша өз клиенттеріне жоғары сапалы байланыс және интернет қызметтерін ұсынуға мүмкіндік береді.

«Толық байланыс желісі» топологиясы (Full Mesh) сенімді және жоғары өнімді желілерді құрудың қуатты шешімі болып табылады. Ол ең жоғары қолжетімділік пен ақауларға төзімділікті қамтамасыз етеді, бұл әсіресе ірі ұйымдар мен телекоммуникациялық компаниялар үшін маңызды. Орналастыру шығындары мен басқарудың күрделілігіне қарамастан, Full Mesh жоғары сенімділікті және деректерді берудің минималды кідірістерін қажет ететін желілер үшін оңтайлы таңдау болып табылады.

2.6 VPN жүйесіндегі ішінара тор топологиясы

Ішінара торлы топология (Partial Mesh) виртуалды жеке желілерді (VPN) құрудың икемді және үнемді әдісін ұсынады. Бұл топологияда желінің кейбір түйіндерінде бірнеше басқа түйіндермен тікелей байланыстар болады, ал басқа түйіндерді аралық түйіндер арқылы қосуға болады. Бұл сенімділік, өнімділік және шығындар арасындағы оңтайлы тепе-теңдікке қол жеткізуге мүмкіндік береді, бұл ішінара торлы топологияны әртүрлі ұйымдар мен қолданбалар үшін тартымды шешім етеді.

Жартылай торлы топологияда желінің әрбір түйінінде бірнеше басқа түйіндермен тікелей байланыстар болуы мүмкін, бірақ міндетті түрде желінің әрбір түйінімен емес. Бұл желіні жобалауда икемділікті қамтамасыз етеді және нақты талаптарға байланысты әр түрлі байланыс деңгейлерін құруға мүмкіндік береді. Кейбір түйіндер орталық болуы мүмкін және басқаларға қарағанда қосылыстар көп болуы мүмкін, олар перифериялық және қосылыстар саны аз болуы мүмкін.



2.5 - сурет – VPN жүйесіндегі ішінара тор топологиясы

Қосылыстардың икемділігі: түйіндерді тікелей немесе аралық түйіндер арқылы қосуға болады, бұл топологияны нақты тапсырмалар мен жағдайларға бейімдеуге мүмкіндік береді.

Теңдестірілген байланыс: жартылай торлы топология қосылыстар саны мен оларды қолдау шығындары арасында жақсы тепе-теңдікті қамтамасыз етеді.Маршруттауды оңтайландыру: түйіндер деректерді беру үшін ең оңтайлы маршруттарды қолдана алады, бұл желінің тиімділігін арттырады.

Экономикалық тиімділік: жартылай торлы топология толық торлы топологиямен салыстырғанда аз қосылыстарды қажет етеді, бұл желіні орналастыру және техникалық қызмет көрсету шығындарын азайтады.

Дизайн икемділігі: топологияны нақты қажеттіліктер мен жағдайларға бейімдеу мүмкіндігі оны әртүрлі сценарийлерде, соның ішінде корпоративтік желілер мен телекоммуникациялық инфрақұрылымдарда қолдануға ыңғайлы етеді.Жақсартылған сенімділік: бірнеше деректер маршруттарының болуы желінің ақауларға төзімділігін арттырады, өйткені түйіндер немесе байланыс арналарының бірі істен шыққан жағдайда деректерді балама жолдармен беруге болады.

Жақсартылған өнімділік: маршруттарды оңтайландыру және ең тиімді деректер жолдарын пайдалану желінің жалпы өнімділігін арттыруға мүмкіндік береді.

Басқарудың күрделілігі: толық торлы топологиямен салыстырғанда күрделілігі аз болғанымен, ішінара торлы топология тиімді жұмысты қамтамасыз ету үшін әлі де мұқият басқару мен конфигурацияны қажет етеді.

Ықтимал кедергілер: көптеген қосылыстары бар түйіндер, егер олардың өткізу қабілеттілігі деректердің бүкіл көлемін өңдеуге жеткіліксіз болса, тар болуы мүмкін.

Негізгі түйіндерге тәуелділік: көптеген байланыстары бар негізгі түйіннің істен шығуы бүкіл желіде маңызды мәселелерге әкелуі мүмкін.

Ішінара торлы топология корпоративті желілерде кеңінен қолданылады, мұнда әр түрлі филиалдар мен кеңселер арасында сенімді және икемді байланыс қажет.

А компаниясының әртүрлі қалаларда бірнеше кеңселері бар. Кеңселер арасындағы сенімді байланысты қамтамасыз ету үшін жартылай торлы топология қолданылады. Орталық кеңседе негізгі деректер маршруттарын қамтамасыз ететін байланыстар көп, ал филиалдар тек жақын орналасқан түйіндерге қосылады, бұл шығындарды азайтады және желіні басқаруды жеңілдетеді.

Телекоммуникациялық компанияларда ішінара торлы топология сенімділік пен экономикалық тиімділік арасындағы тепе-теңдікті қамтамасыз ететін аймақтық және Ұлттық желілерді құру үшін қолданылады.В провайдері бір аймақта байланыс қызметтерін ұсынады және олардың қатысу нүктелері арасындағы байланысты қамтамасыз ету үшін ішінара торлы топологияны пайдаланады. Орталық түйіндерде трафиктің негізгі бағыттарын қамтамасыз ететін байланыстар көп, ал перифериялық түйіндер жақын маңдағы орталық түйіндерге қосылған.

Деректер орталықтарында ішінара торлы топология ресурстар мен деректерді сенімді және тиімді бөлуді қамтамасыз ететін серверлер мен сақтау түйіндерін қосу үшін қолданылады.DCOD өзінің серверлері мен сақтау түйіндерін қосу үшін ішінара торлы топологияны қолданады. Негізгі серверлерде бірнеше басқа түйіндермен тікелей байланыстар бар, бұл жүйенің жоғары өнімділігі мен сенімділігін қамтамасыз етеді.

BGP (border Gateway Protocol): маршруттарды басқаруға және ірі және күрделі желілердегі түйіндер арасында ақпарат алмасуға мүмкіндік беретін маршруттау хаттамасы.

OSPF (Open Shortest Path First): маршруттық ақпаратпен жылдам алмасуды және бірнеше қосылымы бар желілерде динамикалық маршруттауды қолдауды қамтамасыз ететін маршруттау протоколы.

EIGRP (Enhanced Interior Gateway Routing Protocol): маршруттық ақпаратпен алмасу және желіде деректерді тиімді бағыттауды қамтамасыз ету үшін қолданылатын маршруттау хаттамасы.

Аппараттық маршрутизаторлар мен қосқыштар: өнімділігі жоғары маршрутизаторлар мен қосқыштарды пайдалану трафикті тиімді басқаруға

және жартылай торлы топологияда сенімді маршруттауды қамтамасыз етуге мүмкіндік береді.

Бағдарламалық жасақтамамен анықталған желілер (SDN): Sdn технологиялары желіні икемді басқаруға және нақты уақыттағы трафикті бағыттауды оңтайландыруға мүмкіндік береді, бұл ішінара торлы топологиясы бар күрделі және ауқымды желілер үшін өте маңызды.

QoS технологияларын пайдалану: қызмет көрсету сапасын (QoS) қолдану маңызды трафикке басымдық беруге және желіге жоғары жүктеме кезінде де жоғары сапалы қызмет көрсетуге мүмкіндік береді.

Маршрутты оңтайландыру: деректер маршруттарын үнемі оңтайландыру кідірістерді азайтуға және желі өнімділігін жақсартуға мүмкіндік береді.

Негізгі түйіндерді резервтеу: резервтік түйіндер мен байланыс арналарын пайдалану желінің сенімділігін арттыруға және негізгі түйіндер істен шыққан жағдайда оның үздіксіз жұмысын қамтамасыз етуге мүмкіндік береді.

