ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Коммерциялық емес акционерлік қоғамы
Ғұмарбек Даукеев атындағы
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»

«Тлекоммуникация және инновациялық технологиялар» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі
PhD, доцент Қадылбекқызы Э.
(ғылыми дәрежесі, атағы, аты-жөні)

_____
(қолы)
«_____»_____2021 ж.

МАГИСТЕРЛІК ДИССЕРТАЦИЯ

Тақырыбы: Cisco Packet Tracer желілік жабдығы негізінде виртуалды желілерді модельдеу және құру
Мамандық: 7М06201- «Радиотехника, электроника және телекоммуникациялар»
Магистрант: Смажанова А.С. _____ Тобы: МРЭТн 19-1
(аты-жөні) (қолы)
Жетекшісі: т.ғ.к., профессор _____ Айтмагамбетов А.З.
(ғылыми атағы, атағы) (қолы) (аты-жөні)
ЕТ қолдану кеңесшісі т.ғ.к.,профессор _____ Чежимбаева К.С.
(ғылыми атағы, атағы) (қолы) (аты-жөні)
Нормоконтроль: аға оқытушы _____ Павлова Т.А.
(ғылыми атағы, атағы) (қолы) (аты-жөні)
Пікіржазушы_____ _____ _____
(ғылыми атағы, атағы) (қолы) (аты-жөні)

Алматы 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Коммерциялық емес акционерлік қоғамы
Ғұмарбек Даукеев атындағы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

«Телекоммуникация және ғарыштық инжинерия» институты

«Тлекоммуникация және инновациялық технологиялар» кафедрасы

Мамандық : 7М06201- «Радиотехника, электроника және телекоммуникациялар»

Магистрлік диссертацияны орындауға арналған тапсырма

Магистрант: Смажанова Алтынай Смажанқызы
(толық аты-жөні)
Диссертация тақырыбы: «Cisco Packet Tracer желілік жабдығы негізінде виртуалды желілерді модельдеу және құру»

Университеттің Ғылыми кеңесінің №263 бұйрығымен «30» желтоқсан 2020 жылы бекітілген

Аяқталған диссертацияны тапсыру мерзімі «25.05» 2021 ж.

Диссертациялық жұмыстың мақсаты: VLSM мен FLSM ішкі желі әдістеріне салыстыру және анализ жасау.

Дайындылық корсеткіштерін $K_{г\text{-}13} = K^3_{г\text{-}у} * K^2_{г\text{-}і}$ формула арқылы табылды және байланыс желісінің дайындылық көрсеткіш коэфициенттері $K_{г\text{-}і}$ = 0,9999. Деректердің қауіп-қатердің болу ықтималдылық көрсеткіштері, Р=0,07728 және $К_{г\text{-}иб} = 1 - (1 - К_{г\text{-}у}) \times P$ формуласын қоданып $К_{г\text{-}иб}$ = 0,99959 алдық. Деректердегі қауіп-қатердің түсуі қарастырылмаған жағдайда $К_{г\text{-}у} = К^3_{г\text{-}г} \times К^2$ және қауып қатер коэфициенті $К_{г\,1\text{-}\,г\,3}$= 0,999571 болды.

Магистерлік диссертациядағы әзірленуі тиіс сұрақтар тізімі немесе диссертацияның қысқаша мазмұны:

1. Желілік жабдықтың эмуляторын таңдау.
2. Қолданылатын технологиялардың сипаттамасы.
3. Виртуалды желіні модельдеу ұсынысы.

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі

1. VLSM көмегімен шыққан ішкі желінің анализдік диаграммасы.
2. FLSM көмегімен шыққан ішкі желінің анализдік диаграммасы.
3. Cisco Packet Tracer бағдарламасындағы жіберу дестесіндегі «Simulation» режимі.
4. Жүктеме кезінде желінің жұмысын модельдеу.

5. Желінің салыстырмалы талдану диаграммасы.

6. Жоғалған пакеттер санының каналдағы жүктемеге тәуелділігі.

Негізгі ұсынылатын әдебиеттер.

1 CCNP маршрутизация / Т.Лэммсл, Ш.Одом, К. Уоллес. Изд. «Лори», 2015. – 444 с.

2 Тестирование и применение эмуляторов Cisco для моделирования гетерогенной IPсети / А.М. Горячев // Гагаринские чтения – 2016: XLII Международная молодежная научная коференция: Сборник тезисов докладов Т.ё. Московский авиационный институт (национальный исследовательский университет). – 2016. – стр.277-278.

3 Mirza Waseem Hussain, Sanjay JamwalComparative Analysis of Various Routing Protocols, IJMER | ISSN: 2249–6645, Vol.6 Iss. 3 | March 2016 | 67.

4 Todd Lammle: Cisco Certified Network Associate-Study Guide, Seventh Edition. – Twin: Sybex Press, 2013. – 289 p.

6 Таненбаум Э, Уэзеролл Д. Компьютерные сети. – Спб: Питер, 2012. – 960 с.

магистрлік диссертацияны дайындау

КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелер тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Тақырыпқа сәйкес ақпараттық шолу	03.09.2020	
2. Желілік жабдықтың эмуляторын таңдау (теориялық бөлім)	19.10.2020	
3. Қолданылатын технологиялардың сипаттамасы (зерттеу бөлімі)	02.04.2021	
4. Виртуалды желіні модельдеу ұсынысы (есептеу бөлімі)	28.04.2021	

Тапсырманың берілген уақыты «30» _қыркүйек_ 2019 ж.

Кафедра меңгерушісі _____ (Қадылбекқызы Э.)
(қолы) (аты-жөні.)

Ғылыми жетекшісі _____ (Айтмагамбетов А.З.)
(қолы) (аты-жөні)

Тапсырма орындалуға қабылданды

Магистрант _____ (Смажанова А.С.)
(қолы) (аты-жөні)

Аңдатпа

Бұл диссертациялық жұмыста Cisco Packet Tracer бағдарламалық жасақтамасы қолданылған. Бұл бағдарламалық жасақтама студенттерге, оқытушыларға және желілік инженерлерге VLSM желісін талдауға және енгізуге, барлық қажетті ақпаратты жылдам және қарапайым түрде ұсынуға пайдалы. Ішкі желілердің ыңғайлылығын жақсарту үшін көбінесе «ішкі желі» деп аталатын ішкі желі маскалары (VLSM) қолданылған және VLSM-нің тиімділігі анализдік диаграммалар арқылы көрсетілген. Модельденген виртуалды желіні талдау негізінде өнімділігін бағалау жүргізілді. Модельдеу жұмысына арналған бағдарламаланған желіні басқару технологиясын қолданылды.

Аннотация

В данной диссертационной работе был использован программный симулятор Cisco Packet Tracer. Этот симулятор полезен для студентов, преподавателей и сетевых инженеров для анализа и реализации сети VLSM, предоставив всю необходимую информацию, быстрым и легким способом. Для повышения удобства внутренних сетей использовались маски подсети (VLSM), часто называемые «внутренней сетью», а эффективность VLSM была демонстрирована аналитическими диаграммами. Оценка производительности была основана на анализе смоделированной виртуальной сети. Для моделирования использовалась технология управления программируемой сетью.

Abstract

In this dissertation work, we used the Cisco Packet Tracer software simulator. This simulator is beneficial for students, teachers and network engineers to analyze and implement a VLSM network, providing all data they need, in a fast and easy way. Subnet masks (VLSM), often referred to as "internal network", were used in order to improve the convenience of internal networks and the effectiveness of VLSM was demonstrated by analytic diagrams. The performance score was based on an analysis of a simulated virtual network. Programmable network control technology was used for simulation.

Мазмұны

Кіріспе

Қазіргі таңда компьютерлік желілер ақпараттық технологиялар саласының ажырамас бөлігі болып табылады. Оларсыз адамдардың күнделікті өмірін де, компаниялар мен кәсіпорындардың қызметін де елестету мүмкін емес. Жыл сайын компьютерлік желілер технологиясы жетілдірілуде, ал олардың құрылымы күрделене түсуде. Желілік әкімшілер, сондай – ақ компьютерлік бағыттағы студенттер үшін компьютерлік желілердің қолданыстағы моделін жасауға мүмкіндік беретін құрал қажет: әкімшілер оларды ақауларды диагностикалау үшін, ал студенттер алған теориялық білімдерін бекіту үшін пайдалана алады. Сондықтан компьютерлік желілерді модельдеу үшін қосымшаларды әзірлеу міндеті өзекті болып табылады. Осы технологиялардың күрделілігін және әр түрлі өндірушілер нарықта ұсынатын жабдықтардың кең спектрін ескере отырып, желіні құрудың оңтайлы нұсқасын таңдау мақсатында әр түрлі жобалық шешімдерді модельдеу кезеңі желілік жобаларды әзірлеу үшін қажет және осы кезең желілік жобаларды модельдеуге және сипаттауға арналған заманауи құрылғылардың көмегімен орындалады. Сондықтан, бұл жұмыста барлық қажетті цифрлық қадамдарды орындауға және қажетті ақпаратты (ішкі желі идентификаторы, тарату идентификаторы, ішкі желінің қол жетімді адрестері және басқалары) орындауға арналған негізгі графикалық симулятор ұсынылған.

Cisco Packet Tracer бағдарламалық жасақтамасын қолдану арқылы осы жұмысты студенттерге, оқытушыларға және желілік инженерлерге VLSM желісін талдауға және енгізуге, барлық қажетті ақпаратты жылдам және қарапайым түрде ұсынуға пайдалы. Ішкі желілердің ыңғайлылығын жақсарту үшін көбінесе «ішкі желі» деп аталатын өзгермелі ұзындықты ішкі желі маскалары (VLSM) қолданылады. Желілік әкімші бірнеше хосттары бар желілерде ұзын масканы және хосттары көп ішкі желілерде қысқа масканы қолдана алады [1].

Мұнда күрделі жүйелерді зерттеудің заманауи әдісі ретінде таным әдісі және виртуалды орталарда модельдеу сияқты жалпы модельдеудің қажеттілігі туралы біраз ойластыру қажет. Деректер берудің қазіргі заманғы күрделі желілерін оларды енгізгенге дейін моделдеу қажеттілігі мен осы технологиялардың жеткіліксіз дамуы арасындағы қайшылықтар өзектілігі анықталады. Зерттеу объектісі-деректерді беру желілерінің жұмысын модельдеу ортасы және жүйелері. Зерттеу пәні Cisco Packet Tracer жобалау ортасы болып табылады. Зерттеу мақсаты кәсіпорын желісінің моделін құру мысалында деректерді беру жүйесін модельдеу технологиясын әзірлеуден тұрады. Жұмысты орындау барысында келесі міндеттерді шешу қажет: күрделі жүйелерді моделдеу бойынша ғылыми және техникалық әдебиеттерді зерттеу. Желілік жабдықтың жұмысын модельдеудің қолданыстағы жүйелеріне талдау жүргізу. Таңдалған виртуалды ортада кәсіпорын деректерін беру желісінің жұмыс моделін құру.

Модельдеу ғылыми таным әдісі болып табылады, оны пайдалану кезінде зерттелетін объект модель деп аталатын қарапайым нысанмен алмастырылады. Модельдеу процесінің негізгі түрлері оның екі түрін есептеуге болады - математикалық және физикалық модельдеу. Физикалық (заттай) үлгілеу кезінде зерттелетін жүйе оның физикалық табиғатын сақтай отырып, зерттелетін жүйенің қасиеттерін жаңғыртатын оған сәйкес басқа материалдық жүйемен ауыстырылады. Модельдеудің осы түрінің мысалы пилоттық желі бола алады, оның көмегімен қандай да бір компьютерлер, коммуникациялық құрылғылар, операциялық жүйелер мен қосымшалар негізінде желі құрудың принципті мүмкіндігі зерделенеді.

Диссертацияның мақсаты - Cisco Packet Tracer бағдарламалық жабдығы арқылы виртуалды компьютерлік имитациялық модельдеу және осы желілік жабдықты қолдану арқылы VLSM мекенжай сызбасына қатысты IP-адрестерді тиімді бөлу үшін қолданылатын процедураны ұсыну.

Негізгі зерттеу жұмысымыздың өзектілігі ішкі желілерді бөлу болып табылғандықтан VLSM маскаларымен мекенжай сызбасына қатысты IP-адрестерді тиімді бөлуді қарастырылған.

1 Міндет қоюды негіздеу

Қазіргі заманғы жаңа технологиялар әлемінде желілік инженерлер жиі өз қызмет саласындағы проблемаларға тап болады. Бұл вектор жаңа буын қызметтері мен сервистерінің пайда болуына ықпал етеді және берілетін ақпараттың әр түрлі көлемін ұлғайтуға байланыс арналарына қойылатын талаптарды арттырады және соның салдары ретінде телекоммуникациялық жүйелерге (ТКЖ) енгізулер әкеледі. Сынақ ТКЖ стенділерін парадигма негізіндегі жасау жоғарыда айтылған телекоммуникация саласындағы қажеттілік мәселесін көтереді. Бұл стендтерді Имитациялық әдісі бойынша модельдеу тәсілі ұйымдастыру үшін ең релеванттық нұсқа болып табылады. Алайда, сипатталған осы әдістің бағдарламалық құралдары бүгінгі күні орнату күрделілігіне байланысты және жаңа бағдарламалық бағдарланған кешендермен және платформалармен салыстырғанда қолайлы емес.

1.1 Әзірлеу әдісін таңдау

Модельдеу ғылыми таным әдіс және пайдалану кезінде зерттелетін объект қарапайыммодель деп аталатын нысан болып танылады. Процестің негізгі түрлері модельдеу оның екі түрін есептеуге болады - математикалық және физикалық модельдеу. Физикалық (заттай) моделдеу кезінде зерттелетін жүйе оған сәйкес басқа материалдық жүйемен ауыстырылады,оларды сақтай отырып, оқылатын жүйенің қасиеттерін физикалық табиғат. Модельдеудің осы түрінің мысалы бола алады принциптік мүмкіндік зерттелетін пилоттық желі қандай да бір компьютерлер, коммуникациялық операциялық жүйелер және қосымшалар. Физикалық модельдеу мүмкіндіктері өте шектеулі. Ол шағын көлемді тапсырмада жеке тапсырмаларды жүйенің зерттелетін параметрлерінің үйлесімін шешуге мүмкіндік береді. Шын мәнінде, есептеу желісін моделдеу оны тексеру мүмкін емес, сол үшін әр түрлі байланыс түрлерін пайдалана отырып, нұсқаларға арналған жұмысмаршрутизаторлар, коммутаторлар және т.б. әр түрлі маршрутизаторлардың ондаған түрі тек үлкен емес күш-жігермен және уақытша шығындармен, сондай-ақ материалдық емес шығындармен байланысты. Бірақ желіні оңтайландыру өзгермейтін жағдайларда да құрылғы түрлері мен қол жетімді жүйелер, эксперименттер өте көп осы параметрлердің барлық комбинациялары мүмкін емес болжалды уақыт. Тіпті қарапайым пакеттің өлшемін өзгерту кез келген протокол операциялық жүйені қайта конфигурациялауды қажет етеді желілік әкімшіні талап ететін жүздеген желілік компьютерлер өте үлкен жұмыс. Сондықтан, желілерді оңтайландыру кезінде көптеген жағдайларда қолайлы математикалық модельдеуді қолдану көрсетіледі. Математикалық модель-арақатынастар жиынтығы (формулалар, теңдеулер) оның параметрлеріне, кіріс сигналдарына және бастапқы шарттар мен уақыт жай-күйінің өзгеру процесін анықтауға септігін тигізеді [2].

Математикалық модельдердің ерекше сыныбы модельдер. Мұндай модельдер компьютерлік бағдарлама болып табылатын нақты қадамдағы жүйеде болып жатқан оқиғаларды көрсетеді. Есептеу желілеріне қолданылатын

олардың имитациялық модельдері хабарларды қосымшалармен генерациялау және белгілі бір хаттамалардың пакеттері мен кадрларына хабарламалар, байланысындағы кідірістерді бөлу процестерін ойнатады. Операциялық жүйе ішінде хабарламаларды, пакеттерді және кадрларды өңдеу, бөлінетін желілік ортаға компьютер арқылы қол жеткізу процесі, келіп түсетін пакеттерді маршрутизатормен және имитациялық желіні моделдеу қымбат жабдықты сатып алудың қажеті жоқ. Себебі, оның жұмысы өте дәл ойнататын бағдарламалармен имитацияланады. Сондай-ақ имитациялық модельдеу жүйесі бар оқылатын жүйелердің тар класына бағдарланады және модельдерді құруға мүмкіндік береді. Хаттама анализаторлары нақты желілерді зерттеу үшін қажет, бірақ олар әлі де сипаттамаларды сандық баға алуға мүмкіндік бермейді. Осы жағдайларда жобалаушылар пайдалануы мүмкін құралдарды модельдей отырып, ақпараттық жүйелерді қалпына келтіретін модельдер әзірленетін желілерде өтетін процестер қарастырылады.

Желілік жабдықтың бағдарламалық эмуляторлары-бұл бағдарламалық нақты функциялар мен параметрлерді қосуға мүмкіндік беретін өнімдік есептеу желісі. Бұл желі жұмысын модельдеу, тестілеу және оларды жобалау үшін әзірленген. Эмуляторлардың көпшілігі пайдалану жеткілікті ыңғайлы, себебі графикалық желілік инфрақұрылымды басқару интерфейсі, ол әлдеқайда көп нақты құрылғылардың қосылыстарын басқарудан гөрі ыңғайлы.

1.2 Эмуляторлардың жіктелуі

Желілік жабдықтың барлық эмуляторларын екі негізгі бөлікке бөлуге болады топтар:

1) Аппараттық-өткізілген эмуляторла.

2) Бағдарламалық-іске асырылған эмуляторлар.

Бірінші топқа, әдетте, тар мамандандырылған оған нақты қосылған кезде телекоммуникациялық жабдықтардың нақты жұмысын имитациялау немесе оның қандай да бір бөлігі (әдетте-арналар байланыс) іске қосылады. Аппараттық эмуляторларда аппараттық деңгейде үдерістер іске асырылды, нақты желілерде ағатын-пакеттердің кідіруі, жоғалуы, берілген деректерді және т. б. оқиғаларды бұрмалайды. Әзірлеудің негізгі мақсаты мен аппаратты эмуляторларды қолдану нақты әртүрлі жағдайларда және әртүрлі арналардың сипаттамаларына байланысты. Эмуляторлардың екінші тобына арнайы жабдықтар мен жабдықтардың жұмысын имитациялауға мүмкіндік беретін әзірленген бағдарламалар жатады. Бағдарламалық эмуляторларды пайдаланудың негізгі мақсаты-ғылыми эксперименттердің қойылымдары ғылыми-зерттеу қызметі ретінде қолдану үшін қолданылады. Сондай-ақ, бұл бағдарламалар жиі қызметкерлерді жұмысқа даярлау үшін оқыту жүйесі ретінде пайдаланылады.

Есептеу желілерін құру міндеттерін шешу үшін әртүрлі бағыттағы желілік жабдықтар:

- коммутатор-желілік бір немесе бірнеше жергілікті компьютерлерді біріктіруге арналған жабдық арналған құрылғы;

- маршрутизатор – өзара іс-қимыл жасауға арналған құрылғы әртүрлі жергілікті желілерде орналасқан компьютерлер мен желіаралық экран-Интернет желісіне қол жеткізуді қамтамасыз ететін құрылғылар керек.

Желіде Cisco Systems компаниясы желілік жабдық нарығында сөзсіз фаворит болып саналады (шағын кеңседен ірі корпорацияларға дейін есептеу желілерін құру үшін құрылғыларды ұсынады) [3].

Cisco Systems Компаниясы 1984 жылдан бастап осы күнге дейін желілік жабдықты өндіруші болып табылады бұл салада көшбасшы болып табылады. Компанияның желілік жабдықтары Елеулі бәсекелестердің аясында бөлінеді және көптеген артықшылықтары бар:

- сенімділік - Cisco IOS операциялық жүйесі және өзіне құрылғыны теңшеу және теңшеу үлкен спектрі негізінде жұмыс істейтін компания шығаратын желілік жабдық;
- икемділік-Cisco IOS басқарылатын желілік құрылғылар бір уақытта маршрутизациялық, қорғаныс, жөндеу және т.б түрлі функцияларды орынды;
- зияткерлік – компания құрылғылары кең спектрді қамтиды әртүрлі технологиялар мен хаттамаларды, стандартты және әзірленген Cisco компаниясы;
- орталықтандыру - құрылғыларды басқару үшін пайдаланылуы мүмкін қуатты басқару кешендері және жабдықты жөндеу, мысалы, Cisco Security Manager және т. б. кемшіліктерден тек құнды бөлуге болады.

Алайда, айта кету керек Cisco компаниясы шығаратын жабдықтың сенімділігі жоғары құнды болып саналады. Cisco IOS (Internetwork Operating Жүйесі) кең таралуын ескере отырып, сондай-ақ жоғары құны осы жабдықты пайдалану қажеттілігі одан да айқын көруге болады. Бұл жабдықта өндіруші есептеу желілерінің болашақ модельдері жобаланатын болады.

1.3 Желілік жабдықтың эмуляторын таңдау

Cisco Systems шығарған желілік жабдықтың виртуалды көшірмелерін жасауға мүмкіндік беретін ең танымал эмуляторларды егжей-тегжейлі қарастырайық. Cisco Packet Tracer бағдарламалық жасақтамасы.

Желілік Симуляторлар - бұл адамдарға желілік жүйелермен жұмыс істеуге көмектесетін бірінші нәрсе.

Бұл жағдайда, егер бұл жағдай орын алса да, коммутаторлар мен маршрутизаторларды дереу қосуға қабілетті зертханалық ортаны құру мүмкін емес болуы мүмкін, бұл әрқашан қажет емес. Бүгін оны тестілеу үшін виртуалды бағдарламалық қамтамасыз ету құрылды. Олардың бірі-Cisco компаниясы әзірлеген және пайдаланушыларға тегін ұсынылатын Packet Tracer. Packet Tracer - бұл пайдаланушыларға қауіпсіз ортада желілік мәселелерді жобалауға, жасауға және жоюға мүмкіндік беретін визуализация мен модельдеудің қуатты құралы. Ол оңай сүйреп апаратын топологияңызды жасауға мүмкіндік беретін қарапайым интерфейсі бар құрал болып табылады.

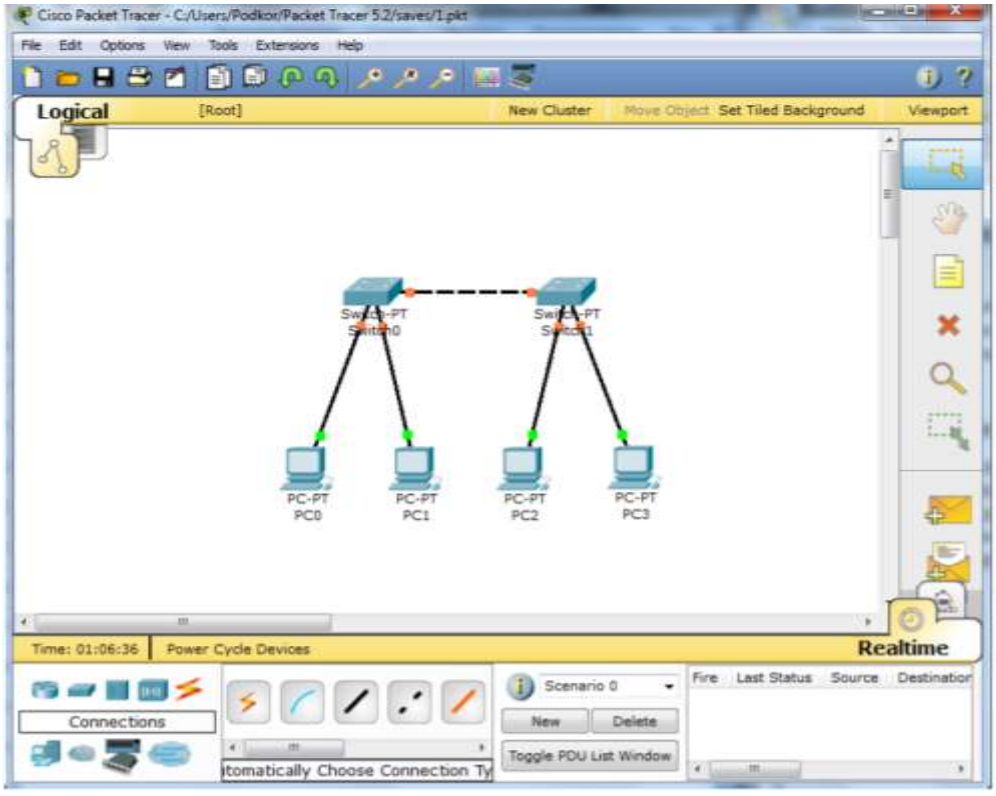
Оны жай ғана басу арқылы құрылғыдағы интерфейстерді қосуға және жоюға болады. Сонымен қатар, құрылғыны таңдау арқылы интерфейстерді

таңдауға болады. Құрылғылар жұмыс істеп жатыр ма көру үшін ping командасын жазу қажет емес & Running (яғни, олар жұмыс істейді), жай ғана конвертті басса пропинг шығады. Ол сынау қажет жабдықтар мен қосылыстары бар барлық желілік функцияларды қолдайды.

Cisco Packet Tracer бағдарламасының артықшылықтары:

- ол жайлы және жақсы ақпараттандырылған ортаны қамтамасыз етеді;
- ол нақты уақыт режимінде бірнеше оқу зертханаларын ұсынады;
- ол Студенттер үшін емтихан дайындап, балл бере алады;
- желілік орта әзірленеді, ал желілік құрылғылар виртуалды жабдықты пайдалана отырып реттеледі.

Желілік жабдықтың ең танымал эмуляторы-Cisco Packet Tracer, бұл Cisco Systems компаниясы әзірлеген эмулятор болып табылады. Packet Tracer үлкен алды өткізу үшін оны қолдану қажеттілігі есебінен тарату Cisco Network Academy бағдарламасы шеңберінде оқыту жыл сайын ондаған мың бастаушы мамандар оқытылады. Интерфейс бастаушы үшін жақсы бейімделген және жаңа желі құру процесін өте жеңілдетеді жүргізу үшін қажетті инфрақұрылымдарды іске қосу және теңшеу практикалық сабақтар сервистердің. Интерфейс үлгісі 1.1 – суретте көрсетілген [4].



1.1 сурет - Cisco Packet Tracer эмуляторының графикалық интерфейсі

Желілік инфрақұрылымды құру және кейіннен түрлендіру интуитивті болып табылатын графикалық интерфейс арқылы жүреді графикалық басқару интерфейстері түсінікті және ең ыңғайлы, қарастырылып отырған

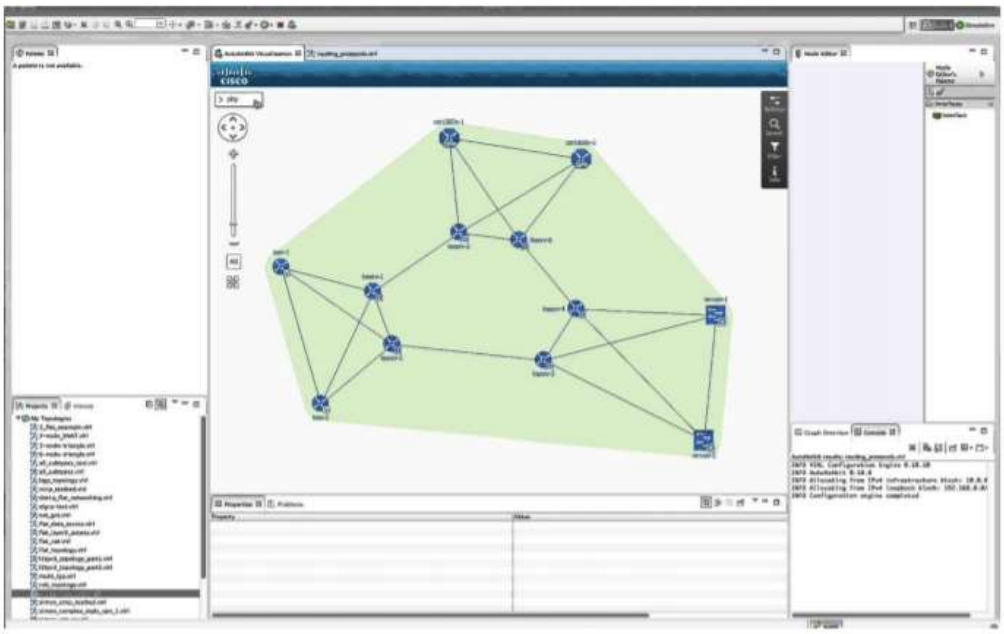
эмуляцияның бағдарламалық құралдарымен ұсынылатын желілік жабдықтар. Қосымша қандай да бір физикалық машинаны немесе көлік құралын пайдаланбай, бізге желілік зертханалық ортаны ұсынады. Жергілікті желіні маршруттау Қосымшаларының көп бөлігі осы үлгілеу бағдарламасымен орындалуы мүмкін .

Cisco пакеттерін трассалау бағдарламасы – Cisco немесе Cisco операцияларын орындауға мүмкіндік беретін модельдеу бағдарламасы.

Packet Tracer эмуляторының негізгі мақсаты CCNA (Cisco Certified Network Associate) және CCNA Security (Cisco Certified Network Associate Security) сертификациялық емтихандарға дайындалу үшін тәжірибелік жұмыстарды жүргізу үшін виртуалды желілерді құруда. Стандартты маршрутизаторлар мен Packet Tracer коммутаторларынан басқа IP-телефондардың, сымсыз қатынау нүктелері мен стандартты қызметтер жиынтығымен серверлердің эмуляциясын қолдайды. Packet Tracer-де қандай да бір құрылғыға берілетін барлық деректер блоктары туралы толық ақпарат алуға мүмкіндік беретін снифферлер, жүктемені жасанды жасауға мүмкіндік беретін желілік трафиктің генераторлары және кез келген пакетпен желі өту бағытын немесе әртүрлі құрылғылардан өту кезінде пакеттің өзгеру процесін қадағалауға мүмкіндік беретін деректер ағындарын бейнелеу құралдары сияқты желілік инфрақұрылымның жұмысын зерттеуді жеңілдететін көптеген құралдар енгізілген. Packet Tracer-білім алушы үшін ғана емес, оқытушы үшін де желілік жабдықты эмуляциялаудың ыңғайлы құралы.

Эмуляторға тапсырманың орындалуын автоматты тексеру құралдары енгізілген. Оқытушы тапсырманың орындалу дәрежесін автоматты түрде тексеретін Packet Tracer үшін зертханалық жұмысты әзірлей алады және барлық хаттамалардың дұрыс жұмыс істеуін және енгізілген командалардың дұрыстығын қолмен тексерудің орнына тапсырманы орындау пайызын және негізгі сервистердің жұмыс қабілеттілігін анықтайтын автоматты тексеруді пайдалану жеткілікті. Cisco Packet Tracer желілік жабдықтың аппараттық және бағдарламалық бөлігінің эмуляциясын шығарады. Осылайша, Packet Tracer үлкен желілік инфрақұрылымдардың көшірмесін жасауға мүмкіндік береді, тек эмуляцияланатын құрылғылар нақты ірі желілерде қолданылатын технологиялардың өте көп мөлшерін қолдамайды, нақты құрылғыларда қол жетімді көптеген функциялар жоқ. Cisco Packet Tracer негізгі артықшылығы осы өнімнің тегін. Осылайша, Cisco Packet Tracer эмуляторы Cisco компаниясының базалық 15 курсы бойынша және маман деңгейін емтихандарға дайындау кезінде практикалық сабақтарды өткізу үшін оңтайлы құрал болып табылады. Бірақ есептеу желілерін моделдеудің неғұрлым күрделі міндеттерін шешу үшін БҚ сәйкес келмейді, себебі симулятор болып табылады және нақты жабдықтың барлық мүмкіндіктерін бермейді, әрі қарай қарастырылмайды. Cisco (VIRL) - бұл физикалық жабдықта қажетсіз желіні моделдеуді жасау және іске қосу үшін Cisco әзірленген бағдарламалық құрал. VIRL OpenStack негізіндегі платформа болып табылады, ол iosv, IOSvL2, IOS XRv, NX-OSv, CSR1000v және ASAv бағдарламалық қамтамасыз ету

бейнелерін ендіреді. VIRL VM Maestro интерфейсін пайдалана отырып, жобалаудың масштабталатын, кеңейтілетін желілік ортасын қамтамасыз етеді. Соңғы уақытта HTML5 пайдаланып браузер негізінде операциялардың кеңдігі мен жетілдірілуі байқалады. VIRL сондай-ақ Juniper, Palo Alto Networks, Fortinet, F5 BigIP, Extreme Networks, Arista, Alcatel, Citrix және т.б. сияқты бөгде виртуалды машиналармен интеграциялау үшін кең мүмкіндіктерге ие. VIRL физикалық маршрутизаторларда сияқты заңды және лицензияланған Cisco IOS бейнелерінің толық жиынтығымен жеткізіледі. Жаңа Cisco IOS шығарылымдары тұрақты негізде беріледі. VIRL үшін жабдыққа қойылатын ең аз талаптар-процессордың төрт "логикалық" ядросы бар Intel базасындағы компьютер (физикалық емес процессорлар), 8 Гбайт жедел жады және 70 Гбайт дискідегі бос орын. Ең соңғы компьютерлер Intel i5 және i7 процессорларымен бірге төрт ядросы бар (кейбір қоспағанда). Cisco 12 Гбайт 20 Түйініне, 15 Гбайт 30 түйініне немесе 18 Гбайт 16 40 Түйініне. Әрбір Cisco IOS-XRv торабы үшін 3 ГБ жады қажет. VIRL бірге жеткізілетін AutoNetkit, оларды іске қосқан кезде IP-адрестерді автоматты түрде тағайындай алады, және ол тіпті кейбір негізгі маршрутизация хаттамаларын баптайды. Bootstrap конфигурациясы оны іске қосқаннан кейін бірден толық конвергентті желі береді. Функцияларға бірден көшу және не тексеру қажет екеніне назар аудару мүмкіндігі беріледі. Бұл желі инженерлері үшін қажетті мүмкіндік, командаларды іздеу және белгілі бір функцияларды тестілеу үшін уақытша ортаны теңшеуге мүмкіндік береді. Егер желі топологиясы нөлден салынса немесе жұмыс ортасының макеті құрылса, онда қолмен IP адрестеу ұсынылады. 1.2 – суретте Cisco VIRL желілерін жобалау ортасының жұмыс аймағы бейнеленген [5].

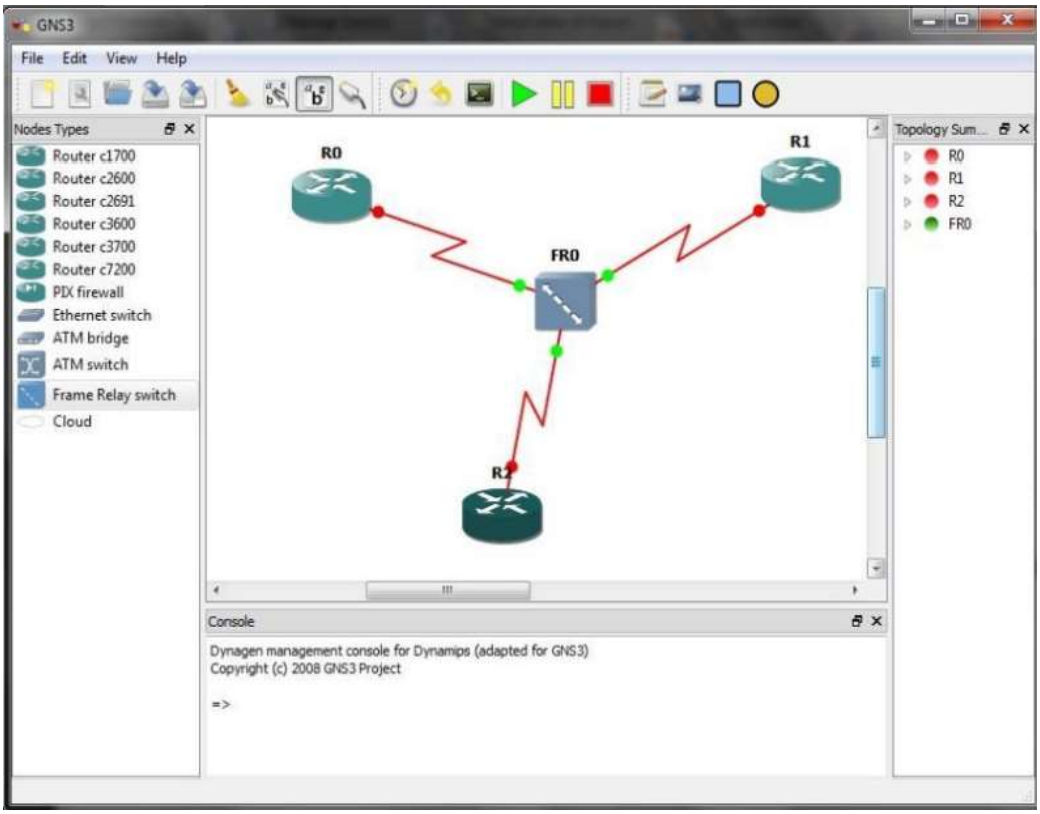


1.2 сурет - Cisco VIRL модельдеу ортасының жұмыс аймағы

Осыған байланысты қазіргі уақытта байланыс және басқару орталықтарының операторларының жұмысының сапасын бақылау, талдау және басқару алгоритмін әзірлеу мен зерттеудің жедел ғылыми-техникалық міндеті тұр, оларды шешу бағалау мен бағалаудың бірыңғай әдістемесін құрудың перспективаларын ашады. байланыс орталығының жұмысын жақсарту, сондай-ақ клиенттердің адалдығын арттыру үшін ішкі сапа қызметтерін тексеру мүмкіндіктері.

GNS3 (Graphical Network Simulator 3) - бұл тәуелсіз бағдарламалық жасақтама маршрутизаторы Cisco үшін тәуелсіз эмулятор. GNS3-ке Linux, Windows және Mac OS X операциялық жүйелерінің көпшілігінде қолдау көрсетіледі және бұл бағдарламалық жасақтама эмуляторы Cisco IOS амалдық жүйесінің нақты бейнесін жүктеу және пайдалану арқылы Cisco маршрутизаторларының аппараттық құралдарын эмуляциялауға мүмкіндік береді.

GNS3 - бұл әртүрлі эмуляциялық бағдарламалық жасақтаманы біріктіретін графикалық фронт. 1.3-суретте көрсетілген эмуляциялық ортаның графикалық интерфейсі жаңадан келген мамандарға бейімделмеген, керісінше эмуляция құралдарымен, желілік жабдықтармен жұмыс тәжірибесі бар және желілік құрылғылардың жұмыс істеуінің негізгі принциптерімен таныс адамдарға арналған.



1.3 сурет - GNS3 эмуляторының графикалық интерфейсі

Бірақ графикалық басқару элементтерінің болуы желілік инфрақұрылымды құру процесін едәуір жеңілдетеді және онымен жұмыс істеуді ыңғайлы етеді. GNS3 құрамында үш бөлек бағдарламалық жасақтама эмуляторлары бар:

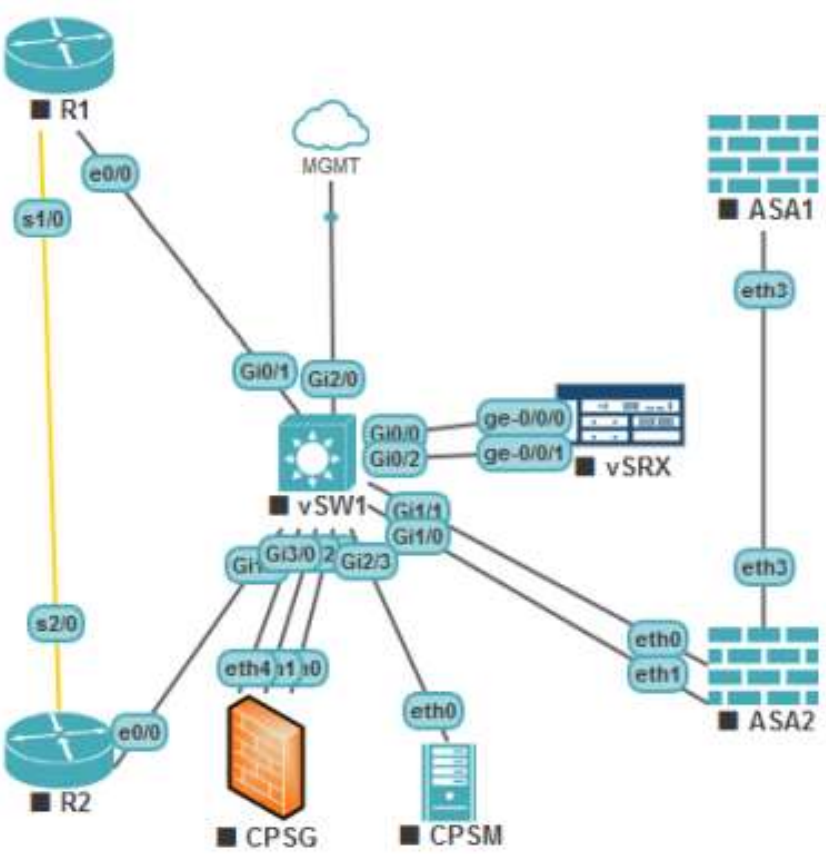
1)Біріншісі - Dynamips. Көптеген желі мамандары Dynamips-ті тек GNS3 ортасында қолданады, өйткені конфигурация файлдарымен және пәрмен жолымен жұмыс істеудің қажеті жоқ.

2)Екіншісі - Cisco PIX және ASA брандмауэрлері мен Cisco IPS енуінің алдын алу жүйелерін шығаратын Qemu, бұл құрылғыларға қолдаудың болуы желілік инфрақұрылымды қорғаумен байланысты салаларда GNS3 оқытуды айтарлықтай кеңейтеді.

3)Үшінші элемент - виртуалды серверлерді немесе виртуалды дербес компьютерлерді желілік инфрақұрылымға эмуляцияланған құрылғылардан біріктіруге мүмкіндік беретін виртуалды виртуалдау жүйесі, бұл сізге нақты ақпараттық инфрақұрылымды дәлірек жасауға мүмкіндік береді және бұл кең ауқымды зерттеуді білдіреді технологиялар.

GNS3 - бұл өте ресурстарды қажет ететін эмуляция жүйесі. Бірнеше тәуелсіз эмуляциялық жүйелер бір уақытта жұмыс істейтіндіктен және олардың үстінен инфрақұрылым күйінің өзгеруін үнемі бейнелейтін графикалық интерфейсті қамтамасыз ететін басқару ортасы қажет, сондықтан есептеу үшін маңызды қуат қажет. GNS3 бізге нақты ақпараттық инфрақұрылымдардың желісі, серверлік аппаратурасы және соңғы пайдаланушы компьютерлерімен нақты көшірмесін жасау функциясын ұсынса да, дербес компьютердің есептеу қуаты өте аз ақпараттық инфрақұрылымға ғана еліктеуге жеткілікті. Нәтижесінде GNS3-тегі практикалық сабақтар нақты инфрақұрылымның көшірмелерінде емес, жасанды түрде құрылған желілік сегменттерде жүргізілуі мүмкін.

Бірыңғай желілік зертхана (UNetLab, UNL) - телекоммуникациялық жабдықтардың әсерлі тізімін қолдайтын, виртуалды желілерді, әртүрлі зертханаларды модельдеуге және құруға арналған көп қолданушы платформасы болып табылатын желілік эмулятор. Қазіргі уақытта UNetLab эмуляторы виртуалды желілерді имитациялау алаңы ғана емес, сонымен қатар әр түрлі Cisco сертификаттарына дайындық құралы болып табылады (CCNA / CCNP үшін жаңадан бастаушылар үшін және CCIE Routing and Switching, CCIE Security және т.с.с.). Сонымен қатар, UNL желілік инженерияда, соның ішінде желілік ақаулықтың негізгі себептерін анықтау мен жоюға (ақаулықтарды жою) жүйелі тәсілдеме қолданылады. UNetLab жобасы 2014 жылы наурызда басталды, бірақ қысқа уақыт ішінде ол өзінің жүктерінде бірқатар үлкен артықшылықтарға ие GNS3 және Cisco Packet Tracer сияқты танымал эмуляторлардың маңызды бәсекелесіне айналды. Осылайша, UNetLab өнімінің тұжырымдамалық жаңалығы - бұл әр түрлі платформалар мен әртүрлі құрылғылар өндірушілері арасында бағдарламаны іске қосу және пайдалану мүмкіндігі. Графикалық интерфейстің мысалы 1.4-суретте көрсетілген [6].



1.4 сурет - UNL эмуляторының графикалық интерфейсі

Осы тәсілді қолдану UNL-ге сәйкес желілік құрылғыларды имитациялау үшін дербес виртуалды машиналарды пайдалану тұжырымдамасынан бас тартуға және барлық қажетті бағдарламалық модульдерді біріктіретін IOU / IOL, Dynamips және QEMU түйіндерінің 20 бағдарламалық эмуляторлары негізінде сандық желілік зертханалар құруға мүмкіндік береді. Бір платформадағы бір файлдағы сценарийлер. UNetLab эмуляторының тиімді артықшылығы - ол мүлдем тегін, сондықтан оны тек коммерциялық мақсаттарда ғана емес, сонымен қатар қарапайым пайдаланушылардың оқуы үшін де қолдануға болады.

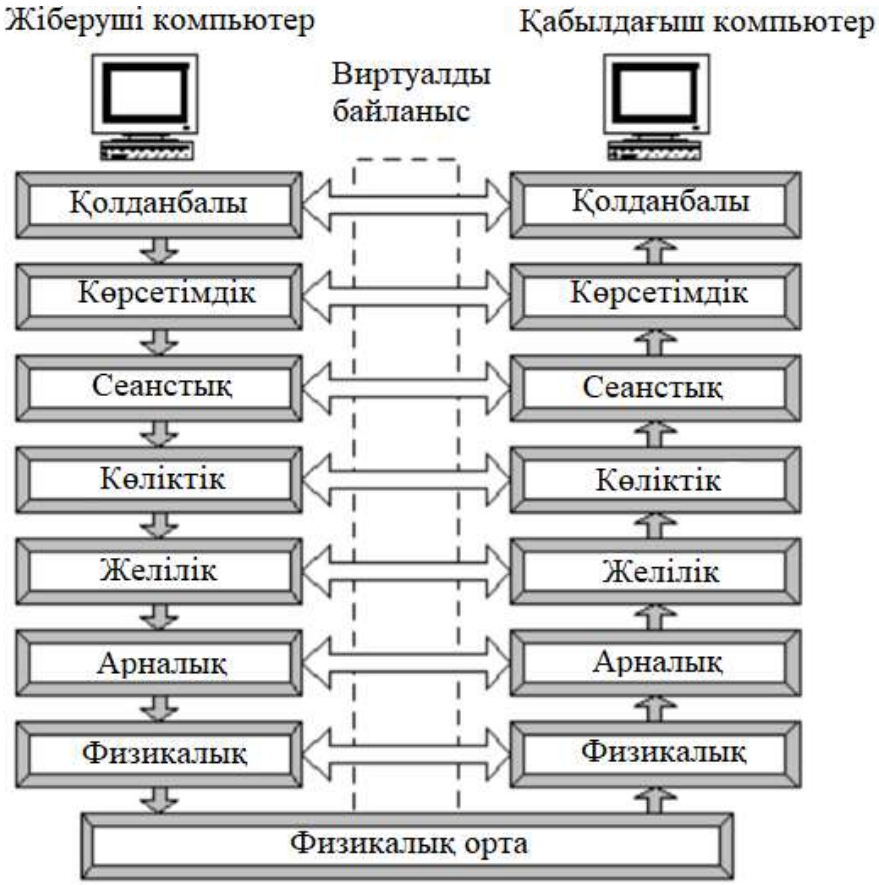
Артықшылықтардың қатарында жабдықтың (маршрутизаторлар, ажыратқыштар, қауіпсіздік құрылғылары және т.б.) шексіз санын іске қосу мүмкіндігі туралы айта кету керек, олардың саны тек жұмыс орнының аппараттық мүмкіндіктерімен шектеледі. UNetLab-тағы аппараттық қолдау өте кең. UNL сізге VIRL (vIOS-L2 және vIOS-L3), ASA кескіндері, Cisco IPS кескіндері, Cisco IPS кескіндері, XRv және CSR1000v кескіндерін, GNS эмуляторынан алынған кескіндерді, Cisco vWLC және vWSA кескіндерін іске қосуға мүмкіндік береді. Тізімделген суреттерден басқа, басқа жеткізушілердің жабдықтарының әсерлі тізіміне қолдау көрсетіледі: Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX виртуалды,

Checkpoint Firewall, HP VSR1000, Juniper Olive (портинг), арша Желілер vMX маршрутизаторы, Juniper vSRX, S-Terra Firewall, MS Windows және т.б.

Желілік жабдықтың эмуляторлық бағдарламалық платформаларының жалпы салыстырмалы талдауына сүйене отырып, біз Cisco Packet Tracer бағдарламасын ең өзекті және тиімді деп бөле аламыз.

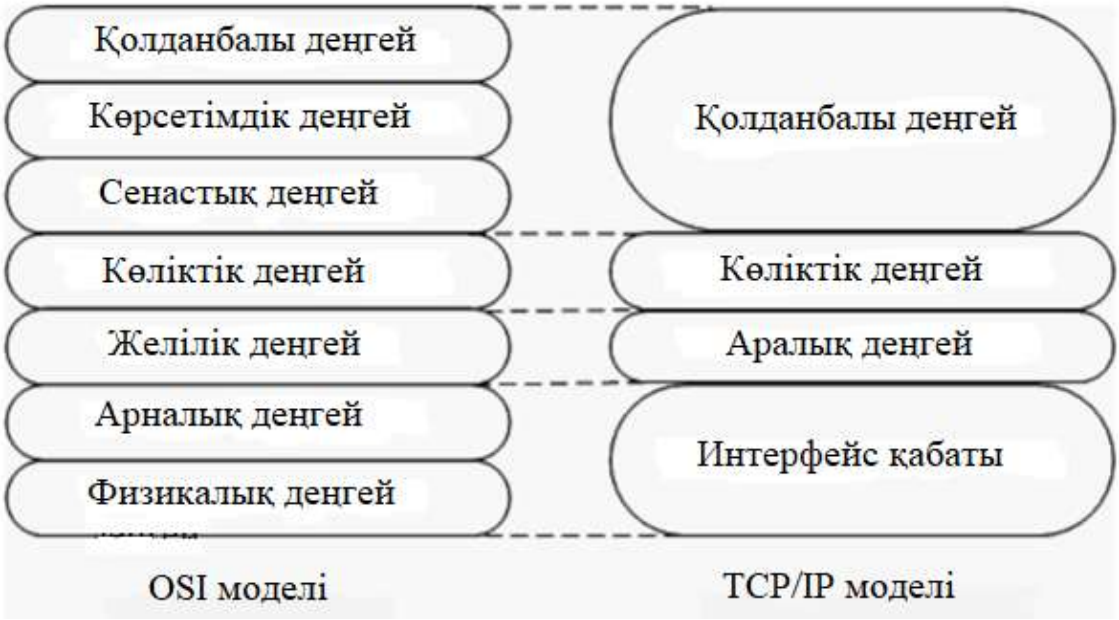
1.4 Виртуалды желі моделі

Бағдарламалық жүйені жобалау алдында жүйенің компоненттері әзірленетін және іске асырылатын компьютерлік желінің пайдаланылатын моделін сипаттау қажет. OSI және TCP/IP эталондық модельдері екі негізгі архитектуралық түрі бар – OSI және TCP/IP эталондық модельдері. OSI эталондық моделімен байланысты хаттамалар қазір пайдаланылмағанына қарамастан, модельдің өзі әлі күнге дейін өзекті, ал оның деңгейлерінің қасиеттері өте маңызды. Өз кезегінде TCP/IP эталондық моделі дерлік қолданылмайды, ал оның хаттамалары кең таралған болып табылады. OSI эталондық моделі, суретте көрсетілген компьютерлердің өзара әрекеттесу 1.5-суретте, жеті деңгейді қамтиды: физикалық, арналық, желілік, көліктік, сеанстық, өкілдік және қолданбалы.



1.5 сурет - OSI эталондық моделіндегі компьютерлердің өзара әрекеттесу сұлбасы

OSI моделіне ұқсас, TCP / IP моделінің көп деңгейлі құрылымы бар, ол төрт деңгейден тұрады: интерфейстік, желіаралық, көліктік және қолданбалы. 1.6-суретте OSI және TCP/IP моделдерінің құрылымын салыстыру кестесі бейнеленген [7].



1.6 сурет - OSI және TCP/IP үлгілерін салыстыру

Осы іргелі ұқсастыққа қарамастан, бұл модельдер бірқатар айырмашылықтар бар. OSI моделі үшін орталық үш концепция болып табылады: қызметтер (сервистер), интерфейстер және хаттамалар. Сервис деңгейді не істеп жатқанын анықтайды, деңгей интерфейсі осы деңгейге қол жеткізу тәсілін анықтайды, ал деңгейде қолданылатын хаттамалар оның ішкі іске асырылуының егжей-тегжейі болып табылады. TCP / IP моделінде бастапқыда қызметтер, интерфейс және протоколдар арасында нақты бөлу болған жоқ,бірақ оны OSI моделіне ұқсас ету үшін оны өзгертуге әрекет жасалған. Нәтижесінде моделін OSI хаттамалары, жасырын қарағанда жақсы моделі TCP/IP технология өзгерген жағдайда олар салыстырмалы түрде оңай ауыстырылды. Басқа деңгейлерді қозғамай, осындай өзгерістерді жүргізу мүмкіндігі көп деңгейлі хаттамалардың басты мақсаттарының бірі болып табылады.

Осылайша, OSI эталондық моделі компьютерлік желілердің абстрактілі құрылымын жақсы сипаттайды. Екінші жағынан, TCP / IP моделі ұзақ уақыт бойы кеңінен қолданылатын хаттамаларды қамтиды. Әзірлеу үшін бағдарламалық жүйесін шешілді пайдалануға келісімді нұсқа: сипаттау үшін жалпы сәулет желісін пайдалануға терминдер OSI моделінің, ал іске асыру хаттамалар сүйенетін моделі TCP/IP. Жобаланатын жүйенің ерекшелігін ескере

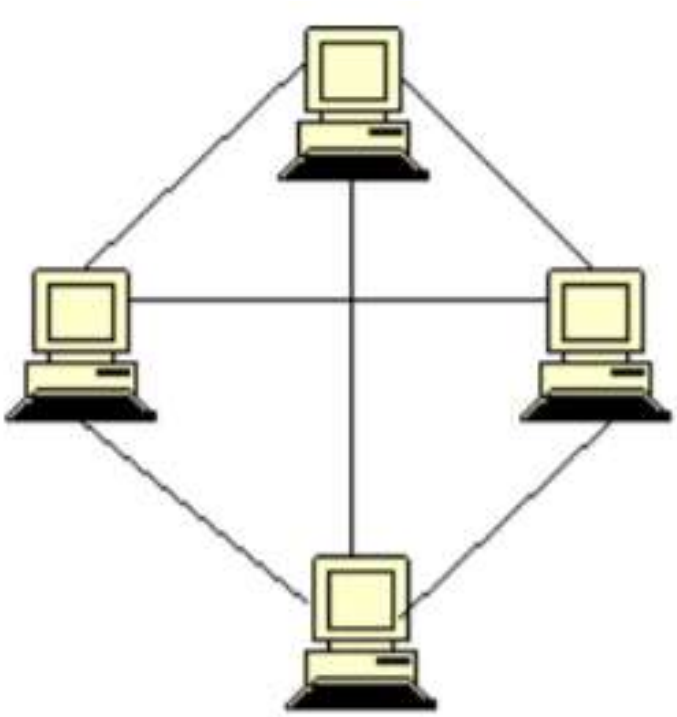
отырып, модельдің келесі үш деңгейін жан-жақты қарастыру қажет: физикалық, арналық және желілік.

1.5 Физикалық деңгей

Физикалық деңгей физикалық байланыс арналары бойынша ақпаратты берумен айналысады. Физикалық деңгейдегі функциялар желіге қосылған барлық құрылғыларда іске асырылады. Физикалық деңгей үшін ол беретін ақпараттың мағынасы жоқ. Ол үшін бұл ақпарат бұрмалаусыз және берілген тактикалық жиілікке (көршілес биттер арасындағы интервал) сәйкес жеткізу қажет биттердің біртекті ағыны болып табылады. Барлық физикалық ақпарат тасығыштарды екі санатқа бөлуге болады: өткізгіш және сымсыз. Өткізгіш тасушыларға коаксиалды кабельдер, оралған булар, электрмен қоректендіру желілері және талшықты оптика жатады. Сымсыз тасымалдаушыларға-радиобайланыс, микротолқынды диапазондағы байланыс, инфрақызыл диапазондағы байланыс, көрінетін диапазондағы байланыс. Физикалық арналар арқылы трафикті беруге байланысты көптеген сипаттамалар бар. Ең маңыздысы болып мыналар табылады – ұсынылған жүктеме-пайдаланушыдан желіге кіріске түсетін деректер ағыны. Берілген жүктемені секундына биттердегі (немесе килобит, мегабит және т.б.) деректердің желіге түсу жылдамдығымен сипаттауға болады). 17-деректер беру жылдамдығы-желі арқылы өткен деректер ағынының нақты жылдамдығы [8].

Бұл жылдамдық ұсынылған жүктеменің жылдамдығына қарағанда аз болуы мүмкін, себебі желідегі деректер бұрмалануы немесе жоғалуы мүмкін. Өткізу қабілеті деп аталатын байланыс арнасының сыйымдылығы арна бойынша ақпаратты берудің ең жоғары ықтимал жылдамдығы болып табылады. Таратқыштың биттік жылдамдығы – бұл сипаттаманың ерекшелігі, ол тек физикалық беру ортасының параметрлерін ғана емес, сонымен қатар осы Орта бойынша дискретті Ақпаратты таратудың таңдалған тәсілінің ерекшеліктерін көрсетеді. Коммуникациялық құрылғының таратқышы арнаның өткізу қабілетіне тең жылдамдықпен жұмыс істеуі тиіс. Әзірленіп жатқан жүйесінде шешілді пайдалануға болмайды қандай да бір белгілі бір түрі қосылыстар. Физикалық ақпарат тасығыштар сипаттамалардың кейбір жиынтығымен абстрактылы ұсынылған. Сонымен қатар, байланыс желілерінің өткізу қабілеті мен таратқыштың биттік жылдамдығы таңдалып алынды. Бұл сипаттамалар байланыс сапасын және деректерді берудің кідіруін дұрыс бағалауға мүмкіндік береді. Бірнеше компьютерді желіге біріктіре отырып, байланыс конфигурациясын немесе топологияны таңдау қажет. Желі топологиясы деп жоғары нүктелеріне желінің соңғы түйіндері (мысалы, Компьютерлер) және коммуникациялық жабдықтар (мысалы, маршрутизаторлар) сәйкес келетін, ал қабырғаларға шыңдар арасындағы физикалық немесе ақпараттық байланыстар сәйкес келетін баған конфигурациясы түсініледі. Физикалық және логикалық байланыстардың топологиялары, сәйкесінше, желінің физикалық және логикалық құрылымы бар. Физикалық байланыстардың конфигурациясы компьютерлердің электрлік

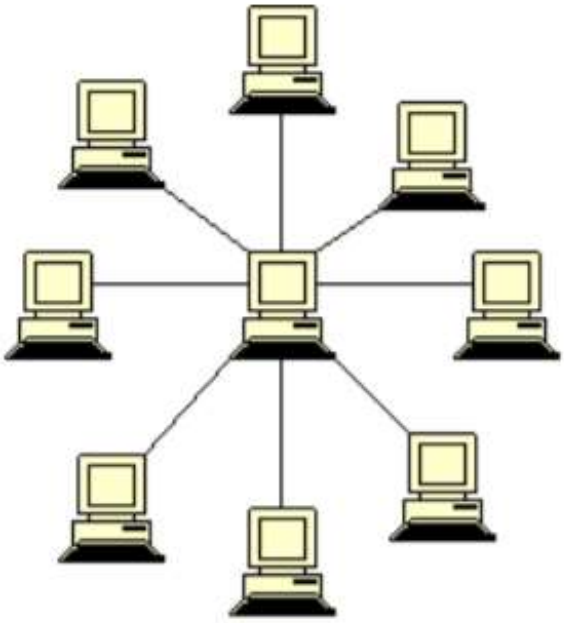
қосылыстарымен анықталады және тораптары компьютерлер мен коммуникациялық жабдықтар болып табылатын баған түрінде ұсынылуы мүмкін, ал қабырғалары тораптардың жұптарын байланыстыратын кабельдің 18 кесіндісіне сәйкес келеді. Логикалық байланыстар желі бойынша ақпараттық ағындардың өту жолдарын білдіреді; олар коммуникациялық жабдықты тиісті күйге келтіру жолымен құрылады. Көптеген ықтимал конфигурациялар арасында Толық байланысты және толық емес байланыс бар. Толық байланыс топологиясы әрбір компьютер басқалармен тікелей байланысты желіге сәйкес келеді. Оның схемасы 1.7- суретте бейнеленген.



1.7 сурет - Толық байланыс топологиясы

Барлық басқа нұсқалар екі компьютер арасында деректерді алмасу үшін басқа желі тораптары арқылы деректерді транзиттік жіберу талап етілуі мүмкін толық емес топологияларға негізделген. 1.8-суретте "жұлдыз" топологиясының схемасы – байланыссыз топологиялардың бір түрі бейнеленген [9].

Толық байланысты топология (толық график) - әр жұмыс станциясы басқаларымен байланысқан компьютерлік желі топологиясы. Бұл опция қисынды қарапайымдылығына қарамастан, күрделі және тиімсіз. Әр жұп үшін тәуелсіз сызық бөлінуі керек, әр компьютерде желіде қанша компьютер болса, сонша байланыс порты болуы керек. Осы себептерге байланысты желі тек салыстырмалы түрде аз мөлшерге ие бола алады. Көбінесе бұл топология көп станокты жүйелерде немесе аз жұмыс станциялары бар кең ауқымды желілерде қолданылады.



1.8 сурет - «Жұлдыз» топологиясы

1.6 Арналық деңгей

Арналық деңгей желілік деңгей үшін қосылымның ашықтығын қамтамасыз етеді. Ол үшін оған келесі қызметтерді ұсынады:

- өзара әрекеттесетін тораптар арасында логикалық қосылыс орнату;
- таратқыш және ақпарат қабылдағыш жылдамдығын қосу шеңберінде келісу;
- сенімді берілуді қамтамасыз ету, қателерді табу және түзету.

Құрылғы арасында логикалық қосылысты орнату міндеті коммутация механизмінің көмегімен шешіледі. Коммутация соңғы тораптарды транзиттік тораптар желісі арқылы қосу деп аталады. Жөнелтушіден алушыға дейінгі жолда жатқан тораптардың жүйелілігі маршрут құрайды. Бір транзиттік торап арқылы бірнеше маршруттардан өтуі мүмкін, сондықтан ол қажетті торапқа әкелетін өзінің интерфейсіне олардың әрқайсысын беруді қамтамасыз ету үшін өзіне келіп түскен деректер ағындарын тани білуі тиіс. Ақпараттық ағыммен, немесе ағынымен деректер деп атайды үздіксіз дәйектілігі деректер, біріккен жиынтығы жалпы белгілері бөлетін бұл деректер жалпы желілік трафик. Ағынның белгілері жаһандық немесе жергілікті болуы мүмкін. Ағынның идентификациясы үшін соңғы тораптардың адрестерінің жұбы-жаһандық белгі үлгісі. Құрылғы шегінде жергілікті ағындарды анықтайтын белгінің мысалы деректер келіп түскен интерфейс идентификаторы бола алады . Коммутация есептерін шешудің екі негізгі тәсілі: арналарды коммутациялау және пакеттерді коммутациялау. Арналардың коммутациясы таратушы және қабылдаушы тораптар арасында үздіксіз байланысты алдын ала орнатуды талап етеді, бұл деректерді ортақ учаскелері бар бағыттар бойынша беруге мүмкіндік бермейді.

Кезінде коммутация пакеттер берілетін барлық деректер разбиваются бастапқы торабында бөлігінде, деп аталатын пакеттермен. Содан кейін пакеттерден деректер өрісінен және тақырыптан тұратын кадрлар қалыптастырылады. Пакет бір немесе бірнеше кадрлардың деректер өрісіне орналастырылады, ал кадр тақырыбы қызметтік ақпаратпен толтырылады. Мұндай тәсіл желінің бір жеке учаскесі бойынша бірнеше ақпараттық ағындардың өту мүмкіндігін қамтамасыз ете отырып, тұрақты қосылыс орнатпай пакеттерді жіберуге мүмкіндік береді [10].

1.7 Желілік деңгей

Желілік деңгей жөнелтушіден алушыға дейін пакеттерді жеткізу маршруттарын әзірлеуге жауап береді. Ол үшін, маршрутизаторлар арасында бірнеше транзитті учаскелерден өту қажет болуы мүмкін. Желі деңгейі ең төменгі деңгей болып табылады, ол бүкіл жол бойынша деректерді бір-бірінен екіншісіне беруге байланысты. Осы мақсаттарға қол жеткізу үшін желілік деңгей желінің топологиясы туралы ақпаратқа (яғни барлық маршрутизаторлар мен байланыстардың жиыны туралы) ие болуы және ол жеткілікті үлкен болса да, осы желі бойынша қажетті жолды таңдау қажет. Сонымен қатар, маршрутизаторларды таңдау кезінде маршрутизаторлар мен байланыс желілерінің жүктемесі мүмкіндігінше біркелкі болуы тиіс. Соңында, егер көзі мен қабылдағышы әртүрлі желілерде болса, дәл осы желілік деңгей желілердегі айырмашылықтарға байланысты мәселелерді шеше білуі тиіс . Сонымен қатар, әр түрлі технологиялар негізінде құрылған желілерді өзара байланыстыру үшін қосымша құралдар қажет және мұндай құралдар желілік деңгейді ұсынады. Желілік деңгейдің функциялары:

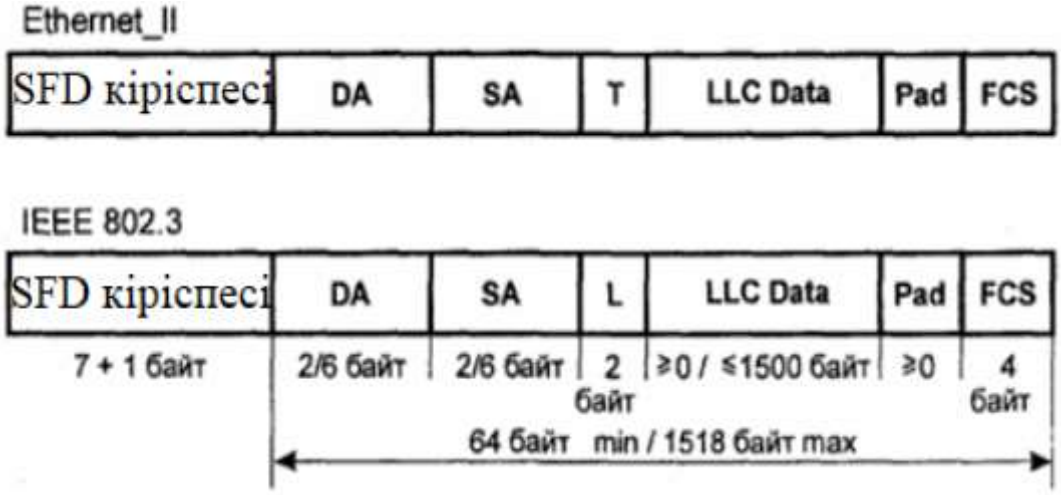
– хаттамалар тобы;
– арнайы маршрутизаторлар құрылғылары іске асырылады [11].

Маршрутизатор функциясының бірі желінің физикалық байланысы болып табылады. Маршрутизатор бірнеше желілік интерфейстерді, ұқсас интерфейстерге компьютер, әрбір мүмкін қосылған бір желісі. Осылайша, маршрутизатордың барлық интерфейстерін әртүрлі желілердің тораптары деп санауға болады. Маршрутты анықтау желілік деңгейдің маңызды міндеті болып табылады. Маршрут адресатқа кіру үшін пакеттен өтуі тиіс желілердің (немесе маршрутизаторлардың) кезектілігімен сипатталады. Бұл жағдайда маршрутизатор желі арасындағы байланыс топологиясы туралы ақпаратты жинайды және осы ақпараттың негізінде адресация кестелерін құрастырады, бұл жағдайда маршруттау кестелерінің арнайы атауы бар. Жіберу үшін пакет арқылы кезекті желісі, желілік деңгейі орналастырады, оның жолында деректер кадрдың тиісті арналық технологиясын көрсете отырып, атауында кадр каналдық мекенжайы интерфейс келесі маршрутизатордың. Желі өзінің арналық технологиясын пайдалана отырып, берілген мекен-жай бойынша оған инкапсуляцияланған пакетпен кадрды жеткізеді. Маршрутизатор келіп жеткен кадрдан пакетті алады және қажетті өңдеуден кейін келесі желіге тасымалдау үшін пакетті жібереді. Осылайша, желілік деңгей желінің бірлескен жұмысын

ұйымдастыратын үйлестіру рөлін атқарады. Маршрутын анықтау қиын міндет болып табылады, әсіресе, желі конфигурациясы мынадай жұп арасындағы өзара іс-қимыл жасайтын желілік интерфейстердің көптеген жолдары. Көбінесе таңдау кейбір критерий бойынша бір оңтайлы маршрутта тоқтатады. Оңтайлылық критерийі метрика деп аталады. Мысалы, маршруттың ұзындығын өлшеу үшін әртүрлі метриктер – транзиттік тораптардың саны, маршруттың сызықтық ұзақтығы және тіпті оның ақшалай мәндегі құны пайдаланылуы мүмкін. Ол үшін әрбір арна-учаскенің ұзындығын, оның кері өткізу қабілетін сипаттайды. Ақпараттық ағындардың топологиясы мен құрамы өзгеруі мүмкін болғандықтан (тораптардың істен шығуы немесе жаңа аралық түйіндердің пайда болуы, мекенжайлардың өзгеруі немесе жаңа ағындарды анықтау), маршруттарды анықтау және тапсыру міндеттерін шешу желінің жай-күйін тұрақты талдауды және маршруттар мен маршруттау кестелерін метрикалардың өзгеруіне сәйкес жаңартуды болжайды.

1.8 Ethernet желісі

Ethernet-қазіргі уақытта әлемдегі компьютерлік желілердің ең көп таралған түрі. Ethernet стандарттары Физикалық деңгейде сымды қосылыстар мен электр сигналдарын, кадрлар пішімін және ортаға қатынауды басқару протоколдарын – арналық деңгейде анықтайды. Кадр пішімі деректерді жіберу үшін қолданылатын кадр пішімі суретте көрсетілген. 1.9-суретте көрсетілгендей кадрдың басында Preamble (кіріспе, тақырып) ұзындығы 8 байт өрісі орналасқан, онда 10101010 тізбегі бар. Соңғы байт кадрдың бастапқы бөлгіші деп аталады (Start of Frame Delimiter).



1.9 сурет - Ethernet кадр пішімі

Содан кейін екі мекен-жай: алушы мен жіберуші. Әр адам 6 Байттан алады. Сонымен қатар, әрбір желілік карта (желілік интерфейс) жасау кезінде жазылған бірегей алтысайттық нөмір (MAC - мекен-жайы) болуы тиіс. Бұл

нөмір кадр жіберушісі мен алушыны сәйкестендіру үшін пайдаланылады. Содан кейін кадрда берілетін деректер түрін сипаттайтын Type өрісі және көлемі 1500 байт шектелген деректер өрісі болады. Соңғы жолында кадр Ethernet стандартты – Checksum, құрамында бақылау сомасын тудыратын 32-биттік код CRC мүмкіндік береді табуы керек. Ethernet желілеріндегі Коммутация пакеттерді коммутациялау механизмі қолданылады. Коммутация арнайы коммутатор құрылғыларымен орындалады. Коммутаторлар кадрларды осы кадрлар арналған порттарға ғана береді. Ол кезде портқа коммутатор келеді кадр, коммутатор тексереді MAC-мекен-жайы және біледі, қандай порт бұл кадр беруге керек. Ол үшін арнайы коммутация кестесі, салыстыратын MAC-адрестері мен порттардың нөмірлері қолданылады. Одан әрі коммутатор кадрды алушының портына жібереді. Алушы порты содан кейін тағайындалған станцияның кадрын оларды қосатын байланыс желісі бойынша жібереді. Коммутация кестесін құру үшін мөлдір көпір алгоритмі қолданылады. Коммутатор өзінің адрестік кестесін оның порттарына қосылған сегменттерде айналатын трафикті пассивті бақылау негізінде құрастырады. Бұл жағдайда коммутатор оның порттарына келетін кадр көздерінің мекен-жайларын ескереді. Жақтаудың бастапқы мекен-жайы бойынша, көпір бастапқы түйін бір немесе басқа желілік сегментке жатады деген қорытындыға келеді. Коммутатордың әр порты өз сегментінің соңғы түйіні ретінде жұмыс істейді, бір ерекшелік - порттың өзінің MAC мекен-жайы болмауы мүмкін, өйткені ол портқа түсетін барлық кадрлар, тағайындалған мекен-жайына қарамастан, біраз уақыт сақталатын болған кезде, ол кадрдың заңсыз түсіру режимінде жұмыс істейді. буферлік жад қосқышы. Коммутаторлардың функционалдығын елеулі шектеу - бұл цикл тәрізді желілік конфигурацияларды қолдаудың болмауы. Ілмектердің болуының салдары:

- жақтауды «көбейту», яғни оның бірнеше данасының пайда болуы;
- кадрдың көшірмелерін бір-біріне қарама-қарсы бағытта циклмен аяқтау, бұл желінің қажетсіз трафикпен бітелетінін білдіреді;
- мекенжай кестелерінің көпірлері арқылы тұрақты қайта құру. Артық байланыстарды бұғаттау қажет, яғни оларды белсенді емес күйге ауыстыру қажет.

Қарапайым топологиясы бар желілерде бұл міндет коммутаторлардың тиісті порттарын бұғаттау жолымен қолмен шешіледі. Күрделі байланыстары бар үлкен желілерде ілмектерді автоматты түрде табу міндетін шешуге мүмкіндік беретін Алгоритмдер қолданылады. Олардың ішінде ең танымалдары-сақиналы ағаш (Spanning Tree Algorithm, STA) принципін пайдаланатын STP және RSTP алгоритмдері. Артық байланыстарды қолданудың тағы бір нұсқасы байланыс желілерін агрегациялау болып табылады. Байланыс желілерін агрегациялау техникасының жабатын ағаштың алгоритмінен айырмашылығы жеткілікті қағидатты:

- STP және RSTP хаттамалары артық байланыстарды ыстық резервке ауыстырады, жұмыс жағдайында желі сегменттерінің байланыстылығы үшін

қажетті желілердің ең аз жиынтығын қалдырады. Бұл жағдайда желінің сенімділігі артады, бірақ оның өнімділігі емес;

- физикалық арналарды агрегациялау кезінде барлық артық байланыстар жұмыс жағдайында қалады, нәтижесінде желінің сенімділігі де, оның өнімділігі де артады, өйткені бірнеше физикалық арналар бір логикалық біріктіріледі,оның өткізу қабілеті біріктірілген байланыс арналарының жиынтығы болады.

1.9 Деректерді тасымалдау

Деректерді тасымалдау кезінде ақпарат пакетке «оралады», жоғарғы (қосымша) қабаттан бастап төменгі (физикалық) деңгейге дейін, бұл процесс инкапсуляция деп аталады. Содан кейін пакет желіге жіберіледі. Оны қабылдаған кезде, ол төменнен жоғарыға қарай «оралады» және бұл процесті инкапсуляция деп атайды.

Компьютерлік желілер:

- жергілікті желілер (LAN, Local Area Network) - салыстырмалы түрде шағын ауданды (бөлме, кеңсе, ғимарат) қамтитын компьютерлік желі;
- ғаламдық желілер (WAN, Wide Area Network) - әдетте, жергілікті желілердің үлкен санын біріктіру.

Интернет (Internet) - бұл мыңдаған корпоративті, ғылыми, мемлекеттік және үйдегі компьютерлік желілерден тұратын ғаламдық желі.

Жергілікті және ғаламдық желілердегі желілік жабдықтар арасындағы байланыс үшін әдетте желілік деңгей протоколы - IP (Internet Protocol) қолданылады. Қазіргі уақытта хаттаманың екі нұсқасы бар:

- IPv4 - әр хостқа 32-биттік IP-мекен-жай беріледі (4 байт - 4 октет);
- IPv6 - әр хостқа 128-биттік IP-мекен-жай беріледі (16 байт - 8 топ).

IP-адрестің форматы (IPv4) - 32 биттік екілік сан, қарапайымдылығы үшін бұл сан әрқайсысы 8 бит 15-тен сегіздікке бөлініп, нүктемен бөлінген. Әр октеттегі екілік сандар 0-ден 255-ке дейінгі ондық мәндерге ауыстырылады.

Жергілікті желілерде ғаламдық желіде қолданылмайтын жеке, ішкі («сұр» жаргонымен) деп аталатын арнайы IP-адрестер (IPv4 протоколы) қолданылады:

- 10.0.0.0 - 10.255.255.255;
- 72.16.0.0 - 172.31.255.255;
- 192.168.0.0 - 192.168.255.255.

Мұндай мекен-жайларға қажеттілік мұндай үлкен өсу мен желіні пайдалану күтілмегендіктен пайда болды. Әрине, IP-мекен-жай санын көбейту мәселесі қазір IPv6 хаттамасымен шешіледі, бірақ қазіргі уақытта бұл хаттама әлі кең қолданыла қойған жоқ.

1.10 Маршруттау

Маршруттау - бұл OSI / ISO моделінің Layer 3 құрылғыларының көмегімен желілер немесе ішкі желілер арасында мәліметтер пакеттерін қайта жіберу процесі.

Маршруттау деректер пакетін бағыттаудың тиімді жолын анықтау үшін маршруттау алгоритмдерін іске асыратын маршруттау кестелері мен хаттамаларын қолданады.

Деректерді бір желіден екіншісіне берудің неғұрлым қолайлы жолын анықтайтын құрылғы маршрутизатор деп аталады.

Желілердегі мәліметтер алмасу үшін маршрутизатор маршруттау кестесін қолдайды. Бұл желі мекенжайларының тізімі, сонымен қатар бағыттар мен байланыстар туралы мәліметтерді келесі секіргіштермен сақтайды. Осы сілтемелер арқылы құрылғы тағайындалған жерге тікелей немесе басқа маршрутизаторлар арқылы жете алатынын түсінеді. Кесте жазбалардың келесі түрлерін сақтай алады (әр желі үшін бір жазба):

- статикалық - маршрут туралы ақпарат қолмен толтырылады, бірақ бұл әдіс желі топологиясы өзгерген немесе кез-келген бөлімде істен шыққан жағдайда қиындықтарға әкеледі;
- динамикалық - толтыру маршруттау хаттамасы арқылы алынған құрылғылар арасында маршруттау туралы ақпарат алмасуының арқасында пайда болады, яғни маршрутизаторлар бір-бірімен жаңарту хабарламаларын жіберу арқылы ақпарат алмасады. Хаттамаға байланысты жаңартулар мезгіл-мезгіл немесе топология өзгерген кезде ғана келуі мүмкін.

Ең төменгі мәні бар хаттама сенімді болып таңдалады.

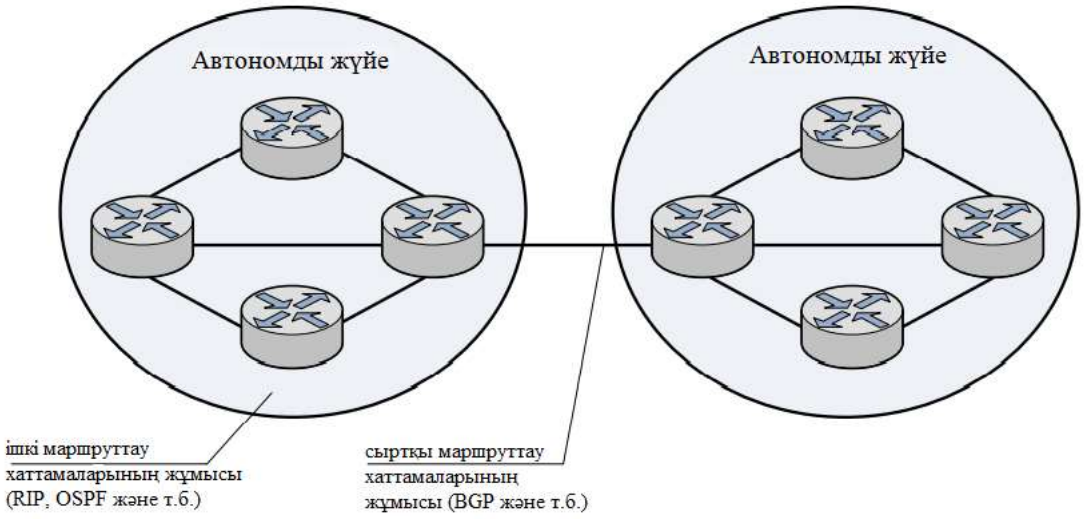
Маршруттау хаттамасы - бұл маршрутизатор басқа маршрутизаторлармен «байланыс» кезінде қашықтағы желілерге жолдарды анықтау үшін, сондай-ақ сол желілердің жазбаларын маршруттау кестесінде сақтау үшін қолданатын ережелер жиынтығы. Шатастыруға болмайтын екі ұғым бар:

- маршрутталған протокол - хосттар арасында пакеттерді тасымалдайтын желілік деңгей адресі бар кез келген хаттама. Әдетте бұл хаттамада көзден межеге дейінгі барлық маршрут туралы ақпарат болмайды. Мысалы, IP хаттамасы;
- маршруттау хаттамасы - желілер арасында маршруттау туралы ақпарат алмасуға мүмкіндік береді және динамикалық маршруттау кестелерін құруға мүмкіндік береді. Маршрутизатор пакетті қайда жіберетінін білуі керек, бірақ басқа маршрутизаторлардан кейінгі жолды білмейді.

Маршруттау хаттамалары желілер арасындағы байланыс түрімен ерекшеленеді. Бұл айырмашылық автономды жүйенің тұжырымдамасымен байланысты (1.10 – сурет).

Статикалық маршруттау - бұл маршрутизаторды конфигурациялау кезінде маршруттар нақты көрсетілген маршруттау түрі. Бұл жағдайда барлық маршруттау кез-келген маршруттау хаттамаларының қатысуынсыз жүреді.

Кейбір маршрутизаторларда желі трафигі бағытталуы керек интерфейсті көрсетуге және маршрут таңдалатын қосымша шарттарды көрсетуге болады (мысалы, cisco маршрутизаторларындағы SLA).



1.10 сурет - Хаттамалардың желілер арасындағы өзара әрекеттесу түрі бойынша жіктелуі

Автономды жүйе (АЖ) - бұл жалпы басқаруы бар желілер жиынтығы; АС-тағы маршрутизаторлардың бірыңғай маршруттау ережелері бар. Осы тұжырымдамаға сәйкес маршруттау хаттамаларының екі түрі бар:

- ішкі маршруттау хаттамасы - АБ шеңберінде ақпарат алмасу үшін қолданылатын хаттама. Мысалы: RIP, OSPF, EIGRP және т.б.;
- сыртқы бағыттау хаттамасы - автономды жүйелер арасында ақпарат алмасу үшін қолданылатын хаттама. Мысалы: BGP.

Хаттамалардың бұл бөлімі маршруттаудың иерархиялық әдісін анықтайды.

Маршруттау хаттамаларын пакеттердің көзден тағайындалған жерге өтуінің оңтайлы жолын анықтау үшін қажет болатын белгілі бір маршруттау алгоритмін қолдану арқылы жіктеуге болады.

Маршруттау алгоритмі бойынша орындалатын талаптар:

- оңтайлылық - алгоритмнің ең жақсы жолды таңдау мүмкіндігі;
- қарапайымдылығы - алгоритм үлкен бағдарламалық жасақтаманы қажет етпеуі керек;
- өміршеңдік - алгоритм күтпеген жағдайлар туындаған жағдайда жұмыс істеуі керек, мысалы жабдықтың істен шығуы, желінің жоғары жүктемесі және т. б .;
- жылдам конвергенция - бұл барлық маршрутизаторлар арасындағы ең жақсы жолдарды келісу процесі. Мысалы, егер маршрутизатор сәтсіздікке ұшыраса, желі топологиясын жаңарту туралы хабарламалар басқа маршрутизаторларға ең аз кідіріспен жетуі керек. Нәтижесінде маршрутизаторлар жолдарды қайта есептеп, оңтайлысын таңдайды. Баяу жинақталатын алгоритмдер жағымсыз салдарға әкелуі мүмкін, мысалы, циклдар пайда болады, бүкіл желінің істен шығуы және т. б.;

- икемділік - алгоритм желідегі өзгерістерге дәл және тез бейімделуі керек. Мысалы, желінің топологиясын, белгілі бір жолдардың өткізу қабілеттілігін, кідірісті және т.с.с. өзгерту.

Маршруттаудың келесі негізгі алгоритмдері ерекшеленеді:

- статикалық. Жүйелік әкімші маршруттау кестесіндегі жазбаларды қолмен тағайындайды. Бұл маршруттау әдісі үлкен желілерге сәйкес келмейді. Сондай-ақ, желінің топологиясы өзгерген кезде оны конфигурациялау қиын;
- динамикалық. Бұл алгоритм желідегі хабарламаларға байланысты өзгерістерді ескереді. Топология өзгерген кезде жолдар қайта есептеледі, содан кейін маршруттың өзгеруі туралы хабарламалардың жаңа таралуы жүзеге асырылады.

Маршруттаудың ішкі хаттамаларын келесі динамикалық маршруттау алгоритмдерінің бірін қолдану арқылы жіктеуге болады:

- арақашықтық векторына негізделген маршруттау әдісі. Бұл әдіс вектор жіберу арқылы басқа желідегі кез-келген арнаға бағыт пен арақашықтықты (мысалы, секірулердің санын) анықтайды. Көршісінен вектор алған кезде маршрутизатор қашықтықты ұлғайтады, сонымен қатар өзі білетін желілер туралы ақпарат қосады және желі бойынша жаңа векторлық мәнді жібереді. Бұл әдістің кемшілігі мынада: таратылымдар үлкен желілердегі желінің жұмысына кері әсерін тигізеді;
- сілтеме күйіне негізделген маршруттау әдісі. Маршрутизаторлар сілтеме күйіндегі хабарламаларды көршілерімен алмасады, әр маршрутизатор алынған хабарламалар негізінде желілік топология мәліметтер базасын жасайды. Осыдан кейін алгоритм қажет емес жолдарды жояды және өзінің ең қысқа жол ағашын құрастырады.

Бүкіл желі үшін жол іздеудің тамаша алгоритмі жоқ [12]. Маршруттау алгоритмдері метрикалар деп аталатын көптеген әртүрлі көрсеткіштерді қолданады. Бұл алгоритм әр жол үшін шығаратын сан. Көбінесе төменгі метрика ең жақсы жолды білдіреді. Маршрутты таңдау кезінде маршруттаудың күрделі алгоритмдері көптеген көрсеткіштерге немесе олардың тіркесіміне негізделуі мүмкін. Төменде маршруттау алгоритмінде жиі қолданылатын көрсеткіштер келтірілген:

- өту саны. Дереккөзден мақсатқа жету үшін пакеттің қанша аппараттық секірмесін жасау керектігін көрсететін сан;
- арна деректерінің жылдамдығы (өткізу қабілеттілігі);
- кешіктіру. Дестені көзден тағайындалған жерге тасымалдауға кететін уақыт. Күтуге көптеген факторлар әсер етуі мүмкін, мысалы, желі жүктемесі, өткізу қабілеттілігі және т.б.;
- жүктелуде. Желілік ресурстың, маршрутизатордың, арнаның және т.б.;
- сенімділік. Сенімділік дегеніміз байланыс арнасының сенімділігі. Желідегі кейбір арналар басқаларға қарағанда жиі істен шығуы мүмкін. Кейбір желілік арналардың істен шығуын басқа арналардың ақауларына қарағанда оңайырақ немесе тезірек жоюға болады. Сенімділік рейтингтерін тағайындау кезінде кез-келген сенімділік факторларын ескеруге болады.

2 Қолданылатын технологиялардың сипаттамасы

Бұрын жасалған тұжырымдамаларда желіде жұмыс істеу мүмкіндігі, байланыс туннельдерін құру, ішкі желілерге логикалық бөлінуден, IP-мекен-жайларды қалыптастырудан бастап, жұмыс станцияларының Интернет желісіне қол жеткізу мүмкіндігіне дейін көптеген әр түрлі міндеттер тұжырымдалды. Сонымен қатар, компьютерлік желінің дұрыс жұмыс істеуі үшін компанияның компьютерлері арасындағы желілік өзара әрекеттесу мүмкіндігі үшін желі ішіндегі барлық ағындарды бағыттау қажет. Осы міндеттердің барлығына, сондай-ақ ақауларға төзімділікті арттыру және байланысатын тоннельдер арқылы ағып жатқан ақпаратты қорғау міндеттеріне қол жеткізу үшін әр түрлі желілік хаттамаларды қолдану қажет, олардың көмегімен ішкі компьютерлік желінің барлық жұмысы ұйымдастырылатын болады.Осы технологияларды толығырақ қарастырайық.

2.1 VLAN

Желіні логикалық құрылымдау мәселесін шешу үшін VLAN (Виртуалды жергілікті желі) технологиясы қолданылады - бұл бір физикалық желілік интерфейсте бірнеше VLAN құруға мүмкіндік беретін технология, осылайша желіні логикалық ішкі желіге бөлу [13]. Технология құрылғылардың байланысу деңгейінде бір-бірімен тікелей байланысуына мүмкіндік береді, дегенмен физикалық тұрғыдан оларды әртүрлі желілік ажыратқыштарға қосуға болады. Керісінше, әр түрлі VLAN-да орналасқан құрылғылар бір-біріне байланыс деңгейінде көрінбейді, тіпті егер олар бір қосқышқа қосылса да, бұл құрылғылар арасындағы байланыс тек желіде және жоғары қабаттарда мүмкін болады, яғни маршрутизаторларды пайдалану.

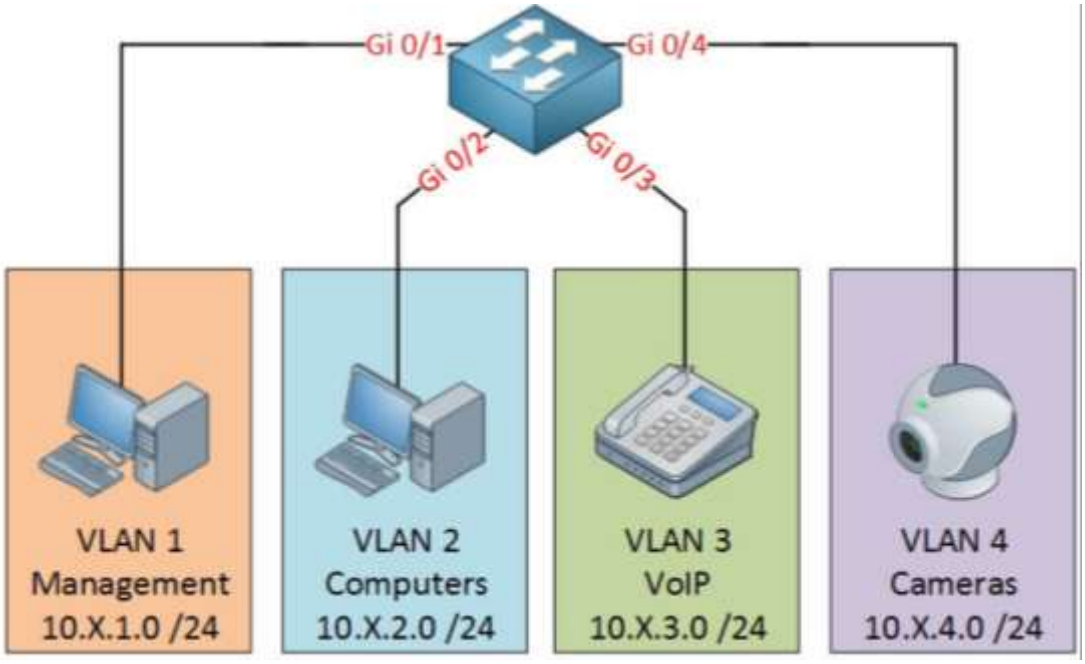
Осы технологияның негізгі артықшылықтарын атап өтейік:

- құрылғыларды икемді топтарға бөлу, әдетте бір VLAN бір ішкі желіге сәйкес келеді. Әр түрлі VLAN желілеріндегі компьютерлер бір-бірінен оқшауланған болады;
- желідегі тарату трафигін азайту, әр VLAN - бұл жеке тарату домені. Трансляция трафигі әр түрлі VLAN желілері арасында таратылмайды;
- виртуалды ішкі желілерге бөлінген желідегі желінің қауіпсіздігі мен басқарылуын арттырыңыз, әр VLAN үшін қауіпсіздік ережелері мен ережелерін қолдану ыңғайлы. Саясат бір құрылғыға емес, бүкіл ішкі желіге қолданылады;
- коммутатор сатып алудың және желілік кабельді тартудың қажеті жоқ жаңа VLAN жасау үшін жабдық пен желілік кабельдің мөлшерін азайту.

Компьютерлік желілерді жергілікті (LAN) және кең (WAN) желілерге бөлуге болады. Бір желіде белгілі бір жерде бір-бірімен байланысқан ажыратқыштар, концентраторлар, көпірлер, жұмыс станциялары және серверлер сияқты желілік құрылғылар әдетте жергілікті желілер деп аталады. Жергілікті желі де таратылатын домен болып саналады.

VLAN бірнеше желілерге бір жергілікті желі сияқты әрекет етуге мүмкіндік береді. VLAN-дың ең пайдалы элементтерінің бірі - бұл желінің

ресурстарын үнемдейтін және желінің тиімділігін арттыратын желінің кешігуін болдырмайды. Сонымен қатар, VLAN қауіпсіздік, желіні басқару және ауқымдылық сияқты салаларда сегментация мен қолдауды қамтамасыз етуге арналған. VLAN көмегімен трафикті оңай бақылауға болады (2.1-сурет).



2.1 сурет - VLAN-ның қосылу сұлбасы

Виртуалды локальды желі (VLAN) дегеніміз - белгілі бір конфигурацияларды ескере отырып, бір дәстүрлі локальды локальды желінің шектерін жергілікті желінің сегменттер тобына дейін кеңейтетін логикалық жергілікті желі (немесе LAN). VLAN - бұл логикалық тұлға, сондықтан оны құру және конфигурациялау бағдарламалық жасақтамада толығымен орындалады. Басқаша айтқанда, VLAN дегеніміз - географиялық таралуына қарамастан бір жергілікті желіде болатындай көрінетін жұмыс станциялары, серверлер және желілік құрылғылардың логикалық тобы. VLAN компьютерлер мен пайдаланушылар желісіне имитацияланған ортада бір локальді желіде бар сияқты сөйлесуге және бірдей тарату және көп арналы доменді пайдалануға мүмкіндік береді. VLAN ауқымдылықты, қауіпсіздікті және желіні басқарудың қарапайымдылығын қамтамасыз ету үшін жүзеге асырылады және өзгеретін желі талаптарына және жұмыс станциялары мен сервер түйіндерінің қозғалысына тез бейімделе алады.

Желіні VLAN желісіне бөлудің басты себебі - үлкен локальды желідегі кептелісті азайту. Бұл мәселені түсіну үшін жергілікті желілердің жылдар бойғы қалай дамығанын қысқаша қарастыруымыз керек. Бастапқыда жергілікті желілер өте тегіс болды - барлық жұмыс станциялары коаксиалды кабельдің бір бөлігіне немесе тізбекті хабтардың жиынтығына қосылды. Жалпақ жергілікті желіде кез-келген құрылғы сымға салған әрбір пакет жергілікті желінің барлық

құрылғыларына жіберіледі. Кәдімгі жергілікті желідегі жұмыс станцияларының саны өскен сайын олар үмітсіз шамадан тыс жүктеле бастады; қақтығыстар өте көп болды, өйткені көбінесе жұмыс станциясы пакет жіберуге тырысқан кезде, сымды басқа құрылғы жіберген пакет алып қойған болатын.

Бұл мәселені шешу үшін шамадан тыс жүктемені болдырмайтын үш негізгі шешім әзірленді:

- жергілікті желілерді сегментациялау үшін маршрутизаторларды қолдану;
- жергілікті желі сегменттері үшін қосқыштарды пайдалану;
- жергілікті желілерді сегментациялау үшін VLAN желілерін пайдалану.

2.2 DHCP

Компьютер желіде жұмыс істеуі үшін оған IP-адрес қажет. Компьютерге IP-мекен-жай беру статикалық (қолданушының IP-мекен-жайын тағайындау) немесе динамикалық (IP-мекен-жайды автоматты түрде тағайындау) арқылы жүзеге асырылуы мүмкін. Біздің желідегі жұмыс станцияларының саны ондаған адамды құрайтындықтан, екінші әдісті қолдану қажет.

DHCP (Dynamic Host Configuration Protocol) - компьютерлерге автоматты түрде IP мекенжайын және желіде жұмыс істеуге қажетті басқа параметрлерді алуға мүмкіндік беретін желілік хаттама. Бұл хаттама DHCP серверінен желіде жұмыс істеу үшін конфигурацияны сұрап, компьютер клиенттің рөлін атқаратын «клиент-сервер» моделі бойынша жұмыс істейді [14]. Автоматты конфигурациялау үшін клиенттік компьютер желілік құрылғыны баптау сатысында DHCP серверімен байланысады және одан қажетті параметрлерді алады. Желілік администратор сервер арқылы компьютерлер арасында таратылатын адрестер ауқымын орната алады. Бұл желілік компьютерлердің қолмен конфигурациясын болдырмайды және қателерді азайтады.

Желіде DHCP сервері IP-адрес пулын, сонымен қатар стандартты шлюз туралы ақпаратты, DNS ақпаратын және клиенттер желісін конфигурациялауға арналған басқа ақпаратты басқарады. Жаңа компьютер DHCP қолдайтын желіге қосылған кезде, DHCP серверіне барлық қажетті ақпаратты сұрау жібереді. Сұраным DHCP серверіне жеткенде, ол жаңа компьютерге жаңа IP-мекен-жай ұсынады - компьютер сол IP-мекен-жайды, сондай-ақ басқа конфигурация деректерін пайдалана алатын уақыт аралығын. Бүкіл процесс жаңа компьютер жүктелгеннен кейін бірден жүреді және оны сәтті аяқтау үшін оны желідегі басқа хосттармен IP-байланысын бастамас бұрын аяқтау керек (2.2-сурет).

DHCP - клиентке IP мекенжайын тағайындау үшін қолданылатын TCP / IP моделінің қолданбалы хаттамасы. Бұл оның атауынан туындайды - Dynamic Host Configuration Protocol. IP-мекен-жайды әр клиентке қолмен тағайындауға болады, яғни жергілікті желідегі компьютер. Бірақ үлкен желілерде бұл өте көп еңбекті қажет етеді, сонымен қатар жергілікті желі неғұрлым үлкен болса, орнату кезінде қате пайда болады. Сондықтан IP тағайындауды автоматтандыру үшін DHCP құрылды.

2.2 сурет - DHCP-дің жұмыс істеу принципі

DHCP тарату әдістері. Динамикалық бөлу: DHCP сервері динамикалық бөлуді қолдану үшін конфигурацияланған кезде, ол лизингтік саясатты қолданатындығын білдіреді. Осылайша, қол жетімді пулдан тағайындалған IP-мекен-жай бұдан былай пайдаланылмай қалған кезде, оны бассейнге итеріп жібереді, оны басқа біреу қол жетімді етеді. Бұл әдістің артықшылығы - IP-адрестер максималды түрде пайдаланылады - оларды клиент қолданбай бастағаннан кейін, олар бірден басқаларға қол жетімді. Бұл әдістің кемшілігі - клиенттің әрқашан кездейсоқ IP-мекен-жайы болады.

Автоматты бөлу: автоматты түрде бөлу әдісі динамикалық бөлу әдісіне өте ұқсас - клиент қосыла салысымен DHCP сервері оны IP-адрес пулынан IP-адресімен қамтамасыз етеді. Алайда, автоматты түрде бөлу қолданылған кезде, DHCP сервері алдыңғы IP гранттар туралы мәліметтер базасын сақтайды және клиентке ол бар болған жағдайда соңғы қолданған IP-мекен-жайын беруге тырысады.

Статикалық тарату: статикалық тарату әдісі қазіргі заманғы Интернет-провайдерлерінде кең таралған, олар теру әдістерін қолданбайды. Статикалық бөлу кезінде DHCP сервері мәліметтер базасын клиенттердің жергілікті желілерінің барлық MAC адрестерімен сақтайды және IP мекенжайын олардың MAC мекен-жайы мәліметтер базасында болған жағдайда ғана береді. Осылайша, клиенттер әр уақытта бірдей IP мекенжайды алатынына сенімді бола алады.

DHCP серверін тарату әдістерінің жиынтығын қолдана отырып конфигурациялауға болады. Мысалы, жалпыға ортақ Wi-Fi желісінде барлық белгілі хосттар мен меценаттар статикалық бөлуді қолдана алады, ал қонақтар динамикалық бөлуді қолданады. Осылайша, белгілі хосттар әрқашан бірдей IP-мекен-жайды қолдана алады және IP-адрес пулына бәріне бірдей қол жетімді.

DHCP клиентінің функциялары. Клиент тұрақты түрде IP-мекен-жай алмайды. Бөлу жалға беру уақыты желілік саясатқа байланысты және жабдықтың әр түріне әр түрлі уақыт аралықтары орнатылуы мүмкін. Егер мекен-жайға бөлінген уақыт өткен болса, DHCP клиенті оны жаңартуға өтініш беруі керек.

Жаңарту процесі алғашқы табу үдерісімен бірдей, тек бұл жолы клиенттің осы мекен-жайды бөлген сервермен байланыса алатын адресі болады. Сондықтан, Discover хабарламасын жібермей, клиент DHCP серверімен тікелей байланыса алады. Клиент бірдей IP-мекен-жайды сұрай алады немесе желілік саясат әр жаңартуды ауыстырылған IP-мекен-жаймен орындау керек деп ұйғаруы мүмкін.

DHCP анықтамасындағы екі қосымша хабар түрі клиенттің қолдануына арналған: DHCPINFORM хабарламасы және DHCPRELEASE опциясы.

DHCP Inform: DHCPOFFER хабарламасы оның пакеттік құрылымындағы бірнеше параметр өрістерінен тұрады. Алайда, сервер бұлардың барлығын сирек қолданады және кез-келгеніне мән бермейді. Клиенттің белгілі бір бағдарламасы құрылғыны желіде дұрыс баптау үшін белгілі бір ақпаратты қажет етуі мүмкін. Егер бұл құпия ақпарат DHCP ұсыныс хабарламасында жоқ болса, ол толық ақпарат сұрап Информер хабарламасын жібере алады. Егер бұл ақпарат болса, оны сервер басқа параметрлер түрінде толтырылған өрістермен бірге «Ұсыныс» хабарламасы түрінде жібереді. DHCP Inform-ті қолданудың мысалы, шолғыш бұл хабарламаны веб-проксиді автоматты түрде табу процедуралары арқылы веб-прокси алу тәсілі ретінде жиі пайдаланады.

DHCP шығарылымы клиент IP-мекен-жай бойынша жалдауды көрсетілген мерзім аяқталғанға дейін тоқтату үшін хабарлама жібереді. Хабарламаның бұл түрі хаттамалық операциялар үшін маңызды емес, өйткені жалдау шартын мерзімінен бұрын тоқтату әдетте пайдаланушы құрылғыны өшірген кезде болады. DHCP клиентіне босату туралы хабарлама жіберуге мүмкіндік беру үшін электр қуатын өшіру процесін кейінге қалдыру рәсімдері жоқ. Бұл жағдайда IP мекенжайы сол клиентке оның жалдау мерзімі аяқталғанға дейін бөлінген болып қалады, тіпті егер құрылғы осы кезеңде жұмыс істемейді.

DHCP тек қол жетімді IP-мекен-жайларды бөлуге қатысты. Ол желі түйіндерімен байланыс орнатпайды. Ол IP мекен-жайы жалға алу мерзімі ішінде пайдаланылады деп болжайды, сондықтан құрылғының желіде әлі де белсенді IP мекенжайын тағайындағанын тексермейді. Желінің конфигурациясы өзгерген жағдайда, DHCP менеджері мекен-жайларды қайта бөлуге күш салмайды.

2.3 EIGRP

Компьютерлік желінің дұрыс жұмыс істеуі үшін компьютерлер арасындағы желілік байланыс мүмкіндігі үшін желі ішіндегі барлық ағымды трафикті бағыттау қажет. Маршруттау - бұл желідегі маршрутты анықтау процесі [15].

Маршруттаудың 2 түрі бар:

- статикалық маршруттау;
- динамикалық маршруттау.

Статикалық маршруттау кезінде маршруттарды желі әкімшісі белгілейді. Маршруттаудың бұл түрі шағын желіні енгізу үшін өте ыңғайлы, бірақ үлкен желіде практикалық емес, өйткені барлық маршруттар маршрутизаторды конфигурациялау кезінде көрсетіледі. Статикалық маршрутизацияға негізделген желі тұрақсыз, сонымен қатар масштабталуы нашар. Маршруттаудың бұл түрі дамушы кәсіпорын үшін компьютерлік желіні енгізу үшін өте тиімсіз.

Динамикалық маршрутизациямен конфигурацияланған желіде маршруттау кестесі бағдарламалық өңделеді, яғни динамикалық маршруттауды іске қосу маршруттау хаттамалары арқылы жүреді.

EIGRP (Enhanced Interior Gateway Routing Protocol) - бұл 1994 жылы Cisco Systems жасаған динамикалық маршруттау хаттамасы. Хаттаманың жұмыс істеу принципі үш негізгі қадамнан тұрады. Біріншіден, маршрутизаторлар көршілес құрылғыларды ашады, содан кейін көршілер арасында топологиялық ақпарат алмасады, соңында маршрутизаторлар алынған ақпаратты талдайды және одан әр желіге ең төменгі көрсеткішпен маршруттарды таңдайды .

Осы үш қадам аяқталғаннан кейін маршрутизатор 3 кестені сақтайды: көрші құрылғылар кестесі; көрші құрылғылардан алынған топологиялық кесте; барлық белгілі ішкі желілерге оңтайлы маршруттармен маршрутизациялық кесте.

EIGRP жұмыс істеу принципі:

1)EIGRP протоколы алдымен көршілерін ашуы керек, ол үшін Hello протоколы қолданылады, ол өз кезегінде сәлем-30 пакетін жібереді (әдепкі бойынша әр 5 секунд сайын). Мультикаст пакеттерді жіберу үшін қолданылады. Сәлем пакеттері көршіңізден келгенше, маршрутизатор оны функционалды деп анықтайды. Егер сәлем пакеті көршіңізден белгілі бір уақыт ішінде келмесе (әдепкі бойынша 15 секунд), ол қол жетімсіз болып саналады.

2)Көршілер құрылғаннан кейін желі топологиясы туралы ақпарат алмасады. Өйткені, маршрутизаторлар арасында желінің толық топологиясы туралы ақпарат жіберіледі. Содан кейін, желіде өзгерген кезде маршрутизаторлар келесі пакеттермен алмасады:

- бағдарларды жаңарту пакеті (Update). Бұл пакеттерде маршруттың өзгеруі туралы ақпарат сақталады. Дестелерді мультикаст немесе біркасттық жіберуге болады;

- сұрақтар пакеті (Query). Бұл пакет маршрутизатор кез-келген маршрутты қайта есептеген кезде қажет және оның резервтік көшірмесі жоқ. Маршрутизатор көршілеріне сұраныс жібереді. Егер көршілерде маршрут болса, олар жауап пакетін жіберу арқылы жауап береді (Reply). Егер маршрут болмаса, онда олар сұранысты көршілеріне жібереді;

- сонымен қатар, жоғарыда аталған пакеттерді алғаннан кейін (жаңарту, сұрау, жауап), растау пакеттері жауап ретінде жіберіледі (Acknowledgment). EIGRP жіберілген пакеттерді жеткізуді қамтамасыз ету үшін сенімді көлік протоколын (RTP) пайдаланады. Хабарлама жоғалған жағдайда хаттама маршруттау туралы ақпаратты қайта жібереді. RTP протоколын қолдану арқылы циклдардың ықтималдығы төмендейді;

3) Әрі қарай ең жақсы жолды таңдау керек. Маршрутизаторлар топология кестесін талдайды және оның ішінен ең төменгі көрсеткіші бар жолды таңдайды. Хаттама оны салмақ коэффициенттерін қолдана отырып есептейді (әдепкі бойынша K1 = 1; K2 = 0; K3 = 1; K4 = 0; K5 = 0), сонымен қатар өткізу қабілеттілігі мен кідірісі.

Өткізу қабілеттілігін есептеу формуласы келесідей:

$$bandwidth = \frac{10000000}{bandwidth(m)} \cdot 256, \quad (2.1)$$

мұндағы өткізу қабілеттілігі (m) - бұл арнаның тағайындалған желіге дейінгі бүкіл маршрут бойынша өткізу қабілеттілігі.

Кідірісті есептеу формуласы келесідей:

$$delay = delay(s) \cdot 256, \quad (2.2)$$

мұндағы delay(s) - бұл тағайындалған желіге дейінгі маршруттағы барлық маршрутизаторлардың жалпы кідірісі.

Алынған мәндер метриканы есептеу үшін қолданылады:

$$Metric = (K1 \cdot bandwidth + \frac{K2 \cdot bandwidth}{256 - load} + K3 \cdot delay) \cdot \frac{K5}{reliability + K4}. \quad (2.3)$$

Егер коэффициенттер әдепкі бойынша қалдырылса, онда:

$$Metric = K1 \cdot bandwidth + K3 \cdot delay. \quad (2.4)$$

EIGRP артықшылықтарына мыналар жатады:

- үлкен желілердегі жылдам конвергенция;
- протокол жұмысы кезінде арналар мен процессордың жүктемесі айтарлықтай аз;
- эквивалентті емес арналар бойынша трафикті теңгеру мүмкіндігі.

EIGRP протоколының кемшілігі оның 100-ге тең түйіндер санымен шектелуі және жабық болуында, яғни оны Cisco Systems жабдықтарында жүзеге асыруға болады [16].

2.4 VPN/GRE/IPsec

Желілік өзара әрекеттесу мүмкіндігі үшін географиялық қашықтағы тармақтар арасында байланыс туннелін құру міндеті маңызды емес және әр түрлі шешімдерге ие. Біріншісі - салалық маршрутизаторлар арасында есеп беру туннелін құру, екіншісі - екі есеп беру туннелін құру, олардың біреуі күту күйінде болады және бастысы істен шыққан кезде ғана қолданылады. Сонымен қатар, бұл байланысатын тоннельдер ішкі желіден шығып, Интернет арқылы өтетін болғандықтан, ағып жатқан ақпаратты осындай туннельдер арқылы рұқсат етілмеген қолданушылардан қорғау қажет болады.

Бірінші мәселені шешу үшін VPN технологиясы қолданылады. VPN (Virtual Private Network) - бұл қосымша бағдарламалық жасақтаманы орнатудың қажеті жоқ, екі кеңсе арасында тұрақты екі жақты арнаны ұйымдастыру үшін қолданылатын технология. Интернетті негізгі филиалдар арасындағы байланыс каналы ретінде пайдалану қымбат жалға алынған жеке желілерге тиімді балама болып табылады [17]. VPN технологиясы қауіпсіздікті қамтамасыз ету және ұстап алудың алдын алу үшін туннель арқылы берілетін деректердің күрделі шифрлануын қолданады.

VPN арқылы өтетін туннельді шифрлау IPSec қауіпсіз қол жеткізу желісінің протоколы арқылы жүзеге асырылады. IPsec (IP Security сөзінің қысқаша мағынасы) - бұл Интернет-хаттама (IP) арқылы берілетін деректердің қорғалуын қамтамасыз етуге арналған протоколдар жиынтығы.

Ол IP-дестелерді аутентификациялауға, туннельдеуге және шифрлауға арналған. IPSec мөлдір және барлық желілерде жұмыс істей алатындығымен өте ыңғайлы. IPSec туннельді бастау кезінде пайдаланушыларды немесе компьютерлерді анықтаудың стандартты әдістерін, туннельдегі соңғы нүктелер арқылы шифрлауды пайдаланудың стандартты әдістерін және соңғы нүктелер арасында шифрлау кілттерін алмастыру мен басқарудың стандартты әдістерін ұсынады.

Осылайша, қауіпсіз байланыс туннелін құрудың бірінші тапсырмасын шешу үшін IPSec хаттамасымен деректерді шифрлаумен VPN туннелі жасалады. Екінші міндет екі есептік туннельдің болуын және олардың біреуі істен шыққан жағдайда оларды автоматты түрде конфигурациялауды көздейтін болғандықтан, ақауларға төзімді туннель мәселесін шешу үшін бұрын сипатталған EIGRP протоколы қолданылады. Алайда, EIGRP протоколының жұмысы жақын көршілерді іздеу сатысында пакеттерді таратуға негізделгендіктен, есепті VPN туннелін салуға арналған бұрын сипатталған хаттама бұл мәселені шешуге жарамайды, VPN протоколының ерекшеліктерінің бірі таратылым трафигінен өтпеу. Сондықтан, есепті туннельді шешу керек екінші тапсырма GRE протоколын қолданады.

GRE (Generic Encapsulation) - бұл Cisco Systems компаниясы жасаған туннельді пакеттік протокол. Бұл протокол пакеттерді бір желіден екінші желіге жіберу үшін қолданылады. GRE туннелі - бұл нүктеден нүктеге қосылу және оны деректерді шифрлаусыз, VPN туннелінің түрлерінің бірі деп санауға болады. GRE-дің басты артықшылығы - оны қолданатын маршруттау протоколдарының құрылған туннель арқылы өтуіне мүмкіндік беретін трафикті тарату мүмкіндігі .

Осылайша, екінші мәселені шешу үшін, ақауларға жол бермейтін есептік туннельдер құру үшін EIGRP динамикалық маршруттау хаттамасымен GRE протоколы қолданылады. GRE протоколы, VPN-ге қарағанда, әдепкі бойынша туннель арқылы өтетін мәліметтерді шифрлауды қажет етпейтіндіктен, оны қосымша конфигурациялау қажет. Ол үшін IPSec деректерінің қорғалуын қамтамасыз ету үшін бұрын аталған хаттамалар жиынтығы қолданылады. Бұл динамикалық EIGRP маршрутизациясы бар және IPSec-пен қорғалған 2 GRE есептік туннелін жасайды.

2.5 BGP

Сыртқы маршруттау хаттамасы - BGP (Border Gateway Protocol). Қазіргі уақытта хаттаманың төртінші нұсқасы күшінде, қалғаны ескірген болып саналады. Хаттама классыз адресті қолдайды.

BGP маршрутизаторлары желі атрибуттарынан тұратын желінің қол жетімділігі туралы ақпаратпен, ішкі маршруттау хаттамаларына арналған көрсеткіштермен алмасады. Бұл атрибуттар тағайындалған желіге өтуі керек барлық автономды жүйелердің тізімін қамтиды. Олар сондай-ақ келесі автономды жүйенің IP-мекен-жайларын және жолдың соңында желінің қалай қосылатындығын белгілейді.

BGP маршруттау хаттамасы тек автономды жүйе деңгейінде маршруттау ережелерін орындайды. Нәтижесінде, осы хаттамамен жұмыс істейтін маршрутизатор көрші автономды жүйеге өзі қолданатын жолдарды ғана жібере алады.

Автономды жүйелер мен бір жүйенің арасындағы BGP байланысының принципі басқаша. Егер маршрутизаторлар бір автономды жүйеге жатса, онда олар ішкі BGP (IBGP) арқылы жұмыс істейді, ал егер олар әр түрлі AS-да орналасса, онда олар сыртқы BGP (EBGP) арқылы жұмыс істейді.

Автономды жүйе (AS) - бұл жалпы басқаруға ие желілер жиынтығы, яғни маршруттаудың бірыңғай ережелері бар маршрутизаторлар жиынтығы. Әрбір автономды жүйенің өз нөмірі болады. Оларды тағайындайтын ұйым Интернеттің нөмірлерін тағайындау органы (IANA) деп аталады. Нөмірдің өзі 16 биттік тіркесім, яғни 1-ден 65535-ке дейінгі сан. Олардың ішінде 64512-ден 65535-ке дейінгі сандар жеке пайдалануға арналған.

Өз жұмысының басында BGP негізіндегі маршрутизаторлар ашық хабарлама жіберу арқылы әр көршісімен TCP байланысын орнатады. Бұл хабар сақталатын хабарламамен расталуы керек. Содан кейін байланыс орнатылады.

Көршілер арасындағы қарым-қатынас әр 60 секунд сайын сақтау құралдарын жіберу арқылы сақталады.

«Қатынастар» орнатылғаннан кейін маршрутизаторлар өздерінің маршруттау кестелерінде сақталатын ең жақсы маршруттармен алмасады. Әрбір маршрутизатор осы маршруттарды әр көршісінен жинап, оларды BGP топология мәліметтер базасына орналастырады. Әр желі үшін ең жақсы маршруттар топология мәліметтер базасынан BGP маршрутын таңдау процесі бойынша таңдалады және маршруттау кестесінде жазылады. Сыртқы BGP маршруттарының әкімшілік арақашықтықтары 20, ал ішкі бағыттары 200 құрайды.

Маршруттау кестесі құрастырылғаннан кейін, маршрутизаторлар желіде өзгерістер болған кезде ғана жаңартулармен (сообщение Update) алмасады. Маршрутизаторлар қателер туралы хабарламалармен және басқа қызмет ақпараттарымен (notification messages) алмасады.

BGP келесі жағдайларда қолданылуы керек:

- автономды жүйе - бұл басқа автономды жүйелерге арналған пакеттер өтетін транзиттік жүйе;
- автономды жүйенің басқа автономды жүйелермен бірнеше байланысы бар;
- автономды жүйелер арасындағы маршруттау саясаты басқарылатын болуы керек, егер кіру және шығу трафигі үшін жолды таңдауға әсер ету қажет болса.

BGP келесі жағдайларда қолданылмауы керек:

- желінің Интернетке немесе басқа автономды жүйеге бір байланысы бар;
- BGP маршрутизациясын пайдалану үшін шекаралық маршрутизатордағы процессор мен жадтың жеткіліксіз қорлары;
- автономды жүйеде қолданылатын маршруттау саясаты провайдердің автономды жүйесіндегі саясатпен үйлесімді.

2.6 RIP

Біздің жағдайымызда RIP протоколы қарастырылған. Қашықтықты векторлық бағыттаудың ең кең таралған протоколдарының бірі - RIP (Routing Information Protocol).

RIP негізгі ерекшеліктері:

- арақашықтықты векторлық бағыттау хаттамасы;
- метрикалық - ауысулар саны;
- өтулердің максималды саны - 15;
- трансляция бағытын жаңарту әдепкі бойынша 30 секунд.

RIP эволюциясы класссыз маршруттау протоколынан (RIPv1) сынпсыз протоколға (RIPv2) көшу болды. Төмендегі RIPv2 бойынша:

- ұзындығы өзгермелі масканы қолдайды;
- бағдар жаңартумен бірге ішкі желі маскасын жібереді;
- көп арналы (RIPv1 - хабар тарату);
- маршруттарды қолмен қорытындылауға қолдау көрсету;

- аутентификацияға қолдау (аутентификация процедурасы).

Класстық және классыз маршруттаудың негізгі айырмашылығы неде? Ішкі желі маскасы сияқты нәрсе бар - IP адресінің қай бөлігінде желілік адрес, ал қай бөлігінде осы желідегі хост адресі көрсетілгенін анықтайтын биттер жиынтығы. Жиын - бұл бірліктер мен нөлдердің үзіліссіз тізбегі (2.1-кесте және 2.2-кесте).

2.1 кесте - 13.14.49.121/=24 хосттың IP мекенжайы

IP мекенжайы			
13	14	49	121
00001101	00001110	00110001	01111001

2.2 кесте - 13.14.49.121/=24 хосттың маскасы

Желі			Хосттар
255	255	255	0
11111111	11111111	11111111	00000000

Маскалық жіктелу сипаттамасы:

- шағын кіру IP мекенжайы - хост 13.14.49.121/24;
- IP мекенжайы - хост 13.14.49.121;
- IP мекенжайы - желі 13.14.49.0.

«Стандартты» маскаларды қолданатын ішкі желілер үшін класстық адресация қажет.

А класының желілері үшін - маска 255.0.0.0, В класындағы желілер үшін - маска 255.255.0.0, С класындағы желілер үшін - маска 255.255.255.0.

С класында ұсынылғаннан гөрі көптеген кішігірім желілер болғандықтан, класссыз адресация енгізілді. Мұндай адресті ұйымдастыру үшін айнымалы ұзындықтағы маскалар қолданылады (2.3-кесте және 2.4-кесте).

2.3 кесте - 13.14.49.121/=26 хосттың IP мекенжайы

IP мекенжайы			
13	14	49	121
00001101	00001110	00110001	01111001

2.4 кесте - 13.14.49.121/=24 хосттың маскасы

Желі			Хосттар
255	255	255	192
11111111	11111111	11111111	10000000

Маскалық жіктелу сипаттамасы:

- шағын кіру IP-мекен-жайы - хост 13.14.49.121/26;
- IP мекенжайы - хост 13.14.49.121;
- IP мекенжайы - желі 13.14.49.64.

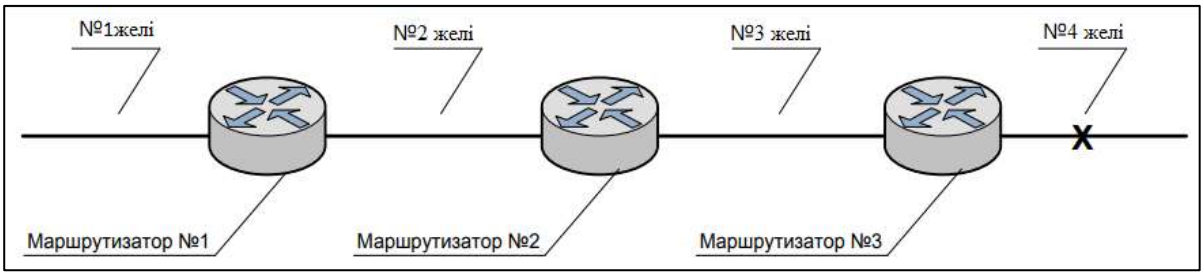
Осыны ескере отырып, класссыз маршрутизацияны қолдайтын RIPv2 протоколының мүмкіндіктері көп деп айтуға болады.

RIP жұмыс істеу принципі. Маршрутизаторлар маршруттау хабарламаларын тек көршілерімен алмастырады (тікелей байланыс). Бұл жаңартулар желі топологиясының өзгергеніне немесе өзгермегеніне қарамастан мезгіл-мезгіл жүреді және толық бағдарлау кестесін қамтиды. Кестені алғаннан кейін маршрутизатор өз кестесіне белгілі бір өзгертулер енгізеді.

RIP-де бірқатар мәселе бар. Мысалы, тізбектей жалғанған үш маршрутизатор бар (2.3-сурет). Әрбір маршрутизаторда әр желі үшін өзінің жеке маршрутизациялық кестесі бар. Күтпеген жерден №4 желі кіруге тыйым салды, сондықтан №3 маршрутизатор бұл желіге пакеттер жіберуді тоқтатады. Бірақ №1 және №2 маршрутизаторлар №4 желінің істен шығуы туралы білмейді.

№1 маршрутизатор желіге №2 маршрутизатор арқылы қол жетімді екенін көреді, яғни маршрутизация кестесінде №4 желісі бар. Маршруттау кестесі №3 маршрутизаторға жіберіледі және ол №2 маршрутизатор арқылы №4 желіге кіре алады деп ойлайды.

Осылайша, метрика шеңбер бойымен шексіздікке дейін өседі. Бұл мәселе максимумды орнату арқылы шешіледі, RIP жағдайында бұл максимум 16 секіруді құрайды.



2.3 сурет - Маршрутизаторлардың тізбектей қосылу мысалы

Кейде циклдар RIP қолданатын желілерде пайда болады. Қарастырылған мысалдан, егер №4 желі істен шықса, №1 желіден жіберілген пакет №2 және №3 маршрутизаторлар арасында шексіз жүретіндігін көруге болады, яғни цикл пайда болады. Кинкингке жол бермеудің бірнеше әдісі бар.

1)Split Horizon. Әдістің мәні маршрутизатор маршрут туралы мәліметтерді кері бағытта жібермейді.

2)Route Poisoning. Егер №4 желі сәтсіздікке ұшыраса, №3 маршрутизатор осы бағыттағы сілтемеге 16 секіру метрін тағайындайды (яғни, желі қол жетімді емес). Осыған байланысты маршрутизатор басқа маршрутизаторлардан келетін жаңартуларды (желі қол жетімді екендігі туралы ақпаратты) қабылдамайды.

3)Ұстап тұру таймері. Ұстау таймері циклдарды болдырмайды, бірақ желінің конвергенция уақытын арттырады. Стандартты RIP ұстау уақыты - 180

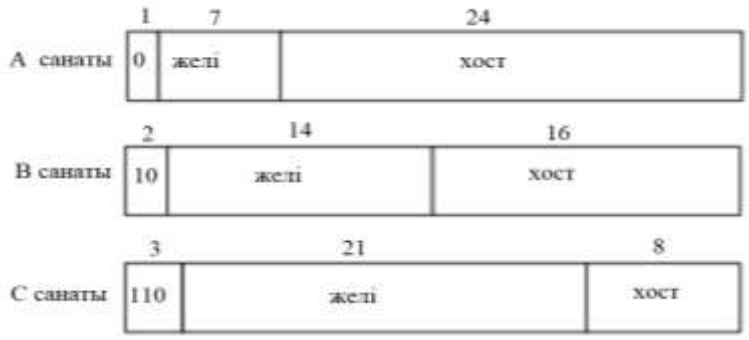
секунд. Бұл уақытты өзгертуге болады. Ең жақсы шешім - бұл кезеңді осы желі үшін маршрутты жаңартудың максималды уақытынан сәл ұзағырақ орнату.

Сонымен, егер № 4 желі істен шықса, кідіртуге арналған таймер №3 маршрутизаторда бірден іске қосылады және № 4 желіге бару мүмкін емес деп белгіленеді. Көршілес маршрутизаторлардан жақсы көрсеткіштермен жаңарту келсе, желі қол жетімді болады және таймер жойылады. Әйтпесе, жаңартулар еленбейді. Бұл желідегі жаңартуларды тарату уақытын көбейтеді.

2.7 VLSM

Негізгі зерттеу жұмысымыздың өзектілігі ішкі желілерді бөлу болып табылғандықтан VLSM маскаларымен мекенжай сызбасына қатысты IP-адрестерді тиімді бөлуді қарастырамыз. Ішкі желіні жасау арқылы желі адресін хосттың адресі немесе ішкі желі блогының қажеттіліктеріне сәйкес келтіру үшін бірнеше кіші ішкі желі блоктарына бөлуге болады. Ішкі желінің бірнеше белгілі әдістері бар, яғни VLSM және FLSM (Fixed length subnet mask). VLSM айнымалы ұзындығының ішкі желік маскасын білдіреді, мұндағы ішкі желі құрылымы бір желіде бірнеше масканы пайдаланады, яғни бір кластың A, B, C санатының немесе желінің әртүрлі ішкі желілері үшін бірнеше маскасы қолданылады. Олар айнымалы көлемде болғандықтан, ол ішкі желілердің ыңғайлылығын арттыру үшін қолданылады.

Классикалық IP-мекен-жай сұлбасында IP мекен-жайы 32 биттік ақпараттан тұрады. Бұл биттер төрт байтқа бөлінеді; ол құрылымдық немесе иерархиялық мекен-жай болып табылады және бұл схеманың артықшылығы, ол көптеген мекен-жайларды өңдей алады, атап айтқанда 4,3 млрд. IP мекенжайды желіге бөлу және түйін адресі біреудің желісінің санатын белгіленуімен анықталады (2.4-сурет).



2.4 сурет - Үш желі санатының көрінісі

Интернет құрылымшылары желінің көлеміне негізделген желілер санатын құруға шешім қабылдады. Түйіндер саны өте аз желілер үшін олар А санатты желіні құрды. Басқа шеткі нүктелерде көптеген желілерге арналған санатты С санатты желі деп, ал өте үлкен және өте кіші санаттық айырашылықты болжам бойынша В санатты желі деп аламыз. Бір желідегі кез-

келген құрылғы осы IP мекен-жайдың бір бөлігі ретінде сол адреспен бөліседі. Одан ары қарай түйін адресті тағайындайды және желідегі әрбір құрылғыны бірегей анықтайды. Бұл нөмірді хост мекен-жайы деп те атауға болады. 2.5 – кестеде үш санатты желілер туралы толығырақ мәліметтер келтірілген [18].

2.5 кесте - IP мекенжай санаттары

Мекенжай санаттары	1-ші октет диапазоны	1-ші октет биті	Негізгі ішкі желі маскасы	Желі мен хосттардың саны
A	1-127*	00000000 – 01111111	255.0.0.0	128 желі (2^7) 16777214 хосттар ($2^{24} – 2$)
B	128-191	10000000 – 10111111	255.255.0.0	16384 желі (2^{14}) 65534 хосттар ($2^8 – 2$)
C	192-223	11000000 – 11011111	255.255.255.0	2097150 желі (2^{21}) 254 хосттар (2^8 - 2)
Д	224-239	11100000 – 11101111		
E	240-255	11110000 – 11111111		

Жоғарыда айтылғандай, IP мекенжай кеңістігінде екі деңгейлі иерархия бар, онда әр адрес өзінің 32-биттік құрылымындағтьы желі адресі мен хост адресінен тұрады. Мұндай жазықтық масштабтылықты бірнеше жолмен нақты шектейді. Мүмкін, ең шегі ретінде мекен-жай кеңістігі барлық желілерді үш әр түрлі, кіші, орта және өте үлкен, көлемдегі желілердің біріне сәйкес келеді деп болжайды.

Ішкі желі маскасы - 32 биттік екілік сан; ішкі желі маскасы құрылымдық жағынан IP-адреске ұқсас. Дегенмен, ішкі желі маскасы маңызды функцияны орындайды: ол ішкі жүйені анықтау үшін IP-мекен-жайдың хост өрісінің қанша биті алынғанын соңғы жүйелерге (жергілікті желідегі маршрутизаторлар мен хосттарды қоса) айту үшін қолданылады.

Маскадағы желі адресін, сонымен қатар ішкі желі адресін анықтайтын биттер 1-ге орнатылған. Әр ішкі желідегі хост адрестері үшін пайдаланылатын қалған биттер 0-ге теңестірілген [19].

Кеңейтілген желінің префиксі. Қолданыстағы биттер әрдайым хост өрісіндегі ең сол жақ биттер екенін ескеру маңызды. Осылайша, ішкі желі мекен-жайы желі адресімен сандық жағынан сабақтас. Олар бірге желінің кеңейтілген префиксін құрайды. Қалған биттер хост идентификациясы үшін қолданылады.

Желі биттерінің өсу деңгейі қажетті ішкі желілер санына және әр ішкі желідегі қажетті хосттар санына байланысты. 2.6 – кестеде префикстің

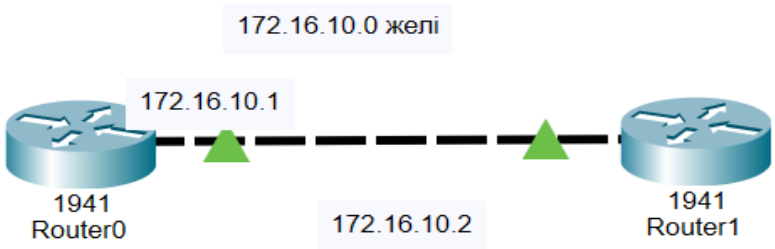
ұзындығы және B санатындағы желілерді қосудың мүмкін жолдары көрсетілген.

Ауыспалы ұзындықтағы ішкі желі маскалары. Ішкі желі, жалпы, адрестік кеңістікті тиімді пайдалануды қамтамасыз етуге арналған, бұл санатқа негізделген желілік адрес блоктарын кіші адрес блоктарына бөлуге мүмкіндік береді. Алғашқыда желіні енгізу тәсілі тиімді болмады. FLSM қалдықтарының және тиімсіздіктің көзі, барлық ішкі желілер үшін бір өлшемді маска болды. FLSM-ді енгізу IP-мекен-жайлар үшін тиімсіз болып табылады, себебі көп мекенжайлар жоғалады [19].

2.6 кесте - B санатының ішкі желісі

Желі маскасы	Префикс	Ішкі желі биті	Шеткі бит	Ішкі желі	Хосттар
255.255.0.0	/16	0	16	0(1желі)	65534
255.255.128.0	/17	1	15	2	32766
255.255.192.0	/18	2	14	4	16382
255.255.224.0	/19	3	13	8	8190
255.255.240.0	/20	4	12	16	4094
255.255.248.0	/21	5	11	32	2046
255.255.252.0	/22	6	10	64	1022
255.255.254.0	/23	7	9	128	510
255.255.255.0	/24	8	8	256	254
255.255.255.128	/25	9	7	512	126
255.255.255.192	/26	10	6	1024	62
255.255.255.224	/27	11	5	2048	30
255.255.255.240	/28	12	4	4096	14
255.255.255.248	/29	13	3	8192	6
255.255.255.252	/30	14	2	16384	2

Мысалы, 2.5 – суретте көрсетілгендей, екі маршрутизатор арасындағы сериялық байланыс сөйлесу үшін бірдей желіні бөліседі.



2.5 сурет - IP мекенжай мысалы

Бұл жерде екі IP нөмір қажет, өкінішке орай әр сериялық интерфейс үшін бір-бірден бөлінеді және сегіз биттік ішкі желі маскасы бар (яғни, 255.255.255.0), сондықтан ішкі желідегі 254 нөмірдің 252 IP-мекен-жайы ысырап болады. Осы дилемманы шешудің бір мүмкіндігі - айнымалы ұзындықты ішкі желі маскаларын (VLSM) пайдалану.

Аты айтып тұрғандай, айнымалы ұзындықтағы ішкі желі маскаларымен әр түрлі ішкі желілерге арналған әр түрлі ішкі желі маскалары бар. Сонымен, 2-суреттегі сериялық сілтеме үшін желінің мекен-жайы 172.16.10.0/30, ішкі желінің маскасы 255.255.255.252 және IP-адрестерді есептеу арқылы осы желіде тек екі хост биті қарастырылатындығын 6-кестеден көруге болады .

Сондықтан, бұл ішкі желі маскасы тек екі хост IP-ін береді ($2^2 - 2 = 2$), дәл осы сериялық сілтеме үшін қажет. Пайдаланушы қажетті IP-адрес пен желінің префиксін енгізген кезде, бағдарламалық жасақтама қажетті IP-адреске жататын желіні және Broadcast IP-адрестерін жасайды. Ол ішкі желілер санын енгізген кезде, бағдарламалық жасақтама ішкі желілер санына тең бірнеше өрістер жасайды. Келесі қадам - әрбір ұяшықта әрбір ішкі желіде қажет хост саны толтырылуы керек.

«VLSM жасау» батырмасы жоғарыда көрсетілген параметрлер енгізілгеннен кейін іске қосылады. Осы түймені басу нәтижесінде әрбір сұлба бойынша маңызды параметрлер және кесте көрсетілген кесте шығады. Бұл параметрлер - желі атауы, Net IP, start IP, End IP, BC IP, префикс, Total хосттар, пайдаланылған хосттар және қалған хосттар.

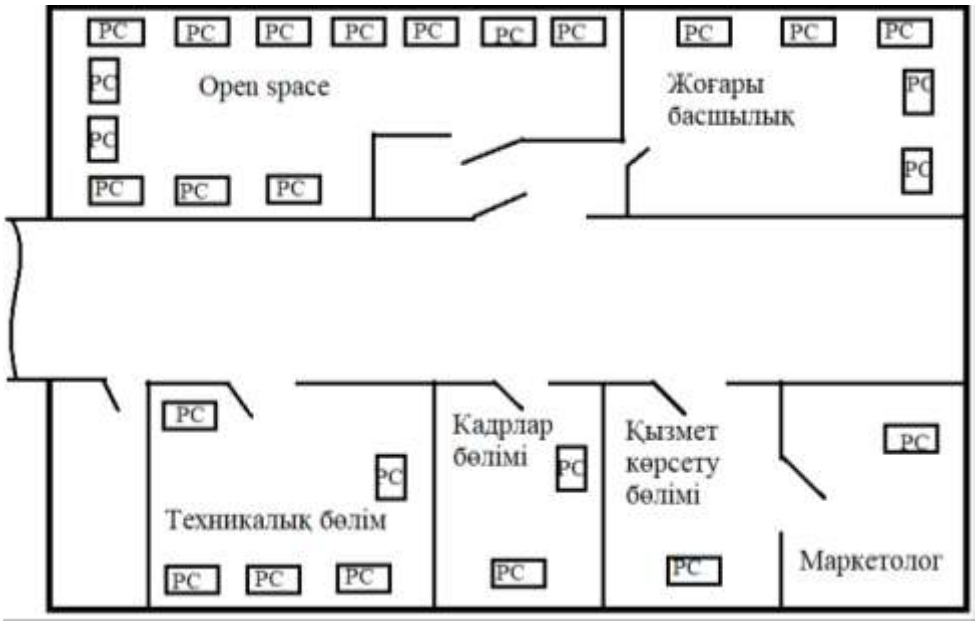
Ұсынылған топологияны ең аз маршрутизаторлармен салу және бейнелеу үшін негізгі терезеде «Сурет топологиясы» батырмасын басуға болады. Ұсынылған топологиядағы әрбір маршрутизаторда ең көп дегенде екі жылдам Ethernet порты және екі сериялық порт бар. Желінің толық IP-ақпаратын «барлық желілерді көрсету IP» командасы деп аталатын «Топологияны сызу» терезесінің жоғарғы жағындағы белгіні басу арқылы қосуға немесе өшіруге болатындығын ескеру керек.

Бұл бөлімде VLSM симуляторының алдыңғы бөлімдерде талқыланған математикалық операциядан құрастырылған бағдарламалық қамтамасыздандыруы көрсетілген. VLSM симуляторында оның жұмысын көрсететін бірнеше терезелер бар; бұл бөлімде VLSM Simulator терезелерінің жұмысы және осы терезелер арасындағы байланыс ұсынылған және түсіндірілген. Модельдеуді жүзеге асыру үшін өте аз жазбалар қажет болды (IP, префикс және ішкі желілер саны). Бұл тренажер студенттерге, нұсқаушыларға және желі инженерлеріне VLSM желісін талдауға және жобалауға барлық қажетті ақпаратты қарапайым, жылдам және қарапайым етіп беру арқылы қажет қадамдар. Сонымен қатар, бағдарламалық жасақтама желі әкімшісі үшін қажет құрал болып табылатын толық ұсынылған желілік топологияны ұсынады.

3. Виртуалды желіні модельдеу ұсынысы

Компьютерлік желіні жобалау кезінде желі параметрлерін модельдеу кезеңі маңызды болып табылады. Модельдеуді әртүрлі әдіс-тәсілдермен жасауға болады. Бірақ модельдеудің ең тиімді және үнемді тәсілі - компьютерлік модельдеу. Қазіргі уақытта компьютерлік желі параметрлерін имитациялауға мүмкіндік беретін бағдарламалық қамтамасыз ету жүйелері өте көп. Модельдеу кезінде желіні конфигурациялаудың әртүрлі нұсқалары сұрыпталады, талдаудан кейін жобалау кезеңіне арналған ең жақсы желілік параметрлер ұсынылады.

Бұл жұмыста “SunShine” компаниялары бөлімшелерінің бірінің желісін модельдеу процесі сипатталған (3.1-сурет). Оның Cisco Packet Tracer бағдарламалық жасақтамасы арқылы құрылған бірнеше бөлімі бар: техникалық бөлімі, кадрлар бөлімі, қызмет көрсету бөлімі, маркетолог, open space және жоғары басшылық. Әр бөлімде серверлер бар, оған басқа да бөлімдердің қызметкерлері кіре алады.



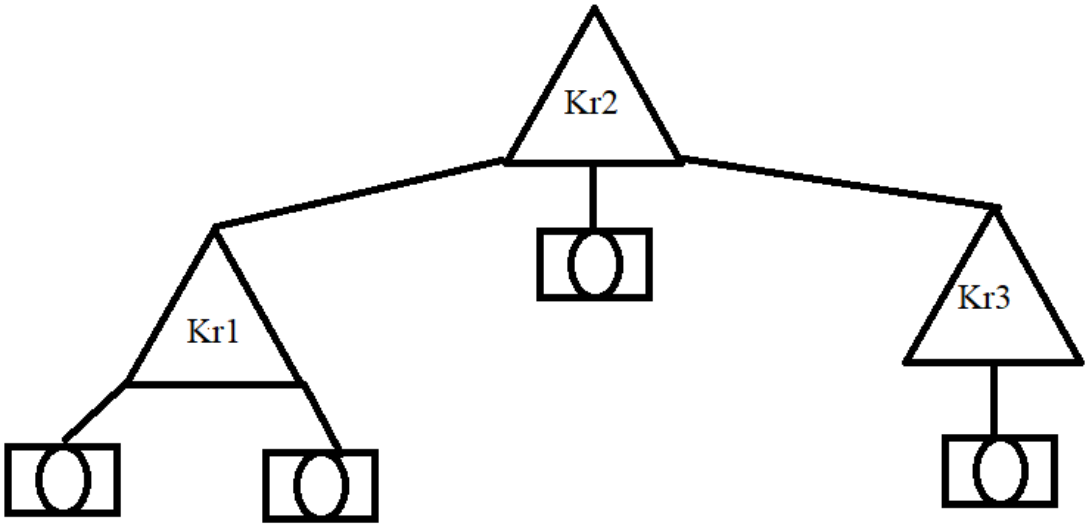
3.1 сурет - “SunShine” компания бөлімшелерінің орналасуы

Бір қарағанда, бұл теория жүзінде онша қиын емес. Әр желінің инфрақұрылымын бөлек жобалауға болатындықтан. Басқа жағынан, мұндай желіні жобалау оңай емес. Сонымен қатар, желі конфигурациясын өзгерту қажеттілігі туындауы мүмкін.

Осы себепті желінің кейбір бөліктерін одан әрі логикалық бөлумен жалпы физикалық желіні жобалау әлдеқайда жеңіл. Бұл әдіс желіні жоспарлау мен басқарудың икемді болуына мүмкіндік береді, сонымен қатар желінің қауіпсіздігін жақсартады.

3.1 Қол жетімділік деңгейінде құрастырылатын желілік топологиясын ұсыну және оңтайландыру

Қазіргі уақытта шағын және орта бизнес үшін интернетке қосылу желісін жоспарлау өзекті мәселе болып табылады. Желіні жоспарлау кезінде басты мақсат - желілік жабдықты құру және пайдалану құны төмен компанияның ресурстарына жоғары жылдамдықта үздіксіз қол жеткізуді қамтамасыз ету. Мен өз зерттеуімде мен берілген деңгей топологиясы үшін трафик ағынын оңтайландыру әдісін қарастырдым. 3.2-суретте “SunShine” компания желісінің топологиясын көре аласыз.



3.2 сурет - “SunShine” компания желісінің топологиясы

Бұл топологияда маршрутизаторларға қосылған 4 коммутаторлар бар. Коммутаторлардың әрқайсысына қосылған пайдаланушылар өздерінің алдын-ала конфигурацияланған Vlan-да жұмыс істейді. Сондықтан, мысалы, 1-коммутарторға және 4-коммутарторға қосылған пайдаланушылар Vlan1-де, ал 2-коммутатор мен 3-коммутаторды пайдаланушылар Vlan2-де жұмыс істей алады.

Телекоммуникация желісінің дайындылық коэфиценті – ең басты толыққанды көрсеткіштерінің тұрақтылығы. Бос уақыттағы нысанды пайдалану ықтималдығын анықтайтын жоспарлау кезеңін қоспағанда, нысанды мақсатты пайдалану көзделмейді [20]. Негізінен, телекоммуникация желісінде мұндай факторға оның дайындық түйіндері (телекоммуникациялық жабдық) және шекаралар (сызықтар) факторлары әсер етеді деп есептеледі. Деректердің қауіпсіздігіне бұл жұмыстың алғашқы екі дерекке дайындығы әсер етеді.

Қарастырылып отырған модельде біз үш түйіннен құралған сызықтық топологияны пайдаланамыз және осы 1-3 түйін арасындағы байланыстың болуын формуламен есептейміз. Мұнда интернет желінің сегменті ретінде алынады. Деректердің қауіпсіздік қателігінің ықтималдығын және әдеттегі

күтілетін CCI Computer and Survey Security Surveys жүйелеріндегі қателерінің қайта қалпына қою процесі. Есептеулерді орындау үшін жоғарыда көрсетілген (3.2-сурет) желілік топологиядағы схемаға қарап жүргізіледі.

3.2 Моделденген желінің дайындылық корсеткіштерін есептеу

3.2-суретте көрсетілген топология бойынша 1 және 3 түйіндердің арасындағы дайындылық корсеткіштерін төмендегі формула арқылы анықтаймыз:

$$K_{г\text{-}13} = K_{г1} \times K_{г1\text{-}2} \times K_{г2} \times K_{г2\text{-}3} \times K_{г3}, \quad (3.1)$$

мұндағы $K_{г1}$, $K_{г2}$, $K_{г3}$ – түйіндің дайындылық көрсеткіш коэфициенттері;

$K_{г1\text{-}2}$, $K_{г2\text{-}3}$, $K_{г1\text{-}3}$ – түйіндер арасындағы дайындылық көрсеткіш коэфициенттері.

$$K_{г\text{-}13} = K^3{}_{г\text{-}у} * K^2{}_{г\text{-}і}. \quad (3.2)$$

Желілік тораптағы құралдың болуы кез-келген келіңсіз жағдайды қалпына келтіру уақытын (сөндірумен байланысты) және медициналық көмек уақытын ескере отырып, жабдыққа жоспардан тыс техникалық қызмет көрсету уақытын ескере отырып есептеледі:

$$K_г = \frac{T_{mtbf}}{T_{mtbf}+(T_{тж}+T_{Қалп})}, \quad (3.3)$$

мұндағы T_{mtbf} – жойылған дестелердің орташа уақыты;

$T_{тж}$ – техникалық жабдыққа қызмет көрсетуге кететін уақыт;

$T_{қалп}$ – келіңсіз жағдайдан кейінгі жабдықты орнына келтіру уақыты.

Байқалып отырған модель қол жетімділік коэффициенті бар келесі элементтерді қамтиды: байланыс желісі, магистральды маршрутизатор және деректерге түсетін қауіп-қатерлер. Дайындылық көрсеткіш коэфициенттері телекоммуникациядағы жабдықтарда ақпараттар негізінде қарастырылады.

$K_{г\text{-}і}$ тораптарының арасындағы байланыс желісінің дайындылық көрсеткіш коэфициенттері $K_{г\text{-}і}$ = 0,9999 тең болады.

Cisco роутерларының қол жетімділік коэффициенті келесі мәліметтерге негізделген: қабылданбаған оқиғалар мен интерфейс карталары үшін орташа уақыт шеңберінен тұрады, яғни $T_{mtbf\text{-}г}$ = 7 жыл = 61320 сағат. Жыл сайынғы техникалық қызмет көрсету үшін (қажетті жабдықтарды өшіру арқылы) $T_{тж\text{-}г}$ = 4 сағат х 7жыл = 28 сағат.

Қолайсыз болтын оқиғалардан кейін құрылғының кездейсоқ істен шығуы (кей мәлеметтерге сүйене отырып 1-2 рет қызмет ету кезін мысал ретінде қарастырамыз) $T_{қалп\ -\ г}$ = 16 сағат х 2= 32 сағат. 3.3-формула арқылы $К_{г\text{-}г}$ есептейміз:

$$К_{г\text{-}г} = \frac{61320}{61320+28+32} = 0{,}99901.$$

ПАК ФПСУ-IP қол жетімділік коэффициенті төмендегідей ақпараттардан тұрады. Ол қабылданбаған оқиғалардың орта мөлшерді уақыттық платформасынан және интерфейс картасынан құралады:

$$Т_{mtbf\text{-}г} = 3 \text{ жыл} = 26280 \text{ [сағат]}.$$

Қолайсыз болтын оқиғалардан кейін жабдықтардың кездейсоқ істен шығуы (кей мәлеметтерге сүйене отырып 1 рет қызмет ету кезін мысал ретінде қарастырсақ) $Т_{қалп\text{-}г}$ = 16 сағат х 2= 32 сағат. 3.3-формула арқылы төмендегі нәтижені алуға болады:

$$К_{г\text{-}г} = \frac{26280}{26280+8} = 0{,}9998.$$

Деректердің қауіпсіздікке төнетін қатерлердің телекоммуникация желісінің қол жетімділігіне әсері BlaskBox сайтының виртуалды желісінің әрбір элементінің артықшылығымен азаяды. Деректерге қауіп төндірмеген жағдайда біз бірнеше рет дайын болатын тәуекелдерді аламыз:

$$К_{г\text{-}иб} = 1 - (1 - К_{г\text{-}у}) \times P. \qquad (3.4)$$

Деректердің қауіп-қатердің болу ықтималдылық көрсеткіштері, яғни P=0,07728 болып табылады. Ал олардың моделін қайта қалпына келтіру көп уақыт алады. Деректік қауіпсіздік $Т_{қалп}Н$ = 48сағат. Осылайша, (3.3, 3.4 формулаларынан) шығатын нәтиже:

$$К_{г\text{-}у} = \frac{8760}{8760+48} = 0{,}99456,$$

$$К_{г\text{-}иб} = 1 - (1 - 0{,}99456) \times 0{,}7728 = 0{,}99959.$$

Сәйкесінше, осынан алдында сипатталған үш нұсқаны іске асыру үшін құрылғы формуласының қол жетімділік индексі тораптарда келесідегідей есептеледі:

1)Тораптардың арасындағы ең басты байланыс жабдығы роутер болып табылады және артық жабдықтар қарастырылмайды, деректердегі қауіп-қатердің түсуі қарастырылмайды:

$$К_{г\text{-}у} = К^{3}_{г\text{-}г} \times K^{2}_{г\text{-}і}. \qquad (3.5)$$

(3.5) және (3.2) формулаларға қойып төмендегі нәтижеге қол жеткізе аламыз:

$$К_{г\,1\text{-}\,г\,3} = 0{,}99902^3 \times 0{,}998^2 = 0{,}99507.$$

2)Тораптардың арасындағы ең басты байланыс жабдығы роутер болып табылады және артық жабдықтар қарастырылмайды, деректердегі қауіп-қатердің түсуі қарастырылмайды:

$$К_{г\text{-}у} = К^3_{\,г\text{-}г} \times К^2_{\,г}. \qquad (3.6)$$

(3.6) және (3.2) формулаларға қойып төмендегі нәтижеге қол жеткізе аламыз:

$$К_{г\,1\text{-}\,г\,3} = 0{,}9998^3 \times 0{,}998^2 = 0{,}999571.$$

3)Тораптардың арасындағы ең басты байланыс жабдығы роутер болып табылады және қосымша құрылғы – ПАК ФПСУ-IP, деректердің қауіп-қатердің түсуі қарастырылмайды:

$$К_{г\text{-}у} = К^3_{\,г\text{-}г} \times К^2_{г\text{-}иб}. \qquad (3.7)$$

(3.7) және (3.2) формулаларға қойып төмендегі нәтижеге қол жеткізе аламыз:

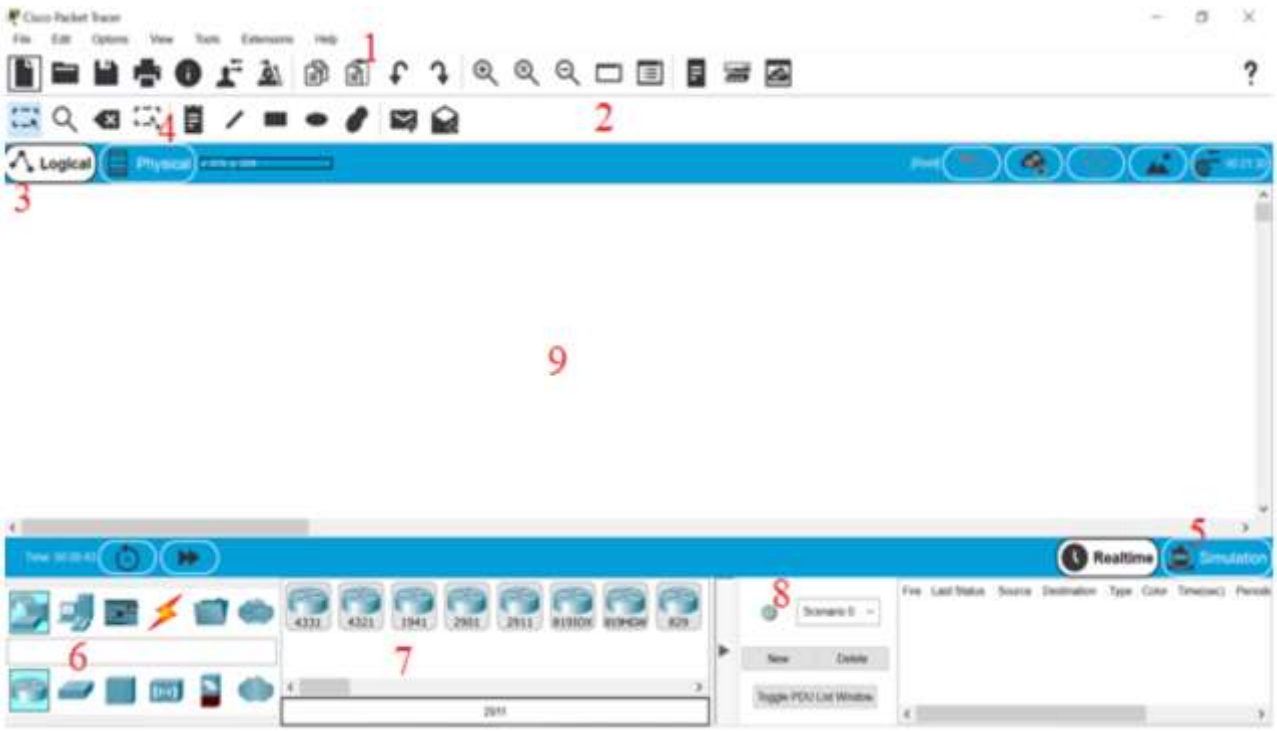
$$К_{г3\text{-}\,13} = 0{,}99872^3 \times 0{,}998^2 = 0{,}99417.$$

Тиімділік жағын қорытындылай келе , деректерді сақтау үшін ПАК ФПСУ-IP қорғанысы алынады, ол роутердің байланыс орталығында орналасуымен салыстырғанда қол жетімділік деңгейінің төмендеуіне қарамастан, деректерді беретін факторлардың болуын арттырады қауіпсіздікке төнетін қатерлер болып табылады.

3.3 Cisco Packet Tracer виртуалды бағадарламалық жасақтамасы.

Packet Tracer әр түрлі мақсаттағы құрылғылардың көп мөлшерін, сондай-ақ кез-келген көлемдегі желілерді жоғары күрделілік деңгейінде жобалауға мүмкіндік беретін көптеген қосылыстардың көптеген түрлерін модельдеуге қабілетті. Cisco Packet Tracer интерфейсі 3.3-суретте көрсетілген.

Тренажер Cisco 800, 1800, 1900, 2600, 2800, 2900 сериялы маршрутизаторлар мен Cisco Catalyst 2950, 2960, 3560 қосқыштарын, сондай-ақ ASA 5505 брандмауэрін қолданады.Сымсыз құрылғылар Linksys WRT300N маршрутизаторымен ұсынылған, қол жетімділік нүктелер мен ұялы мұнаралар. Сонымен қатар, DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP және EMAIL серверлері, жұмыс станциялары, компьютерлер мен маршрутизаторларға арналған әртүрлі модульдер, IP телефондары, смартфондар, хабтар, сонымен қатар WAN-ды эмуляциялайтын бұлт бар.



3.3 сурет - Cisco Packet Tracer эмуляторының негізгі терезесі

Cisco packet tracer эмуляторының сипаттамасы:

1) Бағдарламаның негізгі мәзірі.

2) Құралдар тақтасы - кейбір мәзір пункттерінің көшірмесін жасайды.

3) Логикалық және физикалық ұйымдастыру арасында ауысу.

4) Басқа құралдар тақтасында объектілерді таңдауға, жоюға, жылжытуға, масштабтауға, сондай-ақ ерікті бумаларды құруға арналған құралдар бар.

5) Нақты уақыт пен модельдеу арасында ауысу.

6) Соңғы құрылғылар тобы мен байланыс желілері бар панель.

7) Соңғы қондырғылардың өзінде мұнда барлық типтегі ажыратқыштар, түйіндер, кіру нүктелері, өткізгіштер бар.

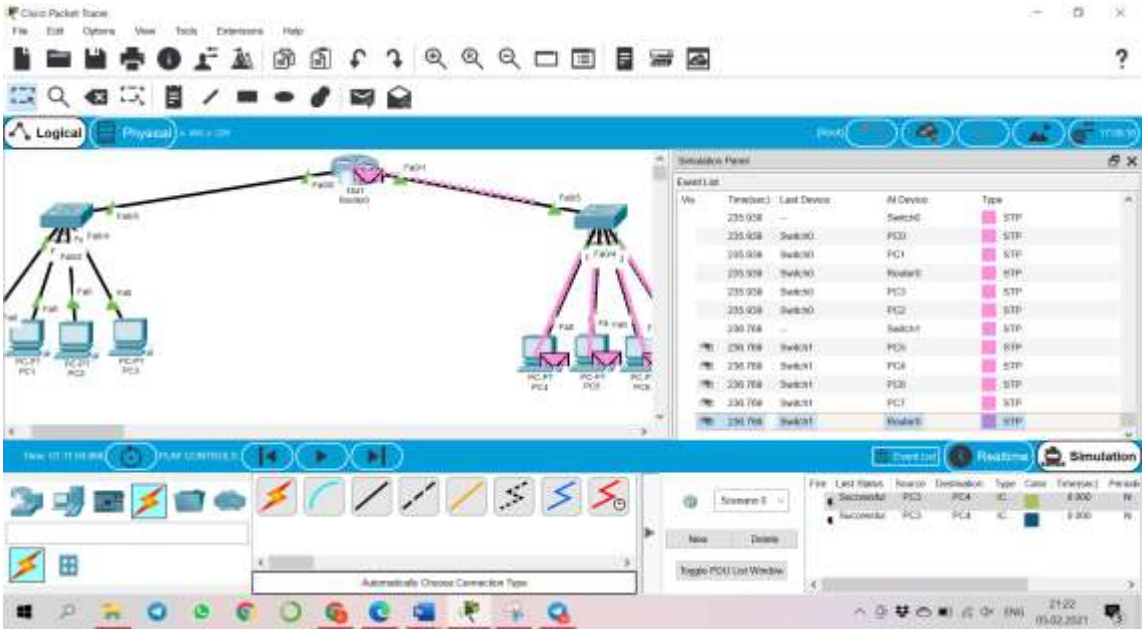
8) Сценарийлерді жасауға арналған панель.

9) Жұмыс кеңістігі.

Төменде 3.4-суретте көрсетілгендей ақпараттардың компьютерлар арасындағы дестелер түрінде сәтті жіберілуіғ коруге болады.

Желілік құрылғыларды әр түрлі типтегі кабельдер арқылы қосуға болады, мысалы, алға және кері патч сымдар, оптикалық және коаксиалды кабельдер, сериялық кабельдер және телефон жұптары.

Бұл сізге желілердің күрделі сызбаларын жасауға, желінің топологиясын тексеруге мүмкіндік береді. Алайда, құрылғылардың іске асырылған функционалдығы шектеулі және нақты жабдықтың барлық мүмкіндіктерін қамтамасыз ете алмайды.



3.4 сурет - Деректердің компьютерлар арасындағы хаттар түрінде сәтті жіберілуі

3.4 Cisco Packet Tracer бағдарламалық жасақтамасында қолданылған керекті әдіс-тәсілдер мен құрал жабдықтар.

Маршрутизаторлардың үш санаты бар:

- бірінші санаттағы маршрутизаторлар кәсіпорын желілерін қосуға көмектеседі. Мұндай санаттағы маршрутизаторлар протоколдар мен интерфейстердің алуан түрін қолдауға қабілетті. Бұл санаттың жабдықтары өте жоғары өнімділікпен, ақаулыққа төзімділікті қамтамасыз ететін қуатты құралдардың болуымен (жеке түйін үшін де, жалпы желі үшін) және BGP және MPLS сияқты негізгі протоколдарды қолдаумен (көп протоколды жапсырманы ауыстыру) сипатталады;
- екінші санатты маршрутизаторлар жалпы кәсіптік желінің өзара байланысын, яғни корпоративті желілерді құрайды және нақты осы санатта біздің желі құрылады. Әдетте, бұл санатта маршруттаудың сәл өзгеше протоколдарын қолдауға баса назар аударылады: BGP орнына RIP немесе OSPF жиі қолданылады.Біздің жағдайымызда RIP протоколы қарастырылады. Маршруттау туралы ақпарат хаттамасы (RIP) - бұл векторлық бағыттауыш таңба ретінде қолданылатын ежелгі қашықтықтағы векторлық маршруттау хаттамаларының бірі;
- маршрутизаторлардың үшінші санаты шағын кеңселерді кәсіпорын желісімен байланыстыруға арналған. Мұнда маршрутизаторлардың бекітілген архитектурасы бар: қатаң кіріктірілген интерфейстер жиынтығы, мысалы Ethernet, xDSL, ISDN , console, interface, Lan port және т.б.

Cisco Packet Tracer бағдарламалық жасақтама студенттерге, оқытушыларға және желілік инженерлерге VLSM желісін талдауға және

енгізуге, барлық қажетті ақпаратты жылдам және қарапайым түрде ұсынуға пайдалы. Ішкі желілердің ыңғайлылығын жақсарту үшін көбінесе «ішкі желі» деп аталатын өзгермелі ұзындықты ішкі желі маскалары (VLSM) қолданылады және осы тәсілді қолдану арқылы желілерге тиімді мекенжайлар беріледі. Cisco Packet Tracer негізінде виртуалды желілерді модельдеу және құру негізгі элементтері 3.1-кестеде көрсетілген.

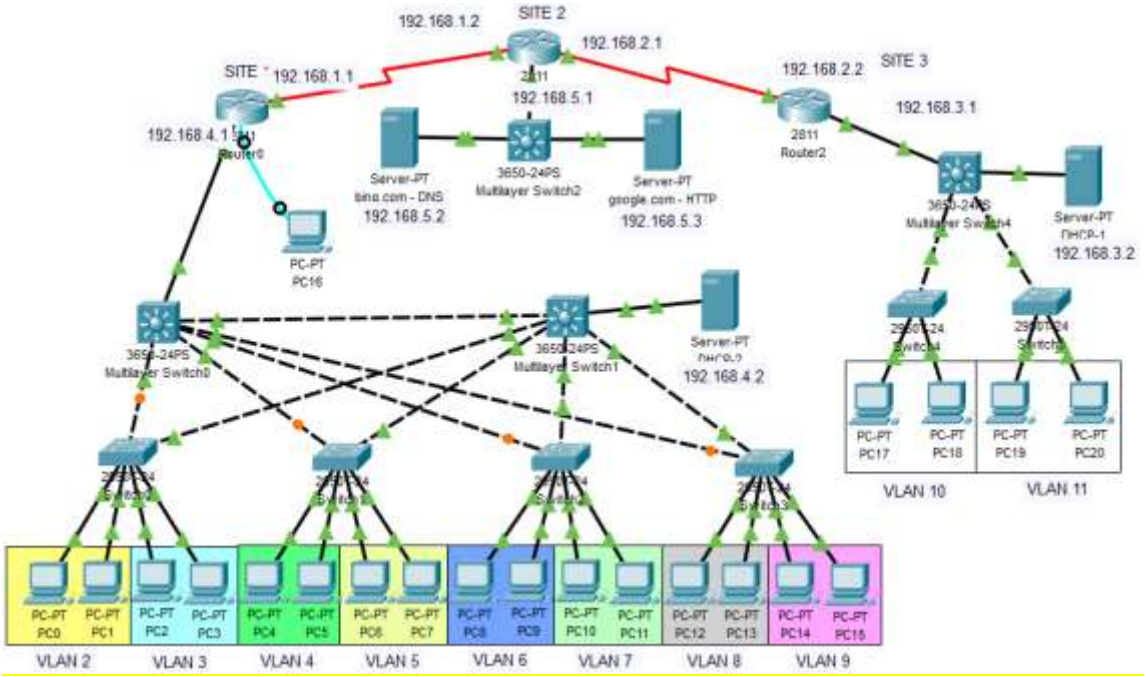
3.1 кесте - Cisco Packet Tracer негізінде виртуалды желілерді модельдеу және құру негізгізіндегі элементтері

Атауы	Түсіндірілуі	Бейнесі
Packet (десте)	Бұл TCP немесе IP желісі және ішкі желілер арқылы деректерді тарататын контейнер немесе қорап	
PC (дербес компьютер)	Бұл ақпаратты жинауға, өңдеуге, сақтауға және шығаруға арналған құрылғы.	
Queue (кезек)	Кезектің бұл түрі трафиктің басымдығы үшін қосымша параметрлерді орындауға мүмкіндік бермейді.	
Server (сервер)	Бұл бағдарлама кодтарын орындау, ақпаратты сақтау, пайдаланушылар мен мәліметтер базасына қызмет етудің белгілі бір міндеттерін шешуге арналған компьютер.	
Connection Type (қосылу түрі)	Желі құрылғысының қосылу күйін және байланыс түрін анықтауға мүмкіндік береді.	
Switch (коммутатор)	компьютерлік желінің бірнеше түйіндерін қосуға арналған құрылғы	
Multilayer switch	ол желілік құрылғы, OSI 2 деңгейінде кәдімгі желілік қосқыш сияқты ауысады және OSI жоғары деңгейлерінде қосымша функционалдылықты қамтамасыз етеді.	
Router (маршрутизатор)	әр түрлі желілік сегменттер арасында пакеттерді жіберетін мамандандырылған құрылғы	

3.5 Cisco Packet Tracer бағдарламасын қолданатын компаниялардың жергілікті желісін виртуалдандыру.

Cisco Packet Tracer-де виртуалды желіні модельдеу, әдетте, бағдарламалауға негізделмейді, бірақ Cisco IOS тілінде тікелей бағдарламалау мүмкіндігі бар. Бірақ та, құрылымдық модельге негізделген сандық мәліметтерге қосылған модельдеу желісін құру үшін модельденетін объект элементтерінің жұмыс істеуіне негізделген [21].

Жергілікті желі - бұл салыстырмалы түрде шағын аумақты немесе ғимараттардың шағын тобын қамтитын компьютерлік желі екені бәріне мәлім.Мұндай желілерді виртуалдандыру үшін маршрутизаторлар, 3-ші және 2-ші деңгейдегі қосқыштар, сонымен қатар веб және DHCP серверлер қолданылады.Компьютерлік модельдеу объектісі - «SunShine» компаниясы болып табылады (3.5-сурет).



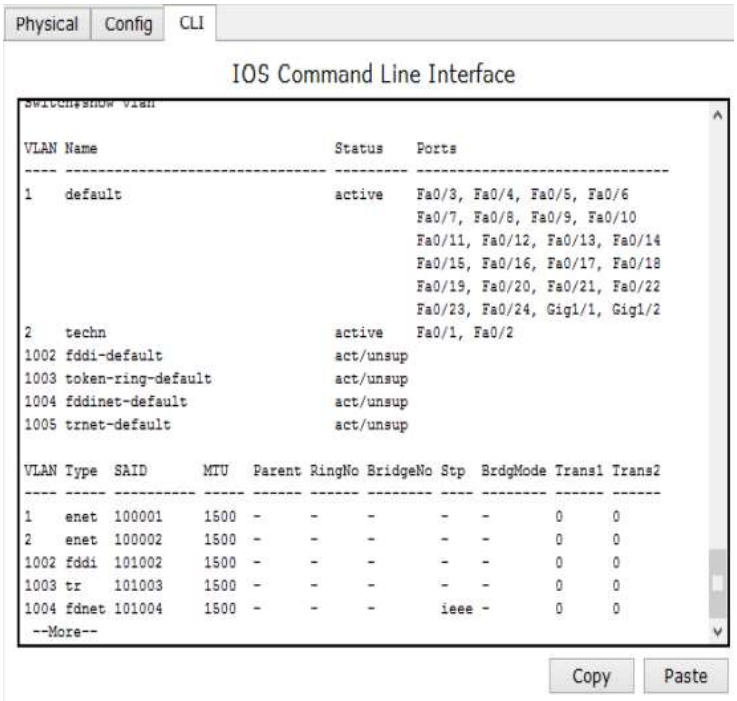
3.5 сурет - «SunShine» компания бөлімшесінің Cisco Packet Tracer-де салынған желі диаграммасы

Бұл жұмыстың басталуы жұмыс кеңістігіне енгізілген және әр бөлімге сәйкес VLAN-ға бөлінетін жұмыс станцияларына (PC-PT) қосылған Cisco 2960-24 қосқышын таңдау болды. Сонымен қатар, Layer 3 қосқыштарына және Cisco 2811 маршрутизаторларына қосылған. DHCP және HTTP серверлері веб-қызметтерді ұсыну және VLSM әдісіне сәйкес IP-адрестерді динамикалық бөлу үшін қолданылады.

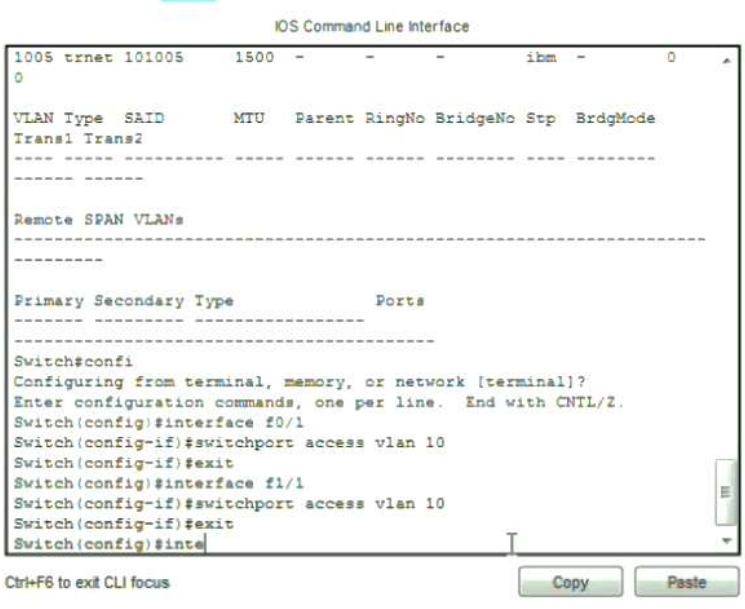
Әрі қарай, құрылғыларды тиісті интерфейсте пайдаланып қосамыз.

Келесі кезекте ең маңызды кезең – баптау. Әр түрлі сегменттердің трафигін бөлу үшін сізге коммутатордың параметрлерінде орналасқан

консольға (CLI) өтіп, осы пайдаланушылар орналасатын VLAN желісін анықтау қажет. Бастапқы диаграммада барлық ауыстырғыш порттары 3.6-суретте көрсетілгендей Vlan1-де орналасқан. Одан ары қарай VLAN2 - VLAN11 құрып, сәйкес желілердегі порттарды анықтауымыз керек (3.7-сурет).

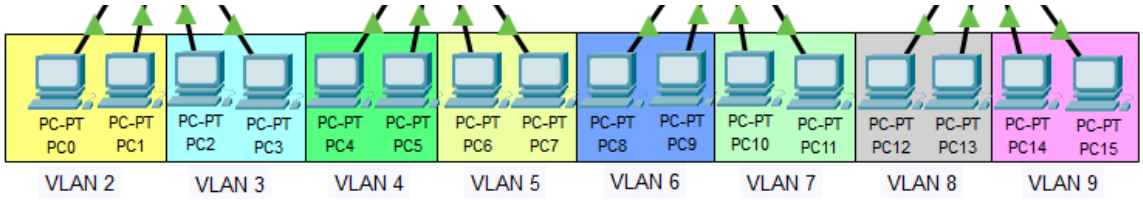


3.6 сурет - Әр түрлі сегменттерден тұратын трафикті бөлуге арналған коммутаторды конфигурациялау

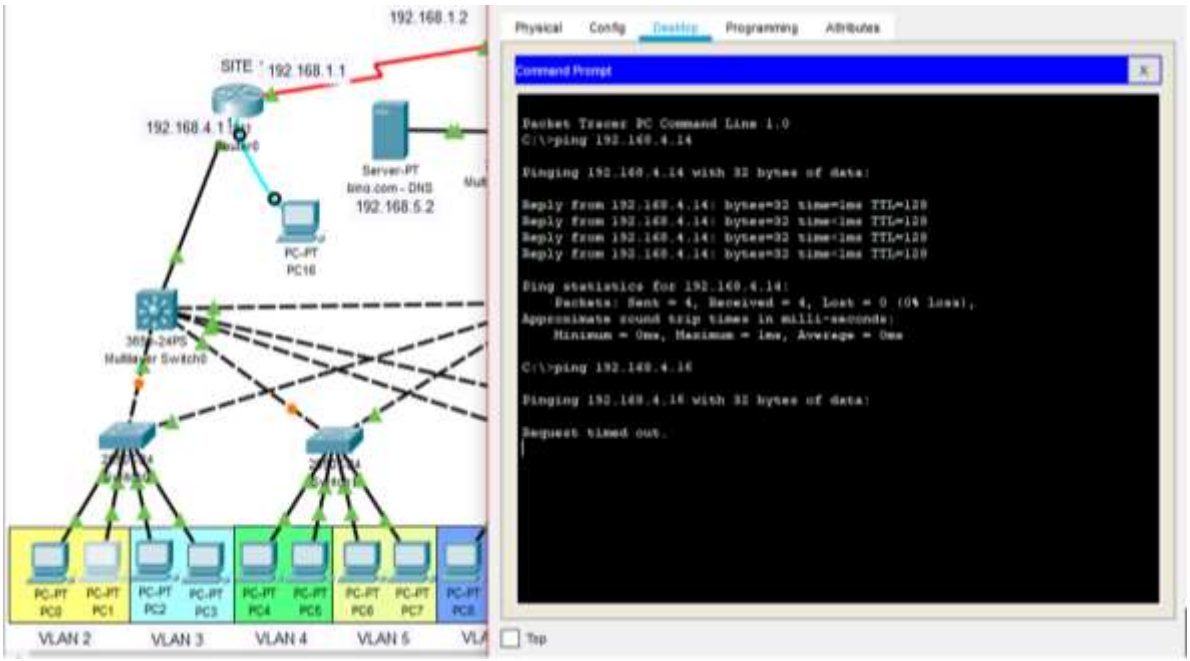


3.7 сурет - Пәрмен жолының интерфейсіндегі VLAN конфигурациясы

Осылайша, кәсіпорынның қарамағындағы жұмыс орындары әр түрлі жергілікті желілерге қисынды түрде таратылды. Жұмыс станцияларын жергілікті желілерге бөлу мұндай желіні болашақ басқаруды жеңілдетуге және оны логикалық түрде құрылымдауға мүмкіндік береді (3.8-сурет және 3.9-сурет).



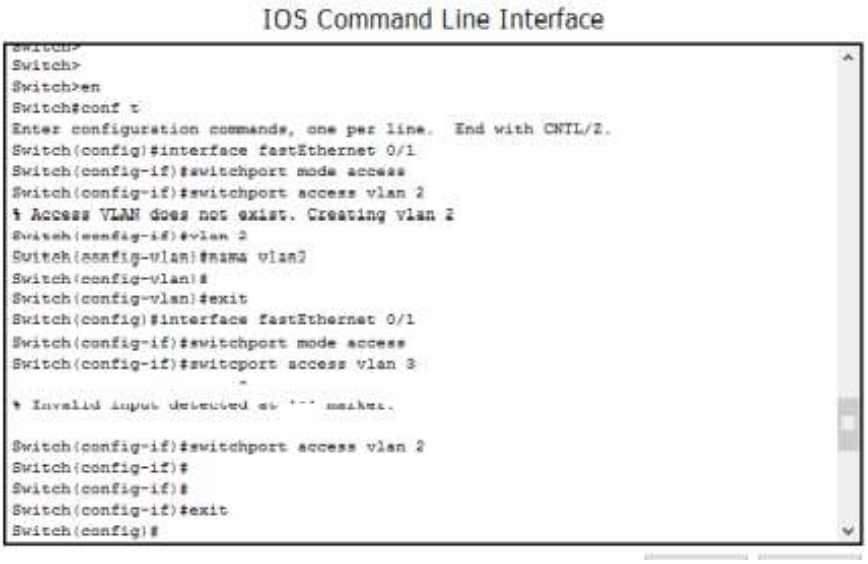
3.8 сурет - Коммутаторларды қолданып VLAN желілеріне сегменттеу



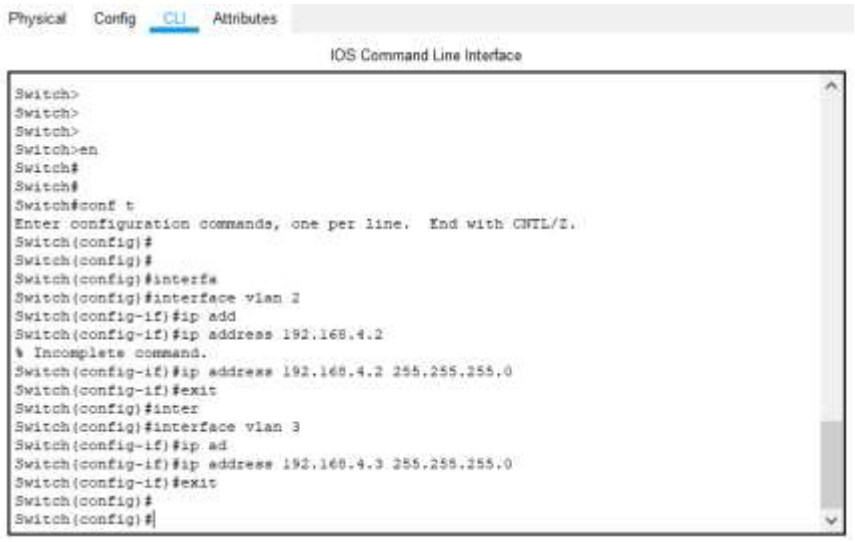
3.9 сурет - Бір коммутатормен жұмыс істегенде VLAN жұмысын тексеру

Әрі қарай қол жетімділік деңгейінің комммутаторлары бапталады. Мұны істеу үшін Switch 0 және Switch1 коммутаторлары үшін негізгі қосқышқа дейін access-порттар мен trunk порттарды конфигурациялаймыз (3.10-сурет және 3.11-сурет).

VLAN (ағылш. Virtual Local Area Network) - виртуалды жергілікті желі. Орналасқан доменмен байланысқан сияқты, олардың физикалық орналасуына қарамастан өзара әрекеттесетін [қайнар көзі анықталмаған 59 күн] бар хосттар тобын ұсынады.



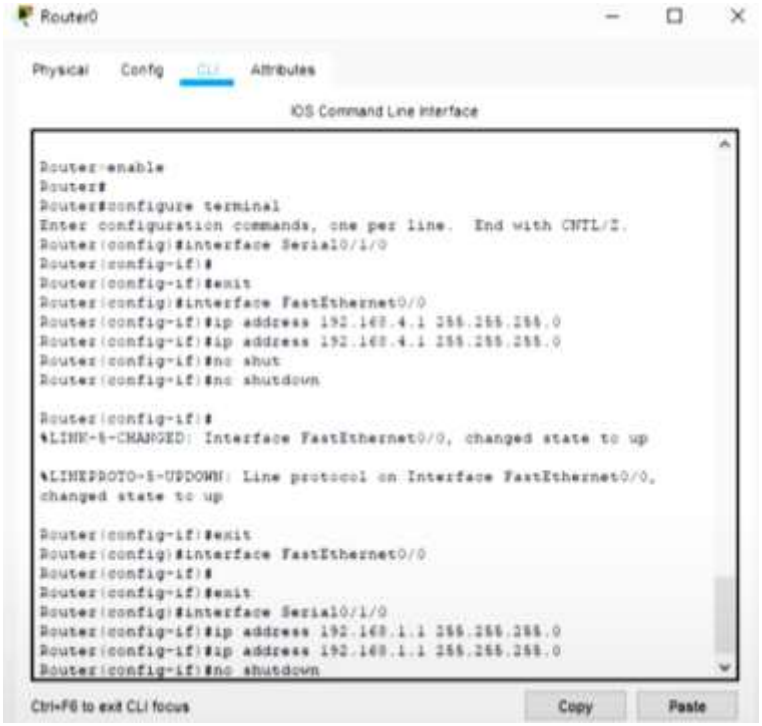
3.10 сурет - Vlan 2 және Vlan 3 баптау мысалы



3.11 сурет - Vlan-ға IP адресстер беру мысалы

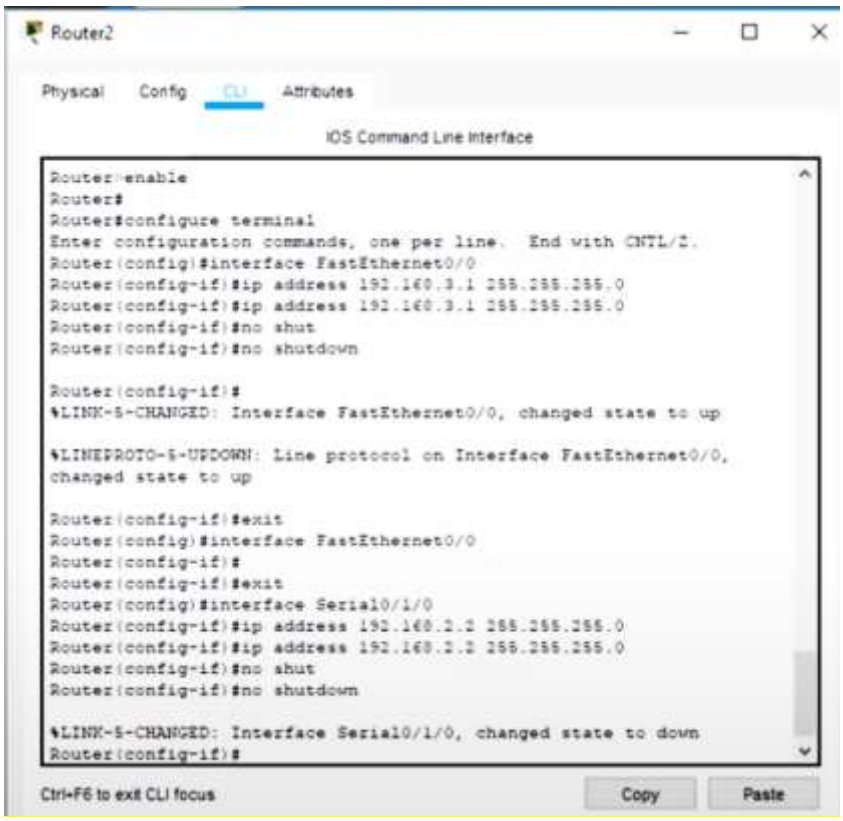
VLAN физикалық жергілікті желі сияқты қасиеттерге ие, бірақ соңғы мүшелер бір физикалық желіде болмаса да, оларды топтастыруға мүмкіндік береді. Бұл қайта құруды физикалық қозғалатын құрылғылардың орнына бағдарламалық жасақтамада жасауға болады.

Ары қарай брілген топология бойынша роутерлар бапталады, яғни (3.12, 3.13, 3.14 суреттерде) көрсетілгендей Router0, Router1 және Router2. Шығыстағы деректерге сәйкес “FastEthernet” және “Serial” интерфейстері әр қайсының IP адрестарымен беріледі.



3.12 сурет - Жоғарыда көрсетілген параметрлерді Router0 маршрутизаторында қолдану

3.13 сурет - Жоғарыда көрсетілген параметрлерді Router1 маршрутизаторында қолдану

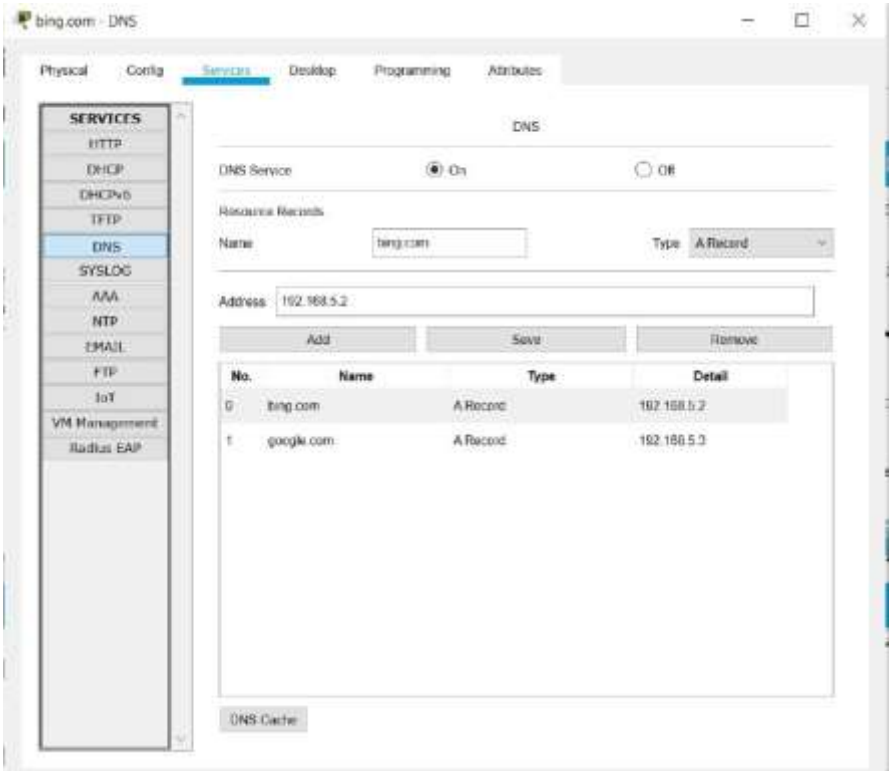


3.14 сурет - Жоғарыда көрсетілген параметрлерді Router2 маршрутизаторында қолдану

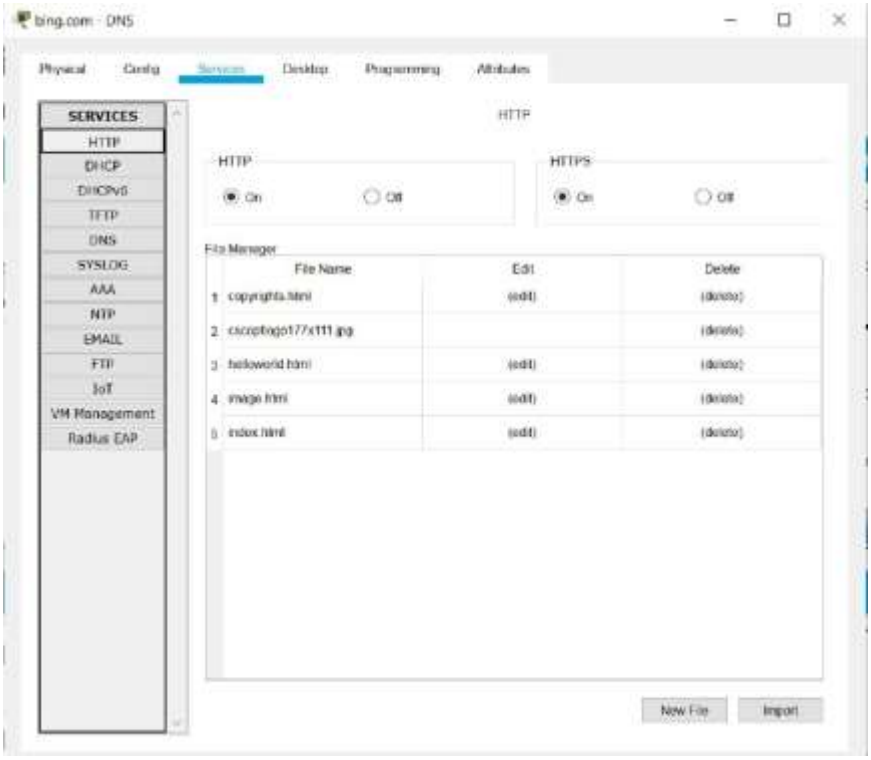
Компанияны web сервиспен қамтамасыз ету үшін DNS және HTTP серверларына баптаулар жүргіземіз. Осы тұста, DNS серверлік бағдарламасы домендер туралы ақпарат алуға арналған компьютерлік жүйе болып табылады. Ал HTTP сервері бұл URL мекенжайларын (веб-мекен-жайларды) түсінетін бағдарламалық жасақтама және клиенттерден, әдетте веб-шолғыштардан HTTP сұрауларын қабылдауға және өңдеуге арналған сервер (3.15, 3.16, 3.17 суреттерде).

HTTP-де манипуляцияның негізгі объектісі - бұл клиенттің сұранысында URI (Uniform Resource Identifier) көрсеткен ресурс. Әдетте, бұл ресурстар серверде сақталатын файлдар болып табылады, бірақ олар логикалық объектілер немесе дерексіз нәрсе болуы мүмкін. HTTP протоколының ерекше ерекшелігі - сұраныста және жауапта бір ресурстарды әртүрлі параметрлермен бейнелеу тәсілін: формат, кодтау, тіл және т.с.с. көрсету мүмкіндігі (атап айтқанда, бұл үшін HTTP тақырыбы қолданылады). Хабарламаның қалай кодталатындығын көрсете білудің арқасында клиент пен сервер екілік деректермен алмаса алады, дегенмен бұл хаттама мәтіндік болып табылады.

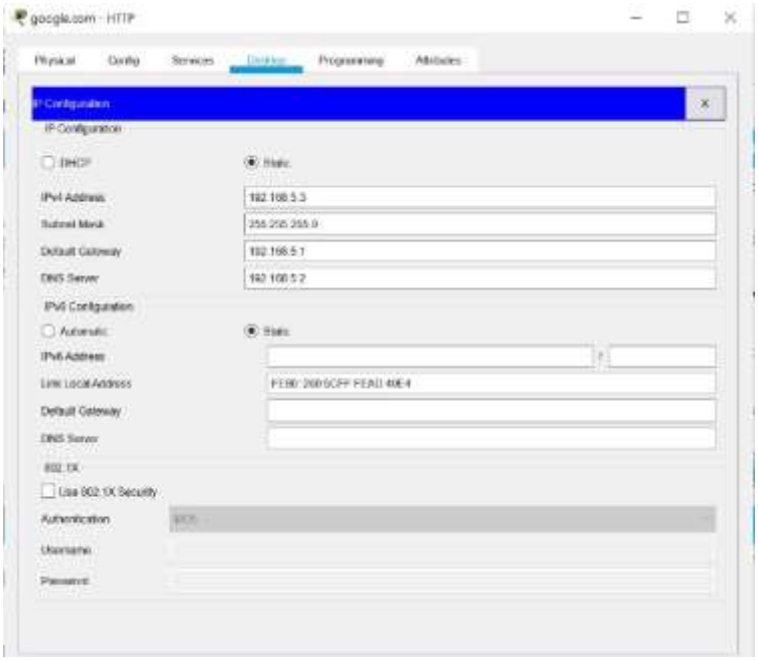
DNS-тің негізі - атау мен зоналардың иерархиялық құрылымын түсіну.



3.15 сурет - DNS қызмет көрсету жүйесін қамтамасыз ету

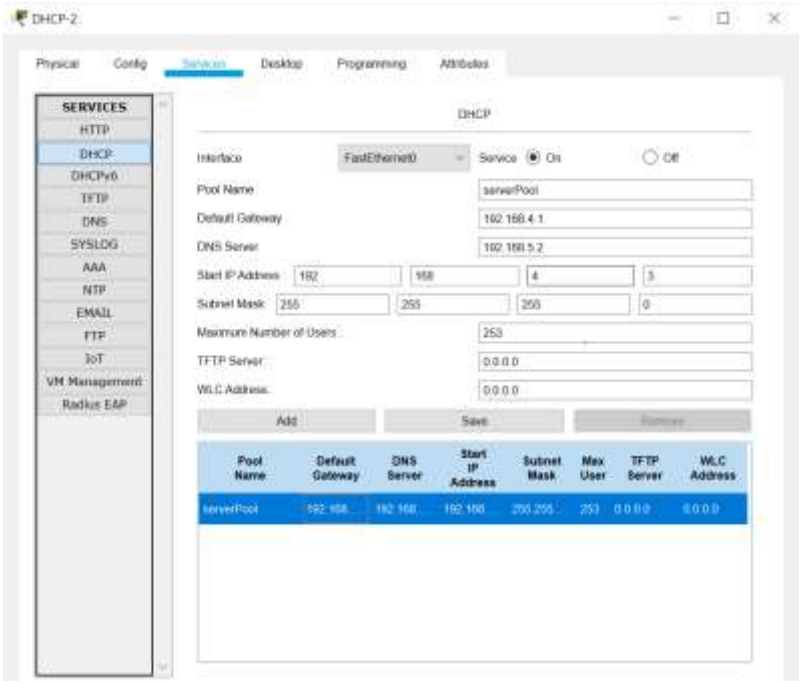


3.16 сурет - HTTP қызметтік жүйесінің DNS серверінде қолданылуы



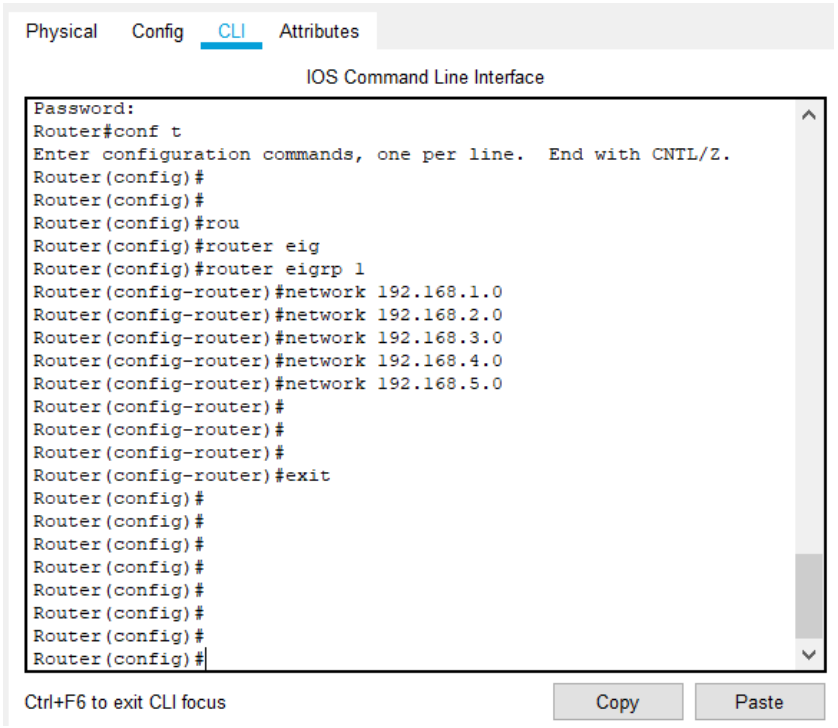
3.17 сурет - HTTP серверіне сәйкес DNS және әдепкі шлюздің IP адрестерін беру

Одан кейін DHCP 1 және DHCP 2 серверларына автоматты түрде компьютерларға IP адрестерді бөлу үшін томендегі баптаулар жүзеге асырылды(3.18 - сурет).



3.18 сурет - DHCP 2 серверінің бапталу мысалы

Бұл модельде үш маршрутизатор (SITE1, SITE 2 және SITE 3) болғандықтан, желіде ағып жатқан трафикті бағыттау қажет болады. Ол үшін жұмыс алмасуды қолдайтын және көршілес маршрутизаторларға желілер туралы ақпарат тарататтын EIGRP динамикалық маршруттау хаттамасы қолданылды. SITE 1 маршрутизаторындағы хаттаманың конфигурациясы 3.19 суретте көрсетілген.

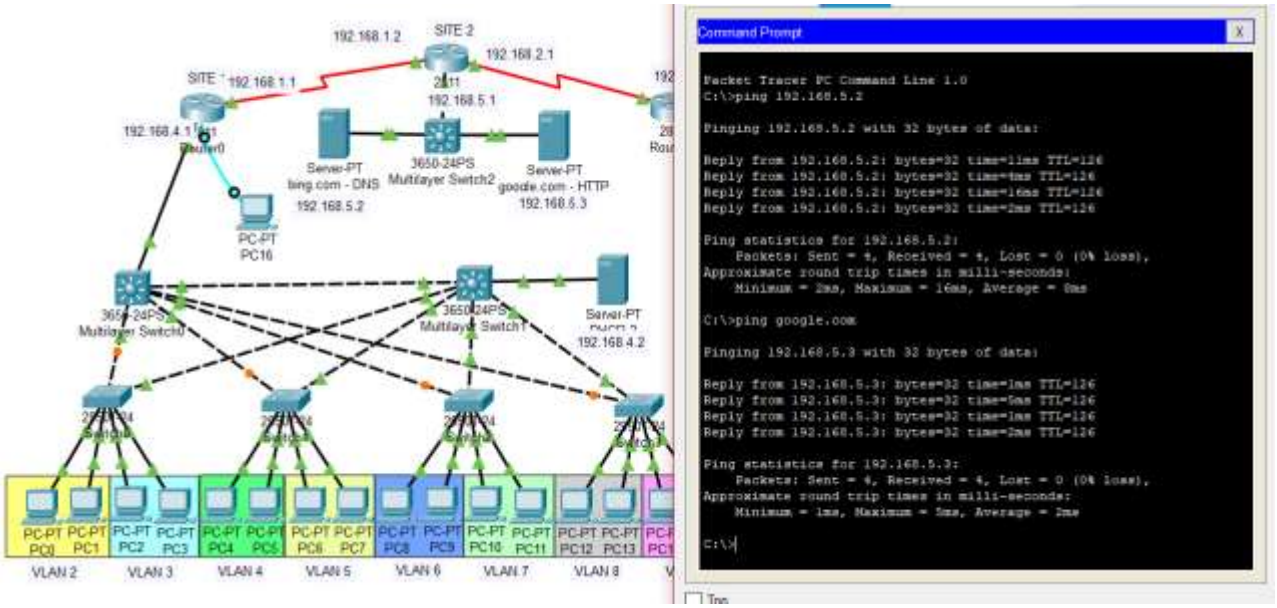


3.19 сурет - Маршрутизатордағы EIGRP динамикалық маршруттау протоколының параметрлері

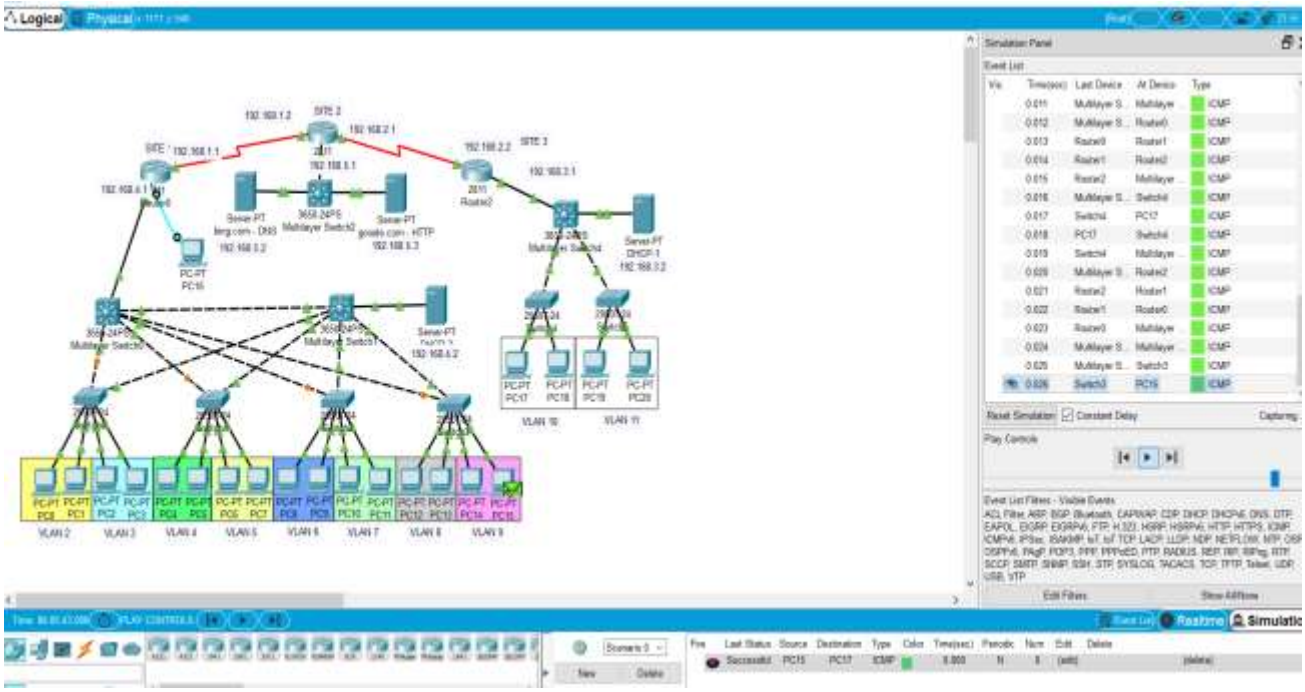
3.6 Компьютерлердің арасындағы байланыс мүмкіндігі туралы зерттеулер жүргізу

Барлық параметрлерді аяқтағаннан кейін тестілеу процесі өткізілді. Бір жергілікті желінің компьютерлері мен әртүрлі жергілікті желілерде орналасқан компьютерлер арасындағы «ping» желілік өзара әрекеттесу мүмкіндігі желілік қосылыстың тұтастығы мен сапасын тексеруге арналған желілік қызметтің сәтті орындалуымен анықталды.

Біріншіден, біз компьютердің веб-қызметке кіруін тексереміз, ол үшін PC3 және PT сервер арасында ping командасын орындаймыз. 3.20, 3.21-суреттерде көрсетілгендей Ping сынағы сәтті өтті.

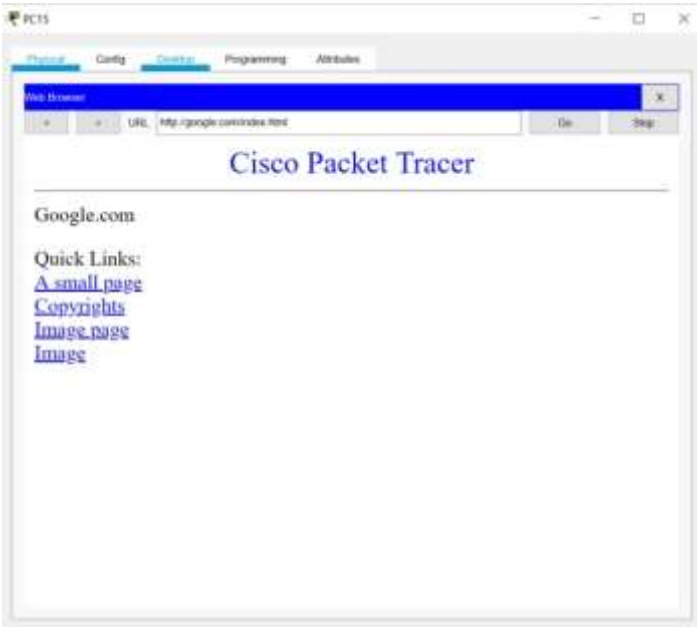


3.20 сурет - Компьютер мен сервер арасындағы сәтті желілік байланыстың нәтижесі



3.21 сурет - Әр түрлі жергілікті желілерде орналасқан компьютерлердің сәтті желілік өзара әрекеттесуінің нәтижесі

Төменде, 3.22-суретте компьютер арқылы веб-шолғышқа сәтті қосылудың нәтижесі көрсетілген.



3.22 сурет - Компьютер арқылы веб-шолғышқа сәтті қосылудың нәтижесі

3.7 VLSM және FLSM әдістері арқылы ішкі желілерді талдау

VLSM-ді жылдам және тиімді құру үшін және VLSM маскаларын жасау үшін блок өлшемдері мен диаграммалары қалай жұмыс істейтінін түсіну қажет. 3.2-кестеде С санаты бар желілермен VLSM құру кезінде қолданылатын блок өлшемдері көрсетілген.

3.2 кесте - Блок өлшемдері

Префикс	Маска	Хост	Блок өлшемі
/25	128	126	128
/26	192	62	64
/27	224	30	32
/28	240	14	16
/29	248	6	8
/30	252	2	4

Мысалы, егер 25 хосттың ішкі желісі қажет болса, онда ол 32 блок өлшеміне жатады. Сондай-ақ, егер 11 хосттың ішкі желісі қажет болса, онда ол 16 блок өлшеміне жатады. Сонымен қатар, егер 40 хосттың ішкі желісі қажет болса, онда ол 64 блок өлшеміне жатады.

VLSM желісін құрудың келесі қадамы VLSM жұмыс парағын немесе диаграммасын пайдалану болып табылады. Бұл кесте мен диаграмманы қолдану себебім желілердің қабаттасуын болдырмау болып табылады.

Біздің жағдайда, «SunShine» компанияның IP мекен-жайы 192.168.1.0 құрайды және бұл компания 3.5-суретте көрсетілгендей төрт ішкі желі және

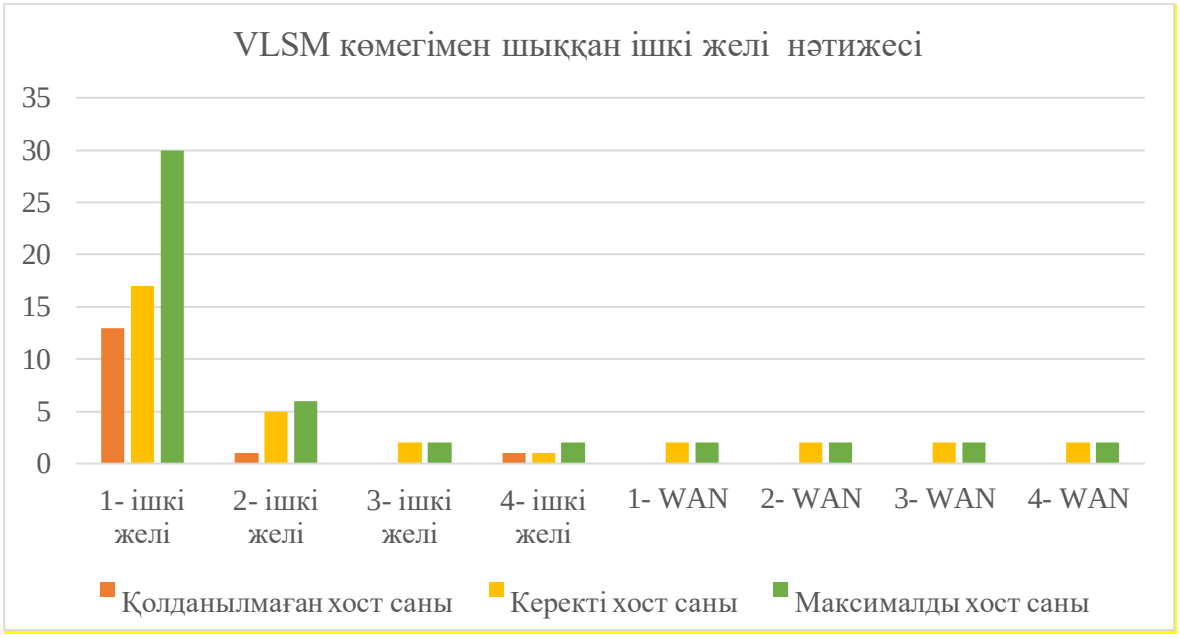
төрт WAN (17, 5, 2, 1, және 2-ден хост / ішкі желі) құралады. Келесі 3.3-кестеден VLSM-нің ішкі желілерге бөлінуін көре аласыздар.

3.3 кесте - VLSM көмегімен ішкі желілерді есептеу

Ішкі желі	Қолданылмаған хост саны	Керекті хост саны	Максималды хост саны
1-желі	13	17	30
2-желі	1	5	6
3-желі	0	2	2
4-желі	1	1	2
1- WAN	0	2	2
2- WAN	0	2	2
3- WAN	0	2	2
4- WAN	0	2	2

VLSM диаграммасы көмегімен ішкі желілерді елестету. VLSM диаграммасы - бұл ішкі желілер мен адрестердің кішірек өлшемдерге бөлінуін бейнелеу үшін қолданылатын әдіс. Жәшіктерге көлеңке қою немесе бояу арқылы адрестердің қабаттасуынсыз ішкі желілерді оңай бұзуға болады. Әрбір ішкі желідегі ішкі желіні қажетті мөлшерде реттеуге болады [22].

Содан кейін VLSM диаграммасын қолдану арқылы қажетті аймақты көлеңкелендіру арқылы әр ішкі желінің қажетті блок өлшемін дұрыс өлшемге бөлуге болады. Аймақтың көлеңкеленуі оны басқа ішкі желі орналастыруынан сақтайды (3.23-сурет).

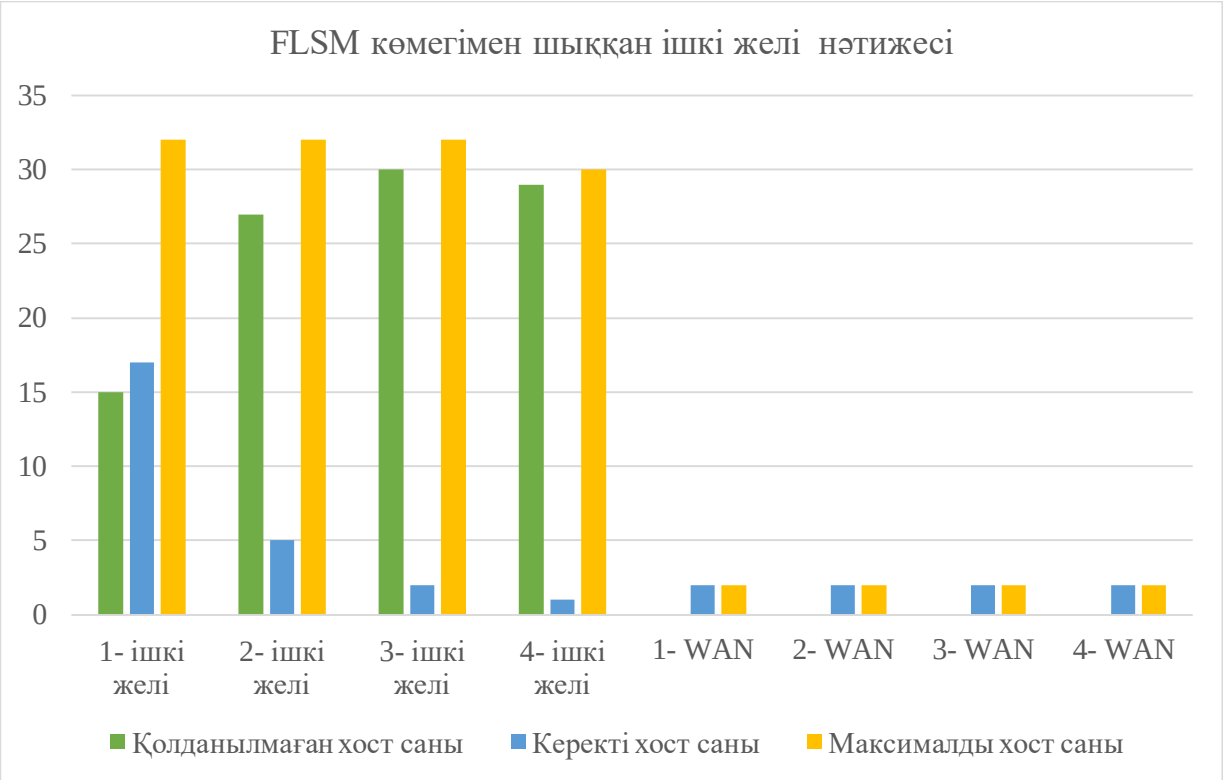


3.23 сурет - VLSM көмегімен шыққан ішкі желінің анализдік диаграммасы

Келесі 3.4-кесте мен 3.24-суретте FLSM ішкі желілерді бөлу нәтижесін байқауға болады.

3.4 кесте - FLSM көмегімен ішкі желіні есептеу

Ішкі желі	Қолданылмаған хост саны	Керекті хост саны	Максималды хост саны
1-желі	15	17	32
2-желі	27	5	32
3-желі	30	2	32
4-желі	29	1	30
1- WAN	0	2	2
2- WAN	0	2	2
3- WAN	0	2	2
4- WAN	0	2	2



3.24 сурет - FLSM көмегімен шыққан ішкі желінің анализдік диаграммасы

Осы зерттеу жағдайындағы қолданбалы мысалда талдау нәтижелері көрсеткендей, VLSM-ді презентация әдісімен қолдану FLSM ішкі желісіне қарағанда 52.8% тиімді екенін көреміз. Барлық ішкі желілерді таратқаннан кейін, желі 3.5–суретте көрсетілгендей болады.

3.8 Модельденген виртуалды желіні талдау негізінде өнімділігін бағалау

Желіні құру кезеңі аяқталды, енді модельденген виртуалды желінің жұмысын талдау негізінде оның сипаттамаларын бағалау қажет.

Бұл тренажердың маңызды ерекшеліктерінің бірі - (3.25 суреттегі) «модельдеу режимі». Бұл режимде желі ішінде жіберілген барлық пакеттер графикалық түрде көрсетіледі. Желі параметрлерін бағалау үшін желінің жүктемесіз жұмысы модельденді. 15000 байт пакеті PC15-тен PC17-ге FTP арқылы жіберілді. Десте жеңіл жүктеме желісіндегі 2-деңгейлі 3-коммутатор арқылы бағытталады. 3.25-суретте көріп отырғаныңыздай, деректерді тасымалдауға 0,109 секунд уақыт кеткен және 3.8-формуладан жылдамдықты табуға болады.

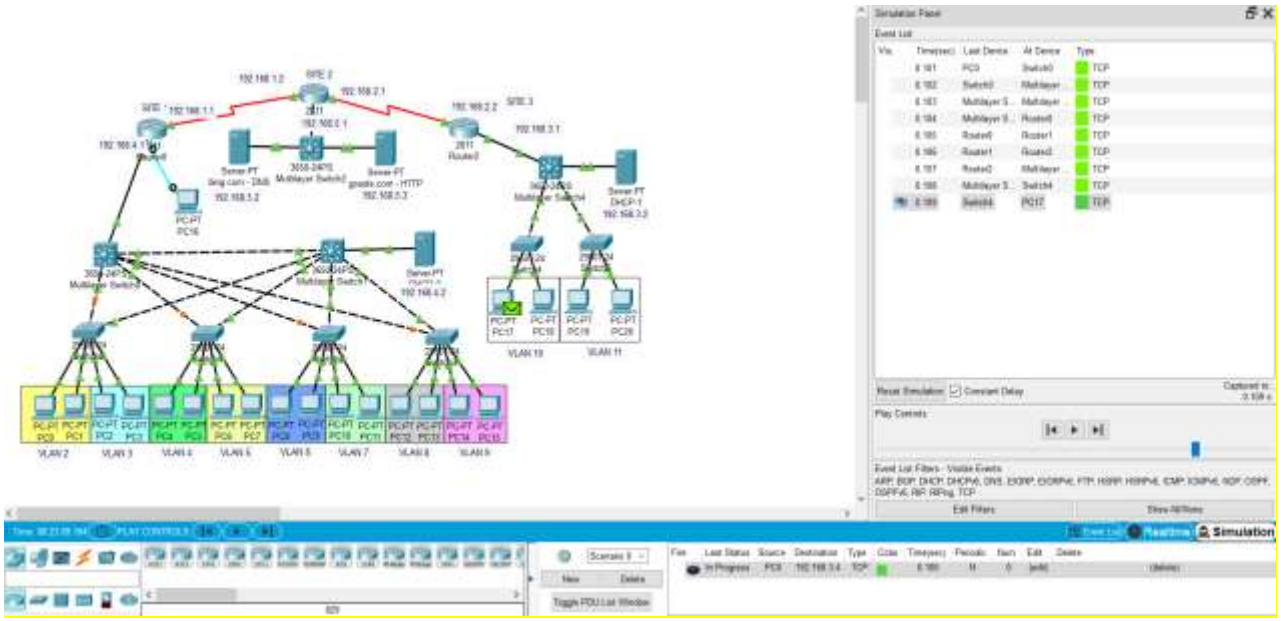
$$q = \frac{V}{t}, \tag{3.8}$$

мұндағы q - желінің өткізу қабілеті (бит / сек);

V – хабарламалардың өлшемі, бит;

t – деректерді жіберу уақыты.

Осылайша, жоғарыдағы мысалда жүктелмеген желідегі деректерді беру жылдамдығы 137,6 Мбит / с құрайды.



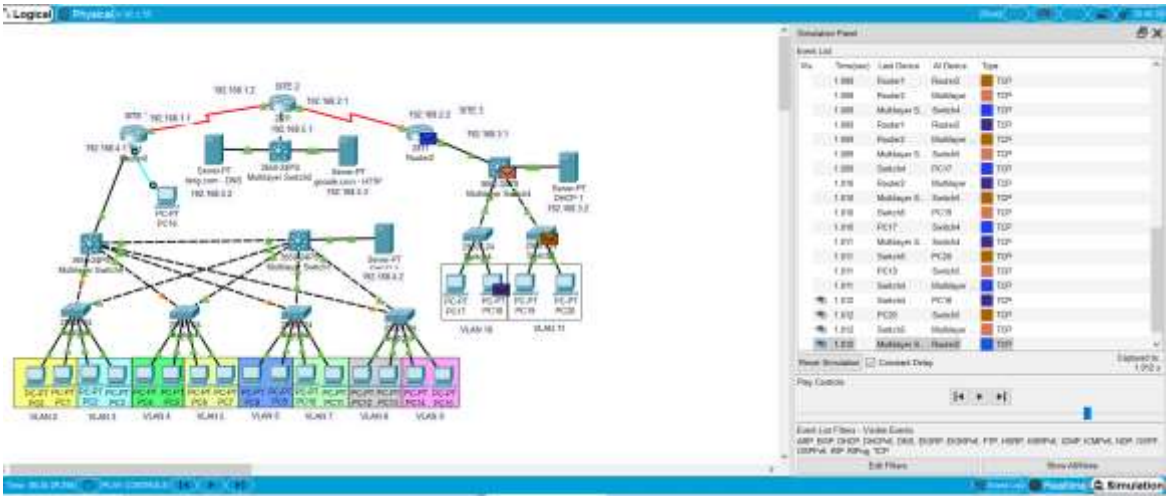
3.25 сурет - Cisco Packet Tracer бағдарламасындағы жіберу дестесіндегі «Simulation» режимі

Кез-келген желіні құрудың басты міндеті - компьютерлер арасында жылдам ақпарат беру. Сондықтан желінің немесе желінің бір бөлігінің

өткізгіштігіне қатысты критерийлер оның негізгі функциясын орындайтын желінің сапасын жақсы көрсетеді.

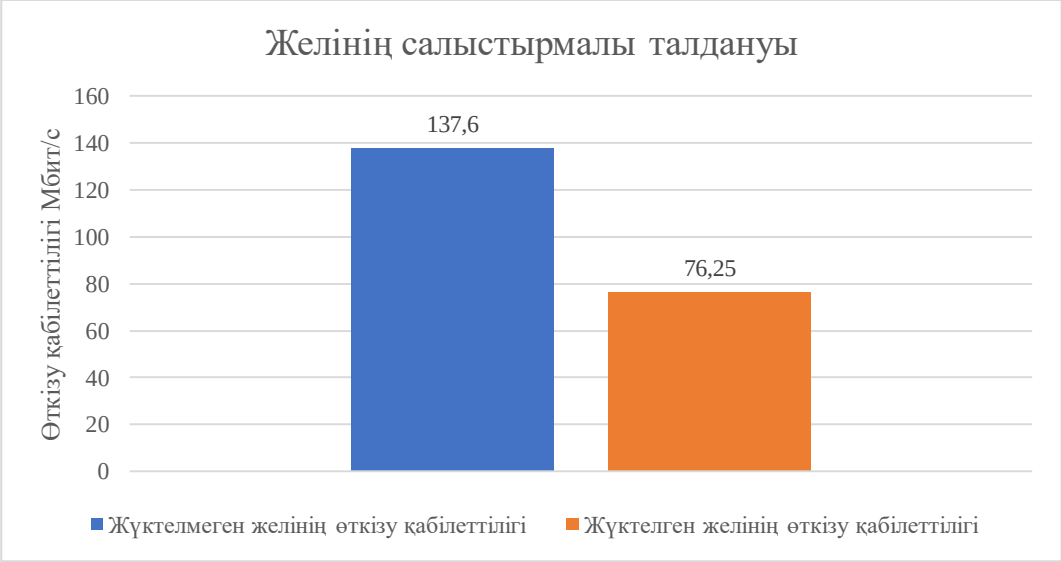
Өткізгіштік уақыт бірлігінде байланыс желісі бойынша берілетін деректердің максималды мүмкін мөлшерін сипаттайды. Әдетте пакеттер немесе биттер берілген ақпараттың өлшем бірлігі ретінде қолданылады.

Әрі қарай біз жүктелген ажыратқыштары бар желінің жұмысын қарастырамыз. Коммутаторға жүктеме ретінде түйіндер арасында деректер беру қосылады: PC0-PC17, PC2-PC18, PC4-PC19, PC8-PC20 (3.26-сурет).



3.26 сурет - Жүктеме кезінде желінің жұмысын модельдеу

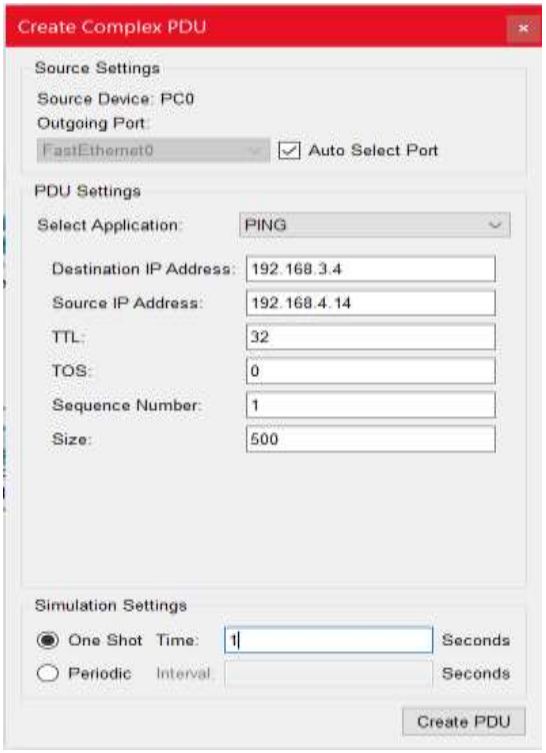
Соңғы пакетті жіберуге 0,012 секунд қажет болды (3.27-сурет). Осылайша, желінің өткізу қабілеті 76,025 Мбит / с құрайды.



3.27 сурет - Желінің салыстырмалы талдану диаграммасы

Осылайша, желі жүктелгенде уақыт бойынша да және жылдамдығы бойынша азаятынын көреміз, нақты біздің жағдайымызда 55.4%-ке төмендегенін байқаймыз. Әдетте, жүктелген желідегі өткізу қабілеттілігін жоғрылату үшін агрегатты каналды қолдану арқылы порттардың санын көбейту тәсілі қолданылады.

Екінші экспериментті қайталайық, бірақ желідегі жүктемедегі трафик генераторы утилитасын қолдана отырып жүргіземіз (3.28-сурет). Бұл жағдайда 100 эхо-сұранысының санын көрсетеміз [23].



3.28 сурет - Traffic Generator утилитасы

Трафик генераторы - кез-келген желілік әкімшінің арсеналындағы ең маңызды утилиталардың бірі және ол RouterOS-та орнатылған. Бұл құрал өнімді аппаратураны қажет етпестен өнімділігін тексеруге мүмкіндік береді. Трафикті желідегі басқа маршрутизатор жасайды. Сіз RAW пакеттерін арнайы порттарда жасайсыз және жібересіз, бағдарлама кешігу мен дірілдеуді, tx / rx жылдамдығын жинайды, жоғалған пакеттерді санап, «Ретсіз» (RX-OOO) пакеттерін анықтайды. Трафик генераторын өткізу қабілетін тексеру құралы сияқты пайдалануға болады. Сондай-ақ, ол пакетті генераторға жіберіп, кеңейтілген желілік талдау үшін жіберіледі.

Бағдарлама әрдайым жаңартылып отырады, әр түрлі қосымшалар үшін функционалдығын кеңейтеді.

Соңғы мүмкіндіктердің бірі - RFC2544-те анықталғандай, пакеттердің жоғалуын жасалған пакеттердің жалпы санынан пайызбен көру мүмкіндігі.

Трафик генераторының мөлшерін cisco packet tracer пакеттің өлшеміне 500 байт орнатылды. Әрі қарай, біз пакеттің максималды өлшемі 15000 байтқа жеткенше, 500 байт қадамымен пакеттің көлемін арттырамыз. Тәжірибе нәтижелері 3.29-суретте келтірілген.

3.29 сурет - Жоғалған пакеттер санының каналдағы жүктемеге тәуелділігі

Тәжірибенің алынған нәтижелері осы жүктеме жағдайындағы арнаның жұмыс күйінен шығады, құрылғылар арасындағы пинг пакеттің жоғалуымен жүреді деп айтуға мүмкіндік береді. Арнаға максималды жүктеме кезінде шығындар жіберілген эхо-сұраныстардың жалпы санының 25% құрады. Шамадан тыс жүктеме мәселесін шешудің тәсілдерінің бірі - модельдеуге жұмысқа арналған бағдарламаланған желіні басқару технологиясын қолдану [24].

Қорытынды

Диссертациялық жұмысты орындау кезінде Cisco Packet Tracer желілік жабдықтарын виртуалдандырудың заманауи онлайн платформасы мен күрделі компьютерлік желілердің модельдерін жасау мақсаты қойылды және жасалды. Желілік жабдықты виртуалдандырудың қолданыстағы жүйелері талданды, күрделі компьютерлік желілердің тұжырымдамалары жобаланып, олардың модельдерін жасалды. Жасалған модельдер негізінде олардың тиімділігі туралы зерттеулер жүргізілді.

Қолданыстағы желілік жабдықты эмуляциялау жүйелеріне талдау жүргізіліп, осы платформалар ең жақсысын анықтау үшін бір-бірімен салыстырылды. Жүйелерді талдау негізінде бұл платформа Cisco Packet Tracer болып табылады.

Таңдалған платформа негізінде кәсіпорынның дамуын көрсететін компьютерлік желілердің модельдері жасалды. Дамудың әр кезеңінде компьютерлік желілердің модельдерін қолдана отырып шешілетін белгілі бір міндеттер қойылды және сол міндеттерді қою арқылы белгіленген мақсатқа жеткізілді. Модельденген виртуалды желінің жұмысын талдау негізінде оның сипаттамалары мен өтімділігі бағаланды.

Осы зерттеу жағдайындағы қолданбалы мысалда талдау нәтижелері көрсеткендей, VLSM ішкі желі әдісімен қолдану FLSM ішкі желісіне қарағанда 52.8% тиімді екені көрсетілді. Сонымен қатар, желі жүктелгенде уақыт бойынша да және жылдамдығы бойынша азаятынын көреміз, нақты біздің жағдайымызда 55.4%-ке төмендегенін көрсетілді. Модельденген виртуалды желінің жұмысын талдау негізінде оның сипаттамалары мен өтімділігі бағаланды.

Қысқартулар тізбесі

VLSM - Variable Length Subnet Mask;
FLSM - Fixed Length Subnet Mask;
VLAN - Virtual Local Area Network;
RIP - Routing Information Protocol;
DHCP - Dynamic Host Configuration Protocol;
EIGRP - Enhanced Interior Gateway Routing Protocol;
BGP - Border Gateway Protocol;
OSI model - Open Systems Interconnection model;
TCP/IP - Transmission Control Protocol/Internet Protocol;
GNS3 - Graphical Network Simulator 3;
VPN/GRE/IPsec - Virtual Private Network/ Generic Routing Encapsulation/ Internet Protocol Security;
STP - Spanning Tree Protocol;
LAN - Local Area Network;
WAN - Wide Area Network;
DNS - Domain name server;
HTTP - HyperText Transfer Protocol.

Әдебиеттер тізімі

1 Mark A.D., Rick M.D. and Antoon W. R.: CCNA Exploration Curriculum-Network Fundamentals, Version 4. – Indy.: Cisco Press, 2010. – 312 p.

2 Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифе – Учебник. – СПб: Изд-во «Питер», 2016. – 992 с.

3 Локальные сети: архитектура, алгоритмы, проектирование. / Ю.В. Новиков, С.В. Кондратенко – М.: ЭКОМ, 2001. – 312 с.

4 Вычислительные сети и сетевые протоколы / Д. Девис, Д. Барбер, У. Прайс – М.: Мир, 1982. – 562с.

5 Компьютерные сети. Книга 1: High-Performance Networking. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 432 с.

6 Корпоративные сети связи / Т.И. Иванова. Пособие. – Москва 2001, – 297с.

7 Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е издание. / А. Мысник – М.: Издательский дом «Вильямс», 2005. – 1168 с.

8 Использование программных средств эмуляции оборудования при модификации сетевой инфраструктуры / Е.Ф. Попов// Сборник научных трудов по материалам всероссийскую научно-практической конференции студентов, аспирантов и молодых ученых «Новые технологии –нефтегазовому региону». Тюмень, 2012.

9 CCNP маршрутизация / Т.Лэммсл, Ш.Одом, К. Уоллес. Изд. «Лори», 2015. – 444 с.

10 Компьютерные сети / Э. Таненбаум – СПБ.: «Питер», 2002. – 248 с.

11 Основы построения виртуальных частных сетей. / С.В. Запечников. – М.: Мир, 2003. – 249 с.

12 Информационная безопасность компьютерных систем и сетей. / В.Шаньгин. – Изд.: Инфра-М, 2011. – 416 с.

13 Использование программных средств эмуляции оборудования в обучении сетевым технологиям / Е.Ф. Попов, А.А. Захаров // Сборник научных трудов по материалам Международной заочной научно-практической конференции «Теоретические и прикладные проблемы науки и образования в 21 веке». Часть 8. – Тамбов, Изд-во ТРОО «Бизнес-Наука и Общество», 2012.

14 Тестирование и применение эмуляторов Cisco для моделирования гетерогенной IPсети / А.М. Горячев // Гагаринские чтения – 2016: XLII Международная молодежная научная коференция: Сборник тезисов докладов Т.ё. Московский авиационный институт (национальный исследовательский университет). – 2016. – стр.277-278.

15 Introduction to Cisco IOS Netflow:A Technical Overview / URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/iosnetflow/prod_white_paper0900aecd80406232.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

16 CiscoIOSFlexibleNetFlow [Электронныйресурс] / URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15mt/fnf-15-mt-book/fnf-fnetflow.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

17 An empirical distribution function for sampling with incomplete information. / M. Ayer, H. Brunk, G. Ewing, W. Reid, and E. Silverman // Annals of Mathematical Statistics – 1995 – 5(26) – 641–647.

18 John Albritton: Cisco IOS Essentials, First edition. – Texas: McGraw-Hill Press, 1999. – 263 p.

19 Todd Lammle: Cisco Certified Network Associate-Study Guide, Seventh Edition. – Twin: Sybex Press, 2013. – 289 p.

20 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб: Питер, 2010. – 944с.

21 Таненбаум Э, Уэзеролл Д. Компьютерные сети. – Спб: Питер, 2012. – 960 с.

22 Todd Lammle, Sean Odom and Kevin Wallace: CCNP Routing Study Guide. – London: Sybex Press, 2001. – 548 p.

23 N.Nazumudeen, C.Mahendran, Performance Analysis of Dynamic Routing Protocols Using Packet Tracer, ISSN: 2319 –8753, (ICETS'14).

24 Mirza Waseem Hussain, Sanjay JamwalComparative Analysis of Various Routing Protocols, IJMER | ISSN: 2249–6645, Vol.6 Iss. 3 | March 2016 | 67.