ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Ш.Ә. Джомартова

А.С.Тергеусизова

**ЖЕЛІЛІК ТЕХНОЛОГИЯЛАР**

***Оқу құралы***

Алматы

«Қазақ университеті»

2020

ӘОЖ

КБЖ

Д

*Баспаға әл-Фараби атындағы Қазақ үлттық университеті*

*ақпараттық технологиялар факультетінің*

*Ғылыми кеңесі және Редакциялық-баспа кеңесі*

*шешімімен үсынылған*

*(№ хаттама 2020 жыл)*

**Пікір жазған**

физика-математикаылымдарының каднидаты, доцент ***К.С.Дуйсебекова***

**Джомартова Ш.А.**

Д Желілік технологиялар: оқу күралы / Ш.А.Джомартова, А.С. Тергеусизова. – Алматы: Қазақ университеті, 2020. - б.

**ISBN**

Автордың редакциясымен шығарылды

**ӘОЖ**

**КБЖ**

**1 БӨЛІМ**

# Желілерінің негіздері

## 1.1 Желіні пайдалану

1.1.1 OSI желісінің моделі

##### 

Желінің жұмысы деректерді бір компьютерден екінші компьютерге беру болып табылады. Бұл процесте бірнеше жеке тапсырмаларды бөлуге болады:

- деректерді тану;

- мәліметтерді басқарылатын блоктарға бөлу;

- мәліметтердің орналасқан жерін көрсетіп, алушыны көрсететін әр блокқа ақпарат қосыңыз;

- синхрондау және қателерді тексеру ақпаратын қосу;

##### - мәліметтерді желіге қойып, көрсетілген мекен-жайға жіберіңіз.

##### Барлық осы тапсырмаларды орындай отырып, желілік операциялық жүйе қатаң рәсімдер жиынтығын ұстанады.



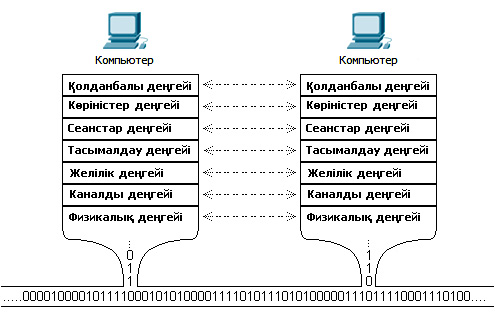
**Хаттама – әр желінің жұмысын реттейтін рәсімдер (тәртіп ережелері).**

Стандартты хаттамалар әртүрлі өндірушілердің бағдарламалық және аппараттық құралдарымен қалыпты байланыс орнатуға мүмкіндік береді. Стандарттардың екі негізгі жиынтығы бар: OSI моделі және оны өзгерту Project 802. Желінің жұмыс істеуінің техникалық жағын зерттеу үшін осы модельдер туралы нақты түсінікке ие болуыңыз керек.



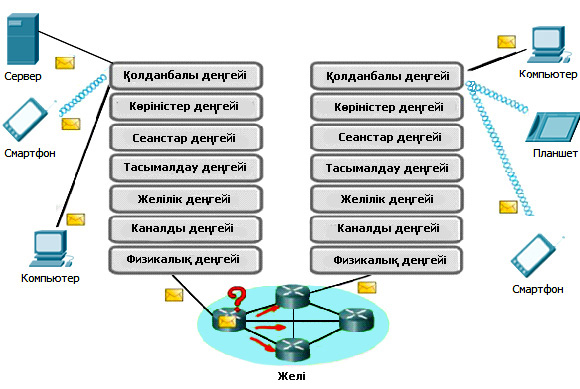
1984 жылы ХСҰ (ISO (International Standards Organization) (Халықаралық стандарттар ұйымы) ашық жүйелердің өзара әрекеттесуіне арналған OSI (Open System Interconnection) анықтамалық моделін шығарды. Ол халықаралық стандартқа айналды: желілік өнімдерді шығаруда өндірушілер нақты ерекшеліктерді және желілерді құру кезінде пайдаланады. OSI моделі жүйелер арасындағы өзара әрекеттесудің әртүрлі деңгейлерін анықтайды, оларға стандартты атаулар береді және әр деңгей қандай функцияларды орындау керек екенін көрсетеді. OSI моделінде өзара әрекет ету құралдары жеті қосымшалар, көріністер, сеанстар, тасымалдау, желілік, каналды (арналы) және физикалық деңгейлерге бөлінеді (1.1 сурет).