Бақылау және басқару: желінің күйін үнемі бақылау және жедел басқару желінің жоғары ақауларға төзімділігін сақтай отырып, мүмкін болатын мәселелерді тез анықтауға және жоюға мүмкіндік береді.

Ресурстарды пайдалануды оңтайландыру: ресурстарды тиімді басқару және жабдықты пайдалануды оңтайландыру желіні орналастыру және пайдалану шығындарын азайтуға көмектеседі.

Бұлтты шешімдерді қолдану: бұлтты технологияларды қолдану өнімділік пен сенімділіктің жоғары деңгейін қамтамасыз ете отырып, жабдық пен желіге техникалық қызмет көрсету шығындарын азайтуға мүмкіндік береді.

Жартылай торлы топология шағын және орта бизнес үшін өте қолайлы, мұнда әртүрлі кеңселер мен филиалдар арасында сенімді және үнемді байланыс болуы керек.G компаниясының әртүрлі қалаларда бірнеше кеңселері мен өндірістік нысандары бар. Жартылай торлы топологияны пайдалану кеңселер мен өндіріс орындары арасында сенімді және үнемді байланыс орнатуға мүмкіндік береді, бұл желіні орналастыру мен техникалық қызмет көрсету шығындарын азайтады.

Телекоммуникациялық компаниялар мен интернет-провайдерлер түйіндер мен клиенттердің кіру нүктелері арасында сенімді және икемді байланыс орнату үшін жартылай торлы топологияны қолданады.Интернет-провайдер Д өзінің аймақтық желісін құру үшін ішінара торлы топологияны қолданады. Орталық түйіндерде негізгі деректер маршруттарын қамтамасыз ететін байланыстар көп, ал клиенттің кіру нүктелері жақын маңдағы орталық түйіндерге қосылған.

Ішінара торлы топология ресурстар мен деректерді сенімді және тиімді бөлуді қамтамасыз ету үшін деректер орталықтарында және бұлттық қызметтерде қолданылады.

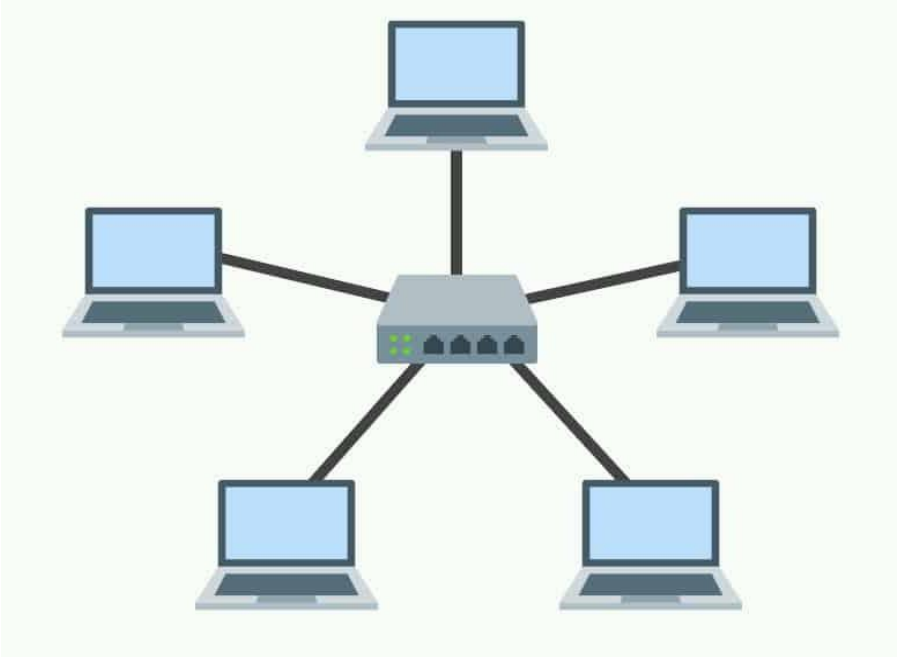
Бұлтты провайдер Е өзінің деректер орталықтары мен сақтау түйіндерін қосу үшін жартылай торлы топологияны пайдаланады. Негізгі түйіндер жүйенің жоғары өнімділігі мен сенімділігін қамтамасыз ететін бірнеше басқа түйіндермен тікелей байланыстарға ие.

Жартылай торлы топология (Partial Mesh) сенімді және жоғары өнімді желілерді құру үшін икемді және үнемді шешім болып табылады. Бұл қосылыстар саны, оларды қолдау шығындары және желінің өнімділігі арасындағы тепе-теңдікке қол жеткізуге мүмкіндік береді. Ішінара торлы топология әртүрлі сценарийлерде, соның ішінде корпоративтік желілерде, телекоммуникациялық инфрақұрылымдарда және деректер орталықтарында кеңінен қолданылады, бұл желінің оңтайлы сенімділігі мен тиімділігін қамтамасыз етеді.

2.7 «Жұлдыз» топологиясы (Star)

«Жұлдыз» топологиясы (Star) - виртуалды жеке желілерді (VPN) қоса алғанда, ең танымал және кеңінен қолданылатын желілік схемалардың бірі. Бұл топологияда барлық перифериялық түйіндер хаб рөлін атқаратын және желінің әртүрлі бөліктері арасындағы байланысты қамтамасыз ететін бір орталық түйінге қосылған. «Жұлдыз» топологиясы қарапайым және тиімді, сонымен қатар ақауларға төзімділігі жоғары, бұл оны көптеген қосымшалар, соның ішінде корпоративті желілер мен телекоммуникациялық жүйелер үшін өте қолайлы етеді.

Жұлдыз топологиясында желінің барлық түйіндері бір орталық түйінге (хаб, маршрутизатор немесе сервер) қосылады. Орталық түйін трафикті басқаруда шешуші рөл атқарады және қосылған құрылғылар арасында деректерді тасымалдауды қамтамасыз етеді. Барлық деректер алмасулары осы орталық түйін арқылы жүреді, бұл желіні бағыттау мен басқаруды жеңілдетеді.



2.6 - сурет – «Жұлдыз» топологиясы (Star)

Орталықтандырылған басқару: орталық түйін деректерді беруді басқарады және қосылымдарды басқарады, бұл желіні басқаруды жеңілдетеді.

Орнату және басқару оңай: «жұлдыз» топологиясы оңай реттеледі және басқарылады, өйткені барлық түйіндер бір орталық түйінге қосылған.

Жоғары сенімділік: перифериялық түйіндердің бірі істен шыққан жағдайда, Желі жұмысын жалғастырады, өйткені қалған түйіндер орталық түйінге қосылған күйінде қалады.

Орнату және басқару оңай: жаңа түйіндерді қосу немесе ескілерін жою орталық түйін арқылы жүзеге асырылады, бұл желіні орнату және басқару процесін жеңілдетеді.

Жоғары ақауларға төзімділік: перифериялық түйіндердің бірі істен шыққан жағдайда, қалған түйіндер жұмысын жалғастырады, өйткені олардың орталық түйінге қосылуы белсенді болып қалады.

Кеңейтудің қарапайымдылығы: желіге жаңа түйіндерді қосу желі құрылымында айтарлықтай өзгерістерді қажет етпейді, өйткені олар жай ғана орталық түйінге қосылады.

Тиімді трафикті басқару: орталық түйін трафикті тиімді басқара алады және желі өнімділігін жақсартатын деректер маршруттарын оңтайландырады.

Ақаулықтардың қарапайым диагностикасы: желінің дұрыс жұмыс істемеуі оңай диагноз қойылады, өйткені проблемалар орталық түйінде немесе белгілі бір перифериялық түйінде орналасады.

Бір сәтсіздік нүктесі: орталық түйін желінің маңызды нүктесі болып табылады. Егер ол істен шықса, бүкіл желі жұмысын тоқтатуы мүмкін.

Шектеулі масштабтау: қосылатын түйіндер санының артуымен орталық түйінге жүктеме артады, бұл оның шамадан тыс жүктелуіне және желі өнімділігінің нашарлауына әкелуі мүмкін.

Орталық түйінге қойылатын жоғары талаптар: орталық түйін трафиктің үлкен көлемін өңдеуге және желінің әрбір Түйініне сенімді қосылуды «Жұлдыз» топологиясы әртүрлі бөлімшелер мен филиалдар арасында орталықтандырылған басқару мен тиімді байланысты қажет ететін корпоративтік желілерде кеңінен қолданылады.

А компаниясында бірнеше бөлім бар, олардың әрқайсысы орталық серверге «жұлдыз»топологиясы арқылы қосылған. Бұл орталықтандырылған деректерді басқаруды және компанияның әртүрлі бөлімшелері арасындағы тиімді өзара әрекеттесуді қамтамасыз етуге мүмкіндік береді.

Телекоммуникациялық компаниялар орталық түйіндер мен клиенттердің кіру нүктелері арасындағы сенімді және жоғары жылдамдықты байланысты қамтамасыз ету үшін «жұлдыз» топологиясын қолданады.

В провайдері клиенттің кіру нүктелерін орталық маршрутизаторға қосу үшін «жұлдыз»топологиясын қолданады. Бұл трафикті тиімді басқаруды және клиенттер үшін деректерді берудің жоғары жылдамдығын қамтамасыз етеді.

Деректер орталықтарында «жұлдыз» топологиясы серверлер мен сақтау түйіндерін орталық қосқышқа немесе маршрутизаторға қосу үшін пайдаланылады, бұл орталықтандырылған басқару мен сенімді қосылымды қамтамасыз етеді.

DCOD өзінің серверлері мен сақтау түйіндерін орталық қосқышқа қосу үшін «жұлдыз» топологиясын пайдаланады, бұл ресурстарды орталықтан басқаруға және деректерді бағыттауды оңтайландыруға мүмкіндік береді.

Ethernet: деректерді берудің жоғары жылдамдығы мен сенімділігін қамтамасыз ететін орталық түйін мен перифериялық түйіндер арасында сымды қосылыстар жасау үшін қолданылады.

Wi-Fi: сымсыз қосылымдарды жасау үшін қолданылады, бұл сымды түрде қосылу қиын мобильді құрылғылар мен түйіндерге ыңғайлы.

MPLS (Multiprotocol Label Switching): «жұлдыз» топологиясы бар ірі желілерде трафикті тиімді бағыттау және басқару үшін қолданылады.

Маршрутизаторлар мен қосқыштар: орталық түйінде өнімділігі жоғары маршрутизаторлар мен қосқыштарды пайдалану трафикті тиімді басқаруға және әрбір перифериялық түйінмен сенімді байланыс орнатуға мүмкіндік береді.Бұлтты шешімдер: бұлтты технологияларды қолдану желіні орталықтан басқаруға және оны масштабтау мен конфигурациялауда икемділікке мүмкіндік береді.Бағдарламалық жасақтамамен анықталған желілер (SDN): Sdn технологиялары желіні орталықтан басқаруға және нақты уақыттағы трафикті бағыттауды оңтайландыруға мүмкіндік береді, бұл әсіресе жұлдыз топологиясы бар күрделі және ауқымды желілер үшін өте маңызды.

Сапалы жабдықты пайдалану: орталық түйінде жоғары өнімді маршрутизаторлар мен қосқыштарды қолдану өткізу қабілеттілігін арттыруға

және желінің жалпы өнімділігін жақсартуға мүмкіндік береді.Маршруттарды оңтайландыру: орталық түйін арқылы деректерді берудің оңтайлы маршруттарын орнату кідірістерді азайтуға және желінің тиімділігін арттыруға мүмкіндік береді.Орталық түйінді резервтеу: резервтік орталық түйіндерді пайдалану негізгі түйін істен шыққан жағдайда желінің үздіксіздігін қамтамасыз етеді. Бақылау және басқару: желінің күйін үнемі бақылау және жедел басқару желінің жоғары ақауларға төзімділігін сақтай отырып, мүмкін болатын мәселелерді тез анықтауға және жоюға мүмкіндік береді.Ресурстарды пайдалануды оңтайландыру: ресурстарды тиімді басқару және жабдықты пайдалануды оңтайландыру желіні орналастыру және пайдалану шығындарын азайтуға көмектеседі.

Бұлтты шешімдерді қолдану: бұлтты технологияларды қолдану өнімділік пен сенімділіктің жоғары деңгейін қамтамасыз ете отырып, жабдық пен желіге техникалық қызмет көрсету шығындарын азайтуға мүмкіндік береді.«Жұлдыз» топологиясы шағын және орта бизнес үшін өте қолайлы, мұнда әртүрлі кеңселер мен филиалдар арасында орталықтандырылған басқару және тиімді байланыс қажет.G компаниясы өзінің кеңселері мен филиалдарын орталық серверге қосу үшін «жұлдыз» топологиясын пайдаланады, бұл деректерді орталықтан басқаруға және бөлімшелер арасында тиімді өзара әрекеттесуге мүмкіндік береді.Телекоммуникациялық компаниялар мен интернет-провайдерлер өздерінің түйіндері мен клиенттерге кіру нүктелері арасында сенімді және жоғары жылдамдықты қосылуды қамтамасыз ету үшін «жұлдыз» топологиясын қолданады.

Интернет-провайдер Д клиенттердің кіру нүктелерін орталық маршрутизаторға қосу үшін «жұлдыз» топологиясын қолданады, бұл трафикті тиімді басқаруға және клиенттер үшін жылдам деректер жылдамдығына мүмкіндік береді.«Жұлдыз» топологиясы серверлер мен сақтау түйіндері арасындағы сенімді және тиімді байланысты қамтамасыз ету үшін деректер орталықтарында және бұлттық қызметтерде қолданылады.

Бұлтты провайдер е өзінің серверлері мен сақтау түйіндерін орталық қосқышқа қосу үшін «жұлдыз» топологиясын пайдаланады, бұл ресурстарды орталықтан басқаруға және деректерді бағыттауды оңтайландыруға мүмкіндік береді.«Жұлдыз» топологиясы (Star) сенімді және жоғары өнімді желілерді құрудың қарапайым және тиімді шешімін ұсынады. Ол орталықтандырылған басқаруды, жоғары ақауларға төзімділікті және кеңейтуді жеңілдетеді, бұл оны корпоративтік желілерді, телекоммуникациялық инфрақұрылымдарды және деректер орталықтарын қоса алғанда, әртүрлі пайдалану жағдайлары үшін өте қолайлы етеді. «Жұлдыз» топологиясы желінің жоғары өнімділігі мен сенімділігіне оны орналастыру мен қызмет көрсетудің салыстырмалы түрде төмен шығындарымен қол жеткізуге мүмкіндік береді.

2.8 VPN желілеріндегі гибридті топологиялар

VPN желілеріндегі гибридті топологиялар нүкте-нүкте, толық байланыс желісі, тор топологиясы және Жұлдыз топологиясы сияқты желі топологияларының екі немесе одан да көп негізгі түрлерінің тіркесімі болып табылады. Бұл гибридті схемалар өнімділік, сенімділік, шығындар және белгілі бір vpn желісінің басқа талаптары арасындағы оңтайлы тепе-теңдікті қамтамасыз ету үшін жасалуы мүмкін.

VPN желілеріндегі гибридті топологиялар оңтайлы инфрақұрылымды құру үшін топология түрлерінің әртүрлі комбинацияларын пайдаланады. Мысалы, біріктіруге болады нүкте-нүкте оңтайлы өнімділік пен сенімділікті қамтамасыз ету үшін торлы немесе жұлдыз тәрізді топологиясы бар кейбір түйіндер арасындағы байланыс.

Гибридті топологиялар желі құрылымын желілік инфрақұрылымның нақты талаптары мен шарттарына бейімдеуге мүмкіндік береді. Бұл нақты тапсырмалар мен пайдалану жағдайлары үшін оңтайландырылған гибридті схемаларды жасауға мүмкіндік береді.

Гибридті схемаларда топологияның әртүрлі түрлерін біріктіру vpn желісінің икемділігі мен ауқымдылығын арттыруға мүмкіндік береді. Бұл желіні Бизнестің өзгеретін талаптарына бейімдеуге және қажет болған жағдайда оны кеңейтуге мүмкіндік береді.Өнімділік пен сенімділіктің оңтайлы үйлесімі: гибридті топологиялар оңтайлы өнімділік пен сенімділікті қамтамасыз ету үшін әртүрлі желі түрлерін біріктіруге мүмкіндік береді.Икемділік және масштабтау: гибридті схемалар жоғары икемділік пен масштабтауды қамтамасыз етеді, бұл желіні Бизнестің өзгеретін талаптарына бейімдеуге мүмкіндік береді.Нақты жағдайларға бейімделу: гибридті топологиялар желілік инфрақұрылымның нақты шарттары мен талаптары үшін оңтайландырылған желілік схемаларды құруға мүмкіндік береді.

Дизайн мен теңшеудің күрделілігі: гибридті топологияларды жобалау және конфигурациялау қиын болуы мүмкін, себебі қосылыстардың әртүрлі түрлерін және олардың өзара әрекеттесуін ескеру қажет.

Жабдықтар мен қолдаудың қымбаттауы: гибридті желілік схемаларды құру және қолдау қосымша жабдық пен техникалық қызмет көрсету шығындарын талап етуі мүмкін.

Ықтимал үйлесімділік мәселелері: гибридті схемаларда әртүрлі желі түрлерін пайдалану әртүрлі құрылғылар мен протоколдар арасында үйлесімділік мәселелерін тудыруы мүмкін.

Көптеген кәсіпорындар өздерінің корпоративтік желілерін құру үшін гибридті топологияларды пайдаланады. Мысалы, біріктіруге болады нүкте-нүкте жоғары өнімділік пен сенімділікті қамтамасыз ету үшін әр кеңсенің ішіндегі жұлдыз тәрізді топологиясы бар кеңселер арасындағы байланыс.

Бұлтты желілер бұлтты қызметтерді жергілікті бизнес желілерімен байланыстыру үшін гибридті топологияларды жиі пайдаланады. Мысалы,

жоғары өнімділік пен қауіпсіздікті қамтамасыз ету үшін желіні бұлттық провайдер серверлері арасындағы толық байланыспен кәсіпорын ішіндегі жұлдыз тәрізді топологиямен біріктіруге болады.

Интернет-провайдерлер өз желілерін басқа провайдерлермен және соңғы пайдаланушылармен байланыстыру үшін гибридті топологияларды жиі пайдаланады. Мысалы, жоғары өнімділік пен қызметтердің қолжетімділігін қамтамасыз ету үшін желіні әртүрлі провайдер түйіндері арасындағы нүктеден нүктеге қосылымдармен біріктіруге болады.

Гибридті топологиялар желі құрылымын желілік инфрақұрылымның нақты қажеттіліктері мен жағдайларына бейімдеуге мүмкіндік беретін VPN желілерін құрудың тиімді әдісін ұсынады. Нүкте-нүкте, толық байланыс желісі, тор топологиясы және Жұлдыз топологиясы сияқты топологиялардың әртүрлі түрлерін біріктіру арқылы желінің өнімділігі, сенімділігі, құны және икемділігі арасындағы оңтайлы тепе-теңдікке қол жеткізуге болады.

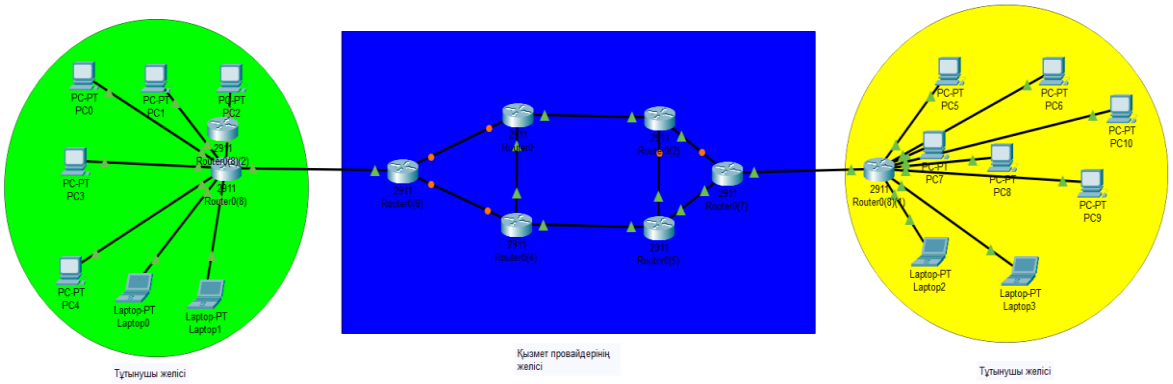
Гибридті топологиялар жоғары икемділік пен масштабталуды қамтамасыз етеді, бұл бизнестің өзгеретін талаптарына тиімді бейімделе алатын желілік схемаларды құруға мүмкіндік береді. Олар сондай-ақ белгілі бір жағдайлар мен пайдалану жағдайлары үшін желі құрылымын оңтайландыруға мүмкіндік береді, бұл оның тиімділігі мен өнімділігін арттырады.

Барлық артықшылықтарға қарамастан, гибридті топологияларды жобалау және конфигурациялау қиын болуы мүмкін және қосымша жабдық пен қолдау шығындарын қажет етуі мүмкін. Сонымен қатар, гибридті тізбектерде әртүрлі желі түрлерін пайдалану үйлесімділік пен басқару мәселелерін тудыруы мүмкін.

Тұтастай алғанда, vpn желілеріндегі гибридті топологиялар бизнестің әртүрлі қажеттіліктерін тиімді қолдай алатын және пайдаланушылар үшін қызметтің жоғары деңгейін қамтамасыз ете алатын сенімді, икемді және өнімділігі жоғары желілік инфрақұрылымдарды құрудың қуатты құралы болып табылады.

3 Эксперименттік бөлім

MPLS (Multiprotocol Label Switching) желілері ресурстарды тиімді бөлуге, жоғары сапалы қызмет көрсетуге (QoS), ең аз кідірістерге және шамадан тыс жүктемелердің алдын алуға көмектесетін кезек пен трафикті басқарудың әртүрлі алгоритмдерін пайдаланады. Негізгі алгоритмдерді толығырақ қарастырайық: салмақты кездейсоқ ерте анықтау (WRED), Class-Based weighted Fair Queuing (CBWFQ), Weighted Fair Queuing (WFQ) және Committed Access Rate (CAR). Осы алгоритмдерді тексеретін желі келесі 3.1 - суретте көрсетілген.



3.1 - сурет – MPLS VPN желісі Cisco Packet Tracer бағдарламасында

3.1 Weighted Random Early Detection (WRED)

Weighted Random Early Detection (WRED) – бұл әр түрлі трафик кластары үшін салмақ коэффициенттерін қолдану арқылы стандартты Random Early Detection (RED) мүмкіндіктерін кеңейтетін кезекті басқару алгоритмі. WRED шамадан тыс жүктемені болдырмау және буферді икемді басқаруды қамтамасыз ету үшін қолданылады, бұл әртүрлі трафик кластарына пакеттерді қалпына келтірудің әртүрлі ықтималдығына мүмкіндік береді [13].

Трафиктің жіктелуі: WRED QoS белгілеріне негізделген трафикті жіктейді(мысалы, DSCP-Differentiated Services Code Point).Шекті анықтау: трафиктің әр класы үшін әр түрлі шекті мәндер орнатылады, оған жеткенде пакеттерді қалпына келтіру басталады.Таразыны қолдану: трафиктің басымдығы мен класына байланысты әр ағынға белгілі бір салмақ беріледі. Жоғары басымдықты Трафик пакеттерді қалпына келтіру үшін жоғары шектерге ие, бұл олардың қалпына келу мүмкіндігін азайтады.

Пакетті қалпына келтіру: кезек белгілі бір шекті деңгейге жеткенде, WRED буфердің шамадан тыс жүктелуіне жол бермеу үшін пакеттерді белгілі

бір ықтималдықпен қалпына келтіре бастайды.Икемділік: әртүрлі басымдықтары бар әртүрлі трафик кластарын қолдау.Шамадан тыс жүктеменің алдын алу: деректер ағынын реттеу арқылы шамадан тыс жүктемені ерте анықтау және алдын алу.

QoS қолдауы: басым трафикке көбірек ресурстар алуға мүмкіндік беретін жақсартылған QoS қолдауы.Желілерде MPLS WRED ресурстарды тиімді бөлуді және шамадан тыс жүктемелердің алдын алуды қамтамасыз ететін әртүрлі техникалық қызмет көрсету кластарын (CoS) қолдайтын түйіндердегі кезектерді басқару үшін қолданылады.

Келесі кестеде WRED – алгоритмінің жұмысының нәтижесі кесте түрінде беріледі.

Кесте 3.1 – C++ бағдарламалау тіліндегі WRED алгоритмінің нәтижесі

Кезек	Басымдық	Өлшем	Күйі	Кезек өлшемі
1	1	100	Қабылданды	100
1	1	50	Қабылданды	150
1	1	75	Қабылданды	225
1	1	25	Қабылданды	250
2	1	50	Қабылданды	50
2	2	95	Қабылданды	145
2	2	40	Қабылданды	185
2	2	70	Қабылданды	255
3	2	20	Қабылданды	20
3	2	45	Қабылданды	65
3	3	115	Қабылданды	180
4	3	90	Қабылданды	90
4	3	65	Қабылданды	155
4	3	40	Қабылданды	195
4	3	15	Қабылданды	210
4	3	30	Қабылданды	240
5	4	35	Қабылданды	35
5	4	60	Қабылданды	95
5	4	70	Қабылданды	165
5	4	85	Қабылданды	250
6	4	25	Қабылданды	25
6	4	110	Қабылданды	135
6	5	55	Қабылданды	190
6	5	30	Қабылданды	220
7	5	80	Қабылданды	80
7	5	60	Қабылданды	140
7	5	105	Қабылданды	245
8	5	20	Қабылданды	20

3.2 Class-Based Weighted Fair Queuing (CBWFQ)

Class-Based Weighted Fair Queuing (CBWFQ) – бұл әр түрлі трафик кластары арасында ресурстарды олардың салмағына қарай әділ бөлуді қамтамасыз ететін кезекті басқару алгоритмі. CBWFQ әкімшіге маңызды трафик үшін қажетті қызмет сапасын қамтамасыз ете отырып, трафиктің әр класы үшін өткізу қабілеттілігін реттеуге мүмкіндік береді [14].

Трафиктің жіктелуі: Трафик QoS белгілері, IP мекенжайлары, порттар және басқа критерийлер негізінде сыныптарға бөлінеді.
Таразының мақсаты: әр кезекке өткізу қабілеттілігінің үлесін анықтайтын салмақ беріледі.Кезекті өңдеу: кезектер олардың салмағына пропорционалды түрде өңделеді, бұл ресурстарды әділ бөлуді және QoS қолдауын қамтамасыз етеді.

CBWFQ артықшылықтары: ресурстарды басқарудағы икемділік: трафиктің әр класы үшін өткізу қабілеттілігін реттеу мүмкіндігі.Әділдік: ресурстарды әр түрлі трафик кластары арасында олардың басымдылығына қарай біркелкі бөлу.
QoS қолдауы: трафиктің әр класы үшін қажетті қызмет деңгейін қамтамасыз етеді.

MPLS CBWFQ маршрутизаторлар мен коммутаторлардағы кезектерді басқару үшін қолданылады, әр түрлі трафик кластары үшін өткізу қабілеттілігі мен QoS қолдауын әділ бөлуді қамтамасыз етеді.Келесі кестеде WRED – алгоритмінің жұмысының нәтижесі кесте түрінде беріледі.

Кесте 3.2 – C++ бағдарламалау тіліндегі CBWFQ алгоритмінің нәтижесі

Өңдеу класы	Өңделген пакеттер
Өңдеу класы 1	0
Өңдеу класы 2	1 2
Өңдеу класы 3	3 8
Өңдеу класы 4	5 6 7
Өңдеу класы 1	4
Өңдеу класы 2	9
Трафик класы	
Трафик класы 1	2
Трафик класы 2	3
Трафик класы 3	2
Трафик класы 4	3

3.3 Weighted Fair Queuing (WFQ)

Weighted Fair Queuing (WFQ) – бұл әр түрлі трафик ағындары арасында өткізу қабілеттілігін олардың салмағына қарай бөлетін кезекті басқару алгоритмі. WFQ ресурстарды әділ бөлуді және әрбір ағын үшін, әсіресе жоғары басымдықты трафик үшін ең аз кідірістерді қамтамасыз етеді [15].

Трафикті бөлу: Трафик ағындарға бөлінеді және бөлек кезектерге орналастырылады.Таразының мақсаты: әр кезекке өткізу қабілеттілігінің басымдығы мен үлесін анықтайтын салмақ беріледі.Кезектерді өңдеу: кезектер олардың салмағына пропорционалды түрде өңделеді, бұл ресурстардың біркелкі бөлінуін және басым трафик үшін ең аз кідірістерді қамтамасыз етеді.Ресурстарды әділ бөлу: өткізу қабілеттілігін олардың салмағына қарай әр түрлі ағындар арасында біркелкі бөлу.Минималды кідірістер: жоғары басымдықты трафик үшін төмен кідірістер.QoS қолдауы: әрбір ағын үшін қажетті қызмет деңгейін қамтамасыз ету.

The MPLS WFQ әр түрлі трафик түрлері үшін өткізу қабілеттілігін әділ бөлуді және QoS қолдауын қамтамасыз ететін желі түйіндеріндегі кезектерді басқару үшін қолданылады.

Кесте 3.3 – C++ бағдарламалау тіліндегі WFQ алгоритмінің нәтижесі

Уақыт	Әрекет	Ағын	Пакет идентификаторы
25	Пакетті өңдеу	3	4
35	Пакетті өңдеу	1	1
55	Пакетті өңдеу	1	2
70	Пакетті өңдеу	2	3
100	Пакетті өңдеу	2	5

3.4 Committed Access Rate (CAR)

Committed Access Rate (CAR) – әртүрлі трафик ағындары үшін деректер жылдамдығын басқаруға және шектеуге мүмкіндік беретін трафикті басқару механизмі. CAR трафикті саясаттандыруды қамтамасыз етеді және өткізу қабілеттілігіне шектеулер қою арқылы шамадан тыс жүктемелердің алдын алады [16].

Трафиктің жіктелуі: Трафик IP мекенжайлары, порттар, QoS белгілері және басқалары сияқты әртүрлі параметрлер бойынша жіктеледі.Лимиттерді орнату: трафиктің әр класы үшін деректерді беру жылдамдығына (бит жылдамдығына) шек қойылады.Саясаттандыру: белгіленген шектеулерден асатын трафикті қалпына келтіруге немесе одан әрі төмен басымдықты өңдеу үшін белгілеуге болады.Трафикті қалыптастыру: артық пакеттер кешіктіріліп, кейінірек ең жоғары жүктемелерді тегістеу үшін жіберілуі мүмкін.

Трафик жылдамдығын басқару: әртүрлі трафик ағындары үшін деректер жылдамдығын тиімді басқару.Шамадан тыс жүктемелердің алдын алу: шамадан тыс жүктемелерден аулақ болу және қызмет көрсету сапасын жақсарту.Орнату икемділігі: желі талаптарына байланысты әртүрлі трафик сыныптары үшін шектеулерді реттеу мүмкіндігі.

The MPLS CAR деректер жылдамдығын бақылауды қамтамасыз ететін және шамадан тыс жүктемелердің алдын алатын желі шекараларында және желі ішінде трафикті саясаттандыру және қалыптастыру үшін қолданылады.

Кесте 3.4 – C++ бағдарламалау тіліндегі CAR алгоритмінің 1 порты бар желі үшін нәтижесі

Пакет	Күйі
1	Сәтті өңделді
2	Өткізу қабілетінің жеткіліксіздігіне байланысты жіберілмеді.
3	Өткізу қабілетінің жеткіліксіздігіне байланысты жіберілмеді.
4	Сәтті өңделді

Келес кестеде өткізу қабілеттілігі әртүрлі болатын 2 порт арқылы жұмыс жасайтын желіні көрсеттім.

Кесте 3.4 – C++ бағдарламалау тіліндегі CAR алгоритмінің 2 порты бар желі үшін нәтижес

1	Сәтті өңделді	Қолданылмайды
2	Өткізу қабілетінің жеткіліксіздігіне байланысты жіберілмеді.	Сәтті өңделді
3	Өткізу қабілетінің жеткіліксіздігіне байланысты жіберілмеді.	Сәтті өңделді
4	Сәтті өңделді	Қолданылмайды

ҚОРЫТЫНДЫ

Қорытындылай келе, виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу ұйымға желіні жобалау және орналастыру кезінде ескеру қажет негізгі аспектілерді ашады. Виртуалды корпоративтік байланыс желісін құру ұйымның қызметкерлері мен ресурстары арасында қауіпсіз, сенімді және тиімді өзара іс-қимылды қамтамасыз етуге мүмкіндік беретін компанияның ақпараттық инфрақұрылымын дамытудағы маңызды кезең болып табылады.

MPLS желілеріндегі кезек пен трафикті басқару алгоритмдерін қарастыру олардың заманауи желілердегі тиімділікті, сенімділікті және қызмет көрсету сапасын қамтамасыз етудегі маңыздылығын көрсетеді. Weighted Random Early Detection (WRED), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Fair Queuing (WFQ) және Committed Access Rate (CAR) сияқты алгоритмдер желі ресурстарын пайдалануды оңтайландыруда және әртүрлі трафик кластарына басымдық беруде шешуші рөл атқарады.

Бұл алгоритмдерді түсіну және оларды маршрутизаторлар мен MPLS қосқыштары сияқты желілік құрылғыларда қолдану желі инженерлеріне деректер ағындарын тиімді басқаруға, шамадан тыс жүктемелердің алдын алуға және соңғы пайдаланушыларға қызмет көрсету сапасын қамтамасыз етуге көмектеседі.

Осылайша, MPLS желілерінде кезек пен трафикті басқару алгоритмдерін одан әрі зерттеу және қолдану желілік инфрақұрылымның оңтайлы өнімділігі мен функционалдығын қамтамасыз етудің маңызды қадамы болып табылады.

Магистірлік диссертация үшін екі мақала жарық көрді[17, 18].

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Y. A. Ushakov, P. N. Polezhaev, A. E. Shukhman, L. V. Legashev and N. F. Bakhareva, "Simulation of a Corporate Network Based on Software-Defined Infrastructure and Network Function Virtualization," 2017 IVth International Conference on Engineering and Telecommunication (EnT), Moscow, Russia, 2017, pp. 42-46, doi: 10.1109/ICEnT.2017.16.

2. S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," 2020 IEEE Conference on Computer Applications(ICCA), Yangon, Myanmar, 2020, pp. 1-5, doi: 10.1109/ICCA49400.2020.9022848.

3. N.K. Tan, Building VPNs with IPsec and MPLS. New York, USA: McGraw-Hill networking, 2003.

4. C. M. Nawej and S. Du, "Virtual Private Network's Impact on Network Performance," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-6, doi: 10.1109/ICONIC.2018.8601281.

5. Google, "Https usage in chrome worldwide," https://transparencyreport. google.com/https/overview?hl=en&time os region=chrome-usage: 1;series:time;groupby:os&lu=load os region&load os region=chromeusage: 1;series:page-load;groupby:os, 2020.

6. M. Cooney, "Coronavirus challenges remote networking," https://www.networkworld.com/article/3532440/coronaviruschallenges- remote-networking.html, 2020.

7. F5, Inc., "What is a reverse proxy server?" https://www.nginx.com/ resources/glossary/reverse-proxy-server/.

8. Y. Rekhter, B. Moskowitz, D. Karrenberg, and G. de Groot, "Address allocation for private internets," IETF RFC 1597 https://tools.ietf.org/ html/rfc1597, 1995.

9. Apache, "Access control," https://httpd.apache.org/docs/2.4/howto/ access.html, 2020.

10. Microsoft Corporation, "Troubleshooting," https://sendersupport.olc. protection.outlook.com/pm/troubleshooting.aspx, 2018.

11. P. Richter, F. Wohlfart, N. Vallina-Rodriguez, M. Allman, R. Bush, A. Feldmann, C. Kreibich, N. Weaver, and V. Paxson, "A multiperspective analysis of carrier-grade NAT deployment," in Internet Measurement Conference. ACM, 2016, pp. 215–229.

12. N. Barya, A. Ashraf, M. Kaur and S. U. Gairola, "Classification and Analysis of Virtual Private Network," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-5, doi: 10.1109/ICCR56254.2022.9996015.

13. Q. Chen, J. Yu, J. Chang and J. Shi, "The improving of WRED mechanism and its simulation in MPLS," 2011 International Conference on Electrical and

Control Engineering, Yichang, China, 2011, pp. 5099-5102, doi: 10.1109/ICECENG.2011.6057162.

14. S. Badr, F. Bayoumi and G. Darwesh, "QoS adaptation in real time systems based on CBWFQ," 2011 28th National Radio Science Conference (NRSC), Cairo, Egypt, 2011, pp. 1-8, doi: 10.1109/NRSC.2011.5873626.

15. T. Minagawa and T. Ikegami, "Double WFQ QoS scheduling based on flow number in diffserve network," 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Gangwon, Korea (South), 2010, pp. 1365-1370.

16. https://www.techopedia.com/definition/31001/committed-access-rate-car

17. Г.М. Юсупова, Д.Р. Эрманова, М.Тузелбаев, С.Б. Сағынай, Фотонды сенсордың жаңа әзірлемелерінің құрылымы ,түрлері және қолдану аясы / «Автоматтандыру, басқару және ақпараттық технологиялардағы жасанды интеллекттің жетістіктері мен қолданылуы» атты Халықаралық ғылыми-тәжірибелік конференцияның Еңбектер Жинағы Том 1 – Алматы:АУЭС, 2024. – 503-509 ББ.

18. Г.М. Юсупова, А.С. Аннабаев, А. Ержан, С.Б. Сагынай,М.Д. Тузелбаев Моделирование и оптимизация спектрального коэффициента Отражения и отклонения брэгговской решетки / РЭжБӘИИ ғылыми еңбектері – Алматы,2024. – 63-70 ББ.

ҚОСЫМША А

```
#include <iostream>
#include <vector>
#include <algorithm>

// Пакет туралы ақпаратты сақтауға арналған құрылым
struct Packet {
    int size;
    int priority;
};

// WRED енгізу класы
class WRED
{
private:
    int min_threshold;
    int max_threshold;
    std::vector<float> drop_probabilities; // Басымдықтың әр деңгейі үшін
шығарылу ықтималдығы

public:
    WRED(int min_thr, int max_thr, const std::vector<float>& drop_probs)
        : min_threshold(min_thr), max_threshold(max_thr),
drop_probabilities(drop_probs) {}

    bool shouldDropPacket(int queue_size, int packet_priority)
    {
        if (packet_priority < 1 || packet_priority > drop_probabilities.size()) {
            std::cerr << "Қате: пакеттің дұрыс емес басымдығы.\n";
            return false;
        }

        float drop_probability = drop_probabilities[packet_priority - 1];

        if (queue_size < min_threshold) {
            return false;
        } else if (queue_size > max_threshold) {
            return true;
        } else {
            float current_drop_prob = (static_cast<float>(queue_size - min_threshold) /
                                       (max_threshold - min_threshold)) * drop_probability;
```

```
            return current_drop_prob >= drop_probability;
        }
    }
};

// WRED тестілеу функциясы
void testWRED()
{
    // 1-ден 5-ке дейінгі басымдықтар үшін шектер мен ықтималдықтарды белгілеңіз
    std::vector<float> drop_probabilities = {0.1, 0.2, 0.4, 0.6, 0.8}; //1 — басымдықтың шығарылу ықтималдығы 10%, 5-80 басымдыққа ие%
    WRED wred(10, 512, drop_probabilities); // Қысқартылған максималды кезек мөлшері

    std::vector<Packet> packets = {
        {20, 5}, {25, 4}, {30, 3}, {40, 2}, {50, 1}, {60, 5}, {70, 4},
        {15, 3}, {20, 2}, {25, 1}, {30, 5}, {35, 4}, {40, 3}, {45, 2},
        {50, 1}, {55, 5}, {60, 4}, {65, 3}, {70, 2}, {75, 1}, {80, 5},
        {85, 4}, {90, 3}, {95, 2}, {100, 1}, {105, 5}, {110, 4}, {115, 3}
    };

    // Басымдықты арттыру бойынша пакеттерді сұрыптау
    std::sort(packets.begin(), packets.end(), [](const Packet& a, const Packet& b) {
        return a.priority < b.priority;
    });

    int queue_size = 0;

    // Біз пакеттерді өңдейміз
    for (const auto& packet : packets) {
        if (queue_size + packet.size > 512) { // Егер пакетті қосу кезектің толып кетуіне әкелсе
            std::cout << "Ағымдағы кезек толы. Жаңасын бастау.\n";
            queue_size = 0; // Кезек өлшемін қалпына келтіріңіз
        }

        queue_size += packet.size;

        if (wred.shouldDropPacket(queue_size, packet.priority)) {
            std::cout << "Packet of size " << packet.size << " with priority " << packet.priority << " dropped. Queue size: " << queue_size << "\n";
        } else {
```

```
            std::cout << "Packet of size " << packet.size << " with priority " <<
packet.priority << " accepted. Queue size: " << queue_size << "\n";
        }
    }
}

int main()
{
    testWRED();
    return 0;
}
```

ҚОСЫМША Б

```
#include <iostream>
#include <vector>
#include <queue>
#include <map>
#include <random>
#include <algorithm>
struct ClassDef {
    int id;
    int weight;
    int rate;
};
struct Queue {
    int classId;
    std::queue<int> packets;
    int servedPackets = 0;
};
class Scheduler {
private:
    std::vector<ClassDef> classes;
    std::map<int, Queue> queues;
    int totalWeight;
    int totalRate;
public:
    Scheduler() : totalWeight(0), totalRate(0) {}
    void addClass(int id, int weight, int rate) {
        classes.push_back({id, weight, rate});
        queues[id] = Queue{id};
        totalWeight += weight;
        totalRate += rate;
    }
    void enqueue(int classId, int packetId) {
        queues[classId].packets.push(packetId);
    }
    void processQueues(int totalPacketsToProcess) {
        int packetsProcessed = 0;
        int maxPacketsPerIteration = std::min(10, totalPacketsToProcess);
        while (packetsProcessed < totalPacketsToProcess) {
            int iterationPacketsProcessed = 0;
            for (const auto& cls : classes) {
                int classId = cls.id;
```

```
            int weight = cls.weight;
            int packetsToProcess = maxPacketsPerIteration * weight / totalWeight;
            std::cout << "Processing class " << classId << ": ";
            while (packetsToProcess > 0 && !queues[classId].packets.empty()) {
                int packetId = queues[classId].packets.front();
                queues[classId].packets.pop();
                queues[classId].servedPackets++;
                std::cout << packetId << " ";
                --packetsToProcess;
                iterationPacketsProcessed++;
                packetsProcessed++;
                if (packetsProcessed >= totalPacketsToProcess) {
                    break;
                }
            }
            std::cout << std::endl;
            if (packetsProcessed >= totalPacketsToProcess) {
                break;
            }
        }
        if (iterationPacketsProcessed == 0) {
            break;
        }
    }
}
void printResults() {
    for (const auto& [id, queue] : queues) {
        std::cout << "Class " << id << " processed " << queue.servedPackets << "
packets." << std::endl;
    }
}
};

int main() {
    Scheduler scheduler;
    scheduler.addClass(1, 10, 1000);
    scheduler.addClass(2, 20, 2000);
    scheduler.addClass(3, 15, 1500);
    scheduler.addClass(4, 25, 2500);
    int totalPackets = 20;
    std::random_device rd;
    std::mt19937 gen(rd());
    std::uniform_int_distribution<> distr(1, 4);
```

```
    for (int i = 0; i < totalPackets; ++i) {
        int classId = distr(gen);
        scheduler.enqueue(classId, i);
    }
    int totalPacketsToProcess = 20;
    scheduler.processQueues(totalPacketsToProcess);
    scheduler.printResults();
    return 0;
}
```

ҚОСЫМША В

```
#include <iostream>
#include <queue>
#include <vector>
#include <unordered_map>
#include <algorithm>
#include <tuple>
struct Packet {
    int id;
    int flowId;
    int size;
    int weight;
    int timestamp;
};
struct PacketComparator {
    bool operator()(const Packet& p1, const Packet& p2) {
        return p1.weight > p2.weight;
    }
};
using PacketQueue = std::priority_queue<Packet, std::vector<Packet>,
PacketComparator>;
class WFQScheduler {
private:
    std::unordered_map<int, PacketQueue> queues;
    int currentTime;
public:
    WFQScheduler() : currentTime(0) {}
    void enqueue(Packet packet) {
        queues[packet.flowId].push(packet);
        std::cout << "Packet " << packet.id << " added to queue of flow " <<
packet.flowId << std::endl;
    }
    void processPacket() {
        if (queues.empty()) {
            std::cout << "No packets to process." << std::endl;
            return;
        }
        auto it = std::min_element(queues.begin(), queues.end(),
            [](const auto& a, const auto& b) {
                return a.second.top().weight < b.second.top().weight;
            });
        if (it != queues.end()) {
```

```
            Packet packet = it->second.top();
            it->second.pop();
            currentTime += packet.size;
            std::cout << "Processing packet " << packet.id << " from flow " <<
packet.flowId << " at time " << currentTime << std::endl;
            if (it->second.empty()) {
                queues.erase(it);
            }
        }
    }
    void processAll() {
        while (!queues.empty()) {
            processPacket();
        }
    }
};
int main() {
    WFQScheduler scheduler;
    scheduler.enqueue({1, 1, 10, 1, 0});
    scheduler.enqueue({2, 1, 20, 1, 1});
    scheduler.enqueue({3, 2, 15, 2, 2});
    scheduler.enqueue({4, 3, 25, 1, 3});
    scheduler.enqueue({5, 2, 30, 2, 4});
    scheduler.processAll();
    return 0;
}
```

ҚОСЫМША Г

```
#include <iostream>
class MPLS_VPN {
private:
    int committed_rate;
public:
    MPLS_VPN(int rate) : committed_rate(rate) {}
    bool checkRate(int packet_size) {
        if (packet_size <= committed_rate) {
            committed_rate -= packet_size;
            return true;
        } else {
            return false;
        }
    }
};
int main() {
    MPLS_VPN vpn(1000);

    int packet_sizes[] = {500, 800, 1200, 300};
    int num_packets = sizeof(packet_sizes) / sizeof(packet_sizes[0]);
    for (int i = 0; i < num_packets; ++i) {
        if (vpn.checkRate(packet_sizes[i])) {
            std::cout << "Packet " << i+1 << " processed successfully.\n";
        } else {
            std::cout << "Packet " << i+1 << " dropped due to insufficient
bandwidth.\n";
        }
    }

    return 0;
}

#include <iostream>
#include <vector>
struct Port {
    int committed_rate;
    Port(int rate) : committed_rate(rate) {}
};
class MPLS_VPN {
private:
```

```
    std::vector<Port> ports;
public:
    MPLS_VPN(std::vector<int> rates) {
        for (int rate : rates) {
            ports.push_back(Port(rate));
        }
    }
    bool checkRate(int port_index, int packet_size) {
        if (port_index < 0 || port_index >= ports.size()) {
            std::cerr << "Invalid port index.\n";
            return false;
        }
        Port& port = ports[port_index];
        if (packet_size <= port.committed_rate) {
            port.committed_rate -= packet_size;
            return true;
        } else {
            return false;
        }
    }
};
int main() {
    std::vector<int> rates = {1000, 2000};
    MPLS_VPN vpn(rates);
    std::vector<int> packet_sizes = {500, 800, 1200, 300};
    int num_packets = packet_sizes.size();
    for (int i = 0; i < num_packets; ++i) {
        for (int j = 0; j < rates.size(); ++j) {
            if (vpn.checkRate(j, packet_sizes[i])) {
                std::cout << "Packet " << i+1 << " processed successfully on port " <<
j+1 << ".\n";
                break;
            } else {
                std::cout << "Packet " << i+1 << " dropped on port " << j+1 << " due to
insufficient bandwidth.\n";
            }
        }
    }
    return 0;
}
```

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

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

магистрлік диссертацияға

Тузелбаев Максат

7М06201 «Телекоммуникация»

Тақырыбы: «Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу»

Магистрлік диссертация кіріспеден, қорытындыдан, үш тараудан тұрады, сонымен қатар магистрлік диссертация жазу кезінде қолданылған әдебиеттер тізімі бар.

Виртуалды корпоративтік байланыс желісін құру кезіндегі ерекшеліктер және оны шешу жолдары қарастырылды. Диссертациялық жұмыс бірнеше бөлімнен тұрады.

Бірінші бөлімде виртуалды корпоративтік байланыс желісі түрлері, олардың артықшылықтары және олардың сенімділігіне байланысты әдеби шолу жасалған.

Екінші бөлімде эксперименттік жұмыстар жүргізілген, эксперимент Cisco Packet tracer бағдарламасында корпоративтік байланыстың моделі құрылған.

Үшінші бөлімде эксперименттен алынған нәтижелерді алып MPLS VPN технологиясының басқа технологияларға қарағандағы артықшылығы көрсетілген.

Магистрлік диссертация өте жақсы орындалды (А+,95%) деп бағаланып, ал магистрант Тузелбаев Максат Джайбергеновичті 7М06201 – «Телекоммуникация» білім беру бағдарламасы бойынша «техника ғылымдарының магистрі» академиялық дәрежесіне ұсынамын.

Ғылыми жетекші
қауымдастырылған профессор, PhD,
_____ Юсупова Г.М.
«30» 05 2024 ж.

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

Магистрлік диссертацияға
РЕЦЕНЗИЯ

Магистрант: Тузелбаев Максат Джайбергенович

Білім беру бағдарламасы: 7М06201 «Телекоммуникация»

Магистрлік диссертация тақырыбы: «Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу»

Магистрлік диссертация кіріспеден, қорытындыдан, үш тараудан тұрады, сонымен қатар магистрлік диссертация жазу кезінде қолданылған әдебиеттер тізімі бар.

Виртуалды корпоративтік байланыс желісін құру кезіндегі ерекшеліктер және оны шешу жолдары қарастырылды. Диссертациялық жұмыс бірнеше бөлімнен тұрады.

Бірінші бөлімде виртуалды корпоративтік байланыс желісі түрлері, олардың артықшылықтары және олардың сенімділігіне байланысты әдеби шолу жасалған.

Екінші бөлімде эксперименттік жұмыстар жүргізілген, эксперимент Cisco Packet tracer бағдарламасында корпоративтік байланыстың моделі құрылған.

Үшінші бөлімде эксперименттен алынған нәтижелерді алып MPLS VPN технологиясының басқа технологияларға қарағандағы артықшылығы көрсетілген.

Жұмысты бағалау

Диссертациялық жұмыс белгіленген талаптарға сәйкес жасалған, аналитикалық кестелер мен сызбалардан тұрады. Жалпы, диссертациялық жұмыстың мазмұны мен көлемі мамандықтың стандарттары мен бейініне толық сәйкес келеді, студенттің жеткілікті теориялық дайындығын сипаттайды. Бұл магистрлік жұмыс өзінің мазмұны бойынша таңдалған тақырыпқа толық сәйкес келеді, оны ашады және магистрлік жұмыстарға қойылатын талаптарды қанағаттандырады.

Магистрлік диссертация жақсы орындалды (А-,90%) деп бағаланып, ал магистрант Тузелбаев Максат Джайбергенович 7М06201 – «Телекоммуникация» мамандығы бойынша «техника ғылымдарының магистрі» академиялық дәрежесіне ұсынылады.

Рецензент
PhD докторы,
Мирас университеті
IT және телекоммуникациялар
секторының менеджері
_____ Көшкінбаев С. Ж.
«06» 06 2024 ж.

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: Тузелбаев Максат Джайбергенович

Тақырыбы: Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу

Жетекшісі: Гульбахар Юсупова

1-ұқсастық коэффициенті (30): 5.8

2-ұқсастық коэффициенті (5): 2.6

Дәйексөз (35): 1.4

Әріптерді ауыстыру: 44

Аралықтар: 4

Шағын кеңістіктер: 5

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:

11.06.2024

Күні *Кафедра меңгерушісі*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тузелбаев Максат Джайбергенович

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу

Научный руководитель: Гульбахар Юсупова

Коэффициент Подобия 1: 5.8

Коэффициент Подобия 2: 2.6

Микропробелы: 5

Знаки из здругих алфавитов: 44

Интервалы: 4

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:

11.06.2024
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тузелбаев Максат Джайбергенович

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Виртуалды корпоративтік байланыс желісін құру ерекшеліктерін зерттеу

Научный руководитель: Гульбахар Юсупова

Коэффициент Подобия 1: 5.8

Коэффициент Подобия 2: 2.6

Микропробелы: 5

Знаки из здругих алфавитов: 44

Интервалы: 4

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:

11.06.2024
Дата

проверяющий эксперт