Әрбір деңгей желілік құрылғылардың белгілі бір ерекшелігімен өзара әрекет етеді. OSI моделі операциялық жүйе, жүйелік аппаратура іске асыратын жүйелік әрекеттесу құралдарын ғана сипаттайды. Модель соңғы қолданушыға арналған өзара әрекеттесу құралдары кірмейді. Бағдарламалар жүйелік құралдарға қол жеткізу арқылы өзара әрекеттесу хаттамаларын орындайды. Сондықтан қосымшалардың өзара әрекеттесу деңгейі мен қосымшалардың деңгейлерін ажырата білу қажет.



1.1 сурет – OSI моделінің деңгейлері арасындағы байланыс

Қалыптастыру процесі қосымшалар деңгейінде басталады (1.2-сурет). Егер бағдарлама қосымша деңгейіне, мысалы, файлдық қызметке сұрауға салынсын. Осы сұраныстың негізінде қолданбалы деңгейдегі бағдарламалық қамтамасыз ету стандартты форматтағы (түрдегі) хабарлама жасайды.



1.2 сурет – Деректер пакетінің берілісі.

Әдеттегі, қарапайым хабарлама тақырыптар мен деректер өрісінен тұрады. Хабарлама тақырыбы қандай жұмыс істеу керектігін айту үшін желі арқылы тағайындалған машина-мекенжайдың қосымша деңгейіне жеткізілуі керек болатын қызмет туралы ақпаратты қамтиды. Хабарламаны қалыптастырғаннан кейін, қосымша деңгейі оны стекпен төмен қарай ұсыну деңгейіне бағыттайды. ұсыныс деңгейінің хаттамасы, қосымша деңгейдің тақырыбынен алынған ақпарат негізінде қажетті әрекеттерді орындайды және өзінің қызмет ақпаратын, ұсыну деңгейінің тақырыбын - қызметтік ақпарат хабарламасына қосады. Алынған хабарлама төменгі сеанс деңгейіне жіберіледі, ол өз кезегінде тақырыпты және т.б. қосады.

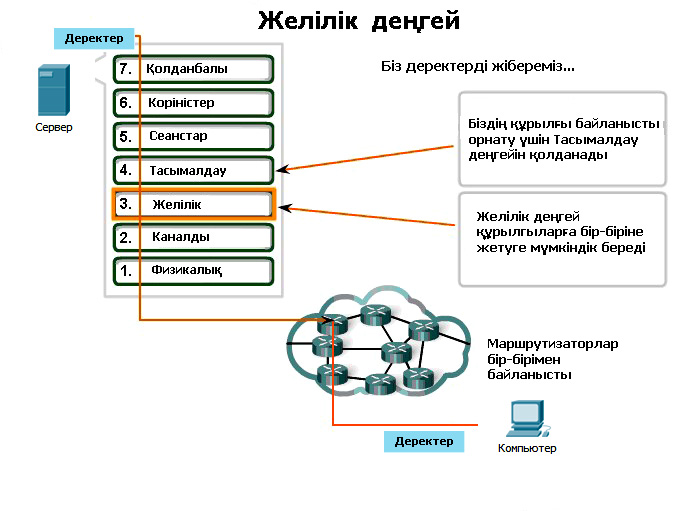
Соңында, хабарлама төменгі физикалық деңгейге жетеді, ол оны байланыс желілері арқылы тағайындалған машинаға жеткізеді. Бұл кезде хабарлама барлық деңгейлердің тақырыптарымен «толып кетті». Хабарлама тағайындалған машинаға желі арқылы келген кезде, оның физикалық деңгейі қабылданады және дәйекті деңгейден деңгейге ауысады. Әр деңгей өз деңгейлеріне сәйкес функцияларды орындай отырып, өз деңгейінің тақырыбын талдайды және өңдейді, содан кейін осы тақырыпшаны алып тастайды және жоғарғы деңгейге хабарлама жібереді.

1.1.2 OSI модел деңгейлері

*Физикалық деңгей* (Physical layer) Физикалық деңгей, физикалық байланыс арналары бойынша биттерді таратумен айналысады, мысалы, коаксиалды кабель, бұралған жұп кабель, талшықты-оптикалық кабель немесе сандық жерүсті каналдар сияқты арналар. Бұл деңгейге деректерді берудің физикалық тасымалдағыштарының сипаттамалары, мысалы, өткізу жолағы, қорғаныс ақаулары,толқындық кедергі және т.б. сияқтылар осы деңгейге байланысты болады. Осы деңгейде дискретті ақпаратты беретін электр сигналдарының сипаттамалары анықталады, мысалы, импульстік жиектердің беріктігі, берілетін сигналдың кернеуі немесе ток деңгейлері, кодтау түрі, сигналдың берілу жылдамдығы. Сонымен қатар, қосқыштың түрлері және әр істіктің қолдану арналымы стандартталады.

*Каналдық (арналық) деңгей* (Data Link layer) Бұл физикалық деңгейде тек биттер жіберіледі. Байланыс желілері бірнеше жұп өзара әрекеттесетін компьютерлердің кезек-кезек пайдаланатынын кейбір желілерде ескермеуі мүмкін, берілістің физикалық ортасы толып кетуі мүмкін. Сондықтан, каналдық (арналық) деңгейдің міндеттерінің бірі – беріліс ортасының болуын тексеру. Каналдық (арналық) деңгейдің тағы бір міндеті – қателерді анықтау және түзету енгізу. Ол үшін каналдық (арналық) деңгейде биттер кадрлар (frames) деп аталатын жиынтықтарға топтастырылады. Арна деңгейі әр кадрдың берілуінің дұрыстығын қамтамасыз етеді, оны таңдау үшін әр кадрдың басында және соңында биттердің арнайы тізбегін орналастырады, сонымен қатар белгілі бір әдіспен кадрдың барлық байттарын өңдеп, бақылау суммасын (мөлшерін) есептеп кадрға қосады. Кадр желі арқылы өткенде, қабылдауыш алынған деректердің бақылау суммасын қайтадан есептеп, нәтижені кадрдан алынған суммамен салыстырады. Егер олар сәйкес келсе, онда кадр жарамды әрі дұрыс және қабылданған болып саналады. Егер бақылау кестелері сәйкес болмаса, онда қате бар деп тіркеледі. Арналық деңгей қателерді анықтап қана қоймай, сонымен қатар бұзылған кадрларды қайта жіберу арқылы түзете алады. Дегенмен, кез-келген топологиялар мен технологиялардың желілерінде хабарламалардың жоғары сапалы тасымалдануын қамтамасыз ету үшін деректерді арналық деңгей функциялары жеткіліксіз, сондықтан OSI моделінде бұл мәселенің шешімі келесі екі деңгейге - желілік және көлікті деңгейлерге жүктеледі.

*Желілік деңгей* (Network layer). Желілік деңгей бірнеше желілерді біріктіретін бірыңғай тасымалдау жүйесін құруға қызмет етеді. Ең жақсы жолды таңдау мәселесі маршруттау деп аталады және оны шешу желілік деңгейдің негізгі міндеттерінің бірі болып табылады. Сонымен қатар, желілік деңгей (1.3 сурет) әртүрлі технологияларды үйлестіру (келістіру), ірі желілерде мекенжайды жеңілдету және желілер арасындағы қажетсіз трафикке сенімді және икемді кедергілерді құрудың мәселелерін шешеді. Желілік деңгей хабарламалары пакеттер (packets) деп аталады.

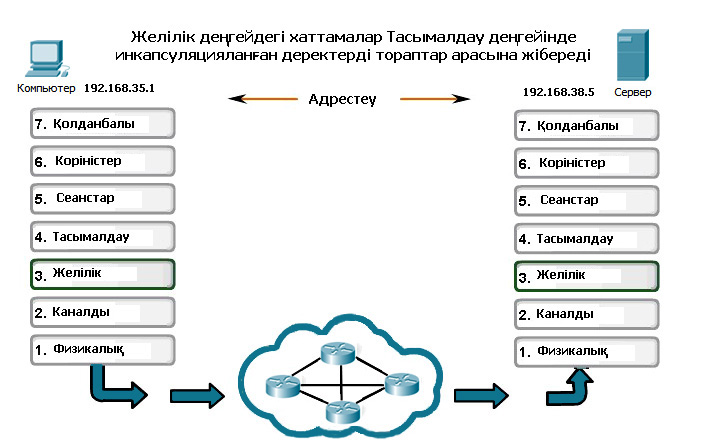


1.3 сурет - Желілі деңгейде деректерді қайта жіберу

*Тасымалдау деңгейі* (Transport layer). Жөнелтушіден алушыға барар жолда пакеттер бұрмалануы немесе жоғалуы мүмкін. Тасымалдау деңгейі пакеттерді қатесіз, бірізділікпен, жоғалтусыз және қайталамай жеткізуге кепілдік береді. Бұл деңгейде хабарламалар қайта жинақталады: ұзын хабарламалар бірнеше пакетке бөлінеді, ал қысқа хабарламалар бір-біріне біріктіріледі. Бұл желі бойынша пакеттік берудің тиімділігін арттырады. Тасымалдау деңгейінде (1.4 сурет) компьютер-алушы хабарлама қораптан шығарылып, бастапқы қалпына келтіріледі және қабылдағаны туралы растау сигналы жіберіледі. Тасымалдау деңгейі ағынды басқарады, қателіктерді тексереді және пакеттерді жіберуге және қабылдауға байланысты мәселелерді шешугеқатысады.

*Сеанс деңгейі* (Session layer). Сеанс деңгейі диалогты басқаруды қамтамасыз етеді: нақты сол уақытта қай жағы белсенді екендігін анықтайды, үндестіру (синхронизация) құралдарымен қамтамасыз етеді. Соңғысы ұзын берілулерге басқару нүктелерін салуға мүмкіндік береді, себебі қиындық не қайтару сияқты жағдайлар туындаған кезде бәрін басынан бастағанға қарағанда басқарудың соңғы нүктесіне қайта оралуға мүмкіндік болу үшін қажет. Іс жүзінде тек бірнеше қосымшалар сеанс деңгейін пайдаланады және ол жеке хаттама ретінде сирек орындалады, дегенмен бұл деңгейдің функциялары көбінесе қолданбалы деңгей функциясымен біріктіріліп, бір хаттамада жүзеге асырылады.

*Ұсыну деңгейы* (Presentation layer). Ұсыну деңгейы оның мазмұнын өзгертпестен желі арқылы берілетін ақпаратты ұсыну түрімен айналысады. Ұсыну деңгейі есебінен бір жүйенің қосымша деңгейімен берілетін ақпарат әрдайым басқа жүйенің қосымша деңгейімен түсіндіріледі. Бұл деңгейде деректерді сандау мен сандарын шешуге болады, осыған байланысты барлық қолданбалы қызметтері үшін дереу мәліметтер алмасудың құпиялылығы қамтамасыз етіледі.



1.4 сурет - Тасымалдау деңгейіндегі деректерді инкапсуляциялау.

##### 

*Қосымша деңгейы* (Application layer) *–* бұл шынымен де желі қолданушыларына электрондық почта хаттамаларының көмегімен файлдар, принтерлер немесе гипермәтіндік веб-беттер сияқты ортақ ресурстарға қол жеткізуге, сондай-ақ, мысалы, оларды пайдалану арқылы өзара әрекеттесуді ұйымдастыруға мүмкіндік беретін әртүрлі хаттамалардың жиынтығы. Қосымша деңгейі жұмыс істейтін мәліметтер бірлігін, әдетте, хабарлама (message) деп атайды.

1.1.3 «Ашық жүйе» түсінігі

OSI моделі, оның аты айтып тұрғандай (Open System Interconnection), ашық жүйелердің өзара байланысын сипаттайды. Ашық жүйе дегеніміз не?

Ашық сипаттамаларға сәйкес құрылған кез-келген жүйені (компьютер, компьютерлік желі, ОЖ, бағдарламалық пакет, басқа аппараттық және бағдарламалық өнімдер) кең мағынада ашық жүйе деп атауға болады. Ескере кететін болсақ, «спецификация» термині (компьютерлік техникада) аппараттық немесе бағдарламалық жасақтама бөліктерінің, олардың қалай жұмыс істейтіндігін, олардың басқа бөліктерімен өзара әрекеттесуін, жұмыс жағдайларын, шектеулерін және арнайы сипаттамаларын қалыптасқан түрде сипаттайды. Әр спецификация стандартты емес екені түсінікті. Өз кезегінде, ашық сипаттама дегеніміз стандартқа сәйкес келетін және барлық мүдделі тараптардың кең талқылауынан кейін келісім нәтижесінде қабылданған, көпшілікке қол жетімді техникалық сипаттамалар.

Жүйелерді әзірлеу кезінде ашық сипаттамаларды пайдалану үшінші тараптарға осы жүйелерді кеңейту және түрлендіруге арналған әртүрлі аппараттық немесе бағдарламалық құралдарды жасауға, сонымен қатар әр түрлі өндірушілердің өнімдерінен бағдарламалық және аппараттық жүйелер жасауға мүмкіндік береді.

Нақты жүйелер үшін толық ашықтық қол жетімсіз идеал болып табылады. Әдетте, тіпті ашық деп аталатын жүйелерде де осы анықтамаға сыртқы интерфейстерді қолдайтын белгілі бір бөліктер ғана сәйкес келеді. Мысалы, операциялық жүйе Unix тобының ашықтығы – бұл ядро мен қосымшалар арасында стандартталған бағдарламалау интерфейсінің болуы, бұл қосымшаларды Unix-тің бір түрінен басқа түріне ауыстыруды жеңілдетеді. Жартылай ашықтықтың тағы бір мысалы, тәуелсіз өндрушілердің желілік адаптерлерін драйверлер жүйесіне қосу үшін жеткілікті түрде жабық Novell NetWare операциялық жүйесінде ашық интерфейсті Open Driver Interface (ODI) пайдалану болып табылады. Жүйенің дамуында қолданылатын техникалық сипаттамалар неғұрлым ашық болса, соғұрлым ашық болады.

OSI моделі ашықтықтың тек бір аспектісін қарастырады, атап айтқанда есептеуіш желіге қосылған құрылғылардың өзара әрекеттесу құралдарының ашықтығы. Мұндағы ашық жүйе дегеніміз – қабылданған және жіберілген хабарламалардың пішінін, мазмұнын және мағынасын анықтайтын стандартты ережелерді қолдана отыра, басқа желілік құрылғылармен өзара әрекеттесуге дайын желілік құрылғы.

Егер екі желі ашықтық принциптеріне толықтай сәйкес болса, онда келесідей артықшылықтарға ие болады:

* әр түрлі өндірушілердің бірдей стандартты ұстанатын аппараттық және бағдарламалық жасақтама желісін құру мүмкіндігі;
* желінің жекелеген құраушыларын басқа жетілдірілген құраушылармен ауыртпалықсыз ауыстыру мүмкіндігі арқылы желінің ең аз шығындармен дамуға мүмкіндік берді;
* бір желіні екіншісіне оңай қосу мүмкіндігі;
* желінің қызмет етуі мен меңгеру өте қарапайым.

#### Халықаралық Интернет желісі ашық жүйенің жарқын мысалы болып табылады. Бұл желі ашық жүйелерге қойылатын талаптарға сәйкес толықтай дамыды. Оның стандарттарын әзірлеуге түрлі университеттерден, ғылыми ұйымдардан және әртүрлі елдерде жұмыс істейтін компьютерлік техниканы және бағдарламалық жасақтаманы өндірушілерден мыңдаған пайдаланушылар қатысты. Интернеттің жұмысын анықтайтын стандарттардың атауы Internet – Request For Comments (RFC) - «Түсініктеме сұрату» деп аударылатын «Түсініктемелерге сұраныс» - қабылданған стандарттардың ашық және мөлдір сипатын көрсетеді. Нәтижесінде Интернет бүкіл әлемде орналасқан көптеген желілердің әртүрлі жабдықтары мен бағдарламаларын біріктіре алды.

#### OSI моделі - бұлжелінің негізі функиясы. Сондықтан, егер сіз OSI моделінің әртүрлі деңгейлерін желілік қосылыстары кезінде өзара әрекеттесетінін түсінсеңіз, нақты желілік функциялардың принциптерін түсінуге болады.

1.1.4 Деректерді желі және кабель арқылы беру

OSI моделі – бұл желінің негізі функиясы. Сондықтан, егер сіз OSI моделінің әртүрлі деңгейлерін желілік қосылыстары кезінде өзара әрекеттесетінін түсінсеңіз, нақты желілік функциялардың принциптерін түсінуге болады. Зерттеуді драйверлерден бастасақ, драйвер – аппараттық желі құраушыларының жұмысын қамтамасыз ететін бағдарламалар.



Драйверлер (driver) – бұл компьютерге әртүрлі құрылғылармен жұмыс істеуге мүмкіндік беретін бағдарламалық жасақтама (қамтамасыз етулер).

Драйверлер компьютерлік құрылғылар мен сыртқы құрылғылардың кез-келген түріне арналған. Драйверді қолданудың жақсы мысалы – принтер драйвері. Принтерлерді көптеген компаниялар шығарады және әртүрлі функциялары мен ерекшеліктері бар. Компьютер өндірушілері компьютерлерді принтердің әр түрімен жұмыс істеуге арналған бағдарламалық жасақтамасымен қамтамасыз ете алмай жатыр. Оның орнына, принтер өндірушілері өз принтерлеріне драйверлер жасайды, және сіздің компьютерініз құжаттарды принтерге жібере алатын болса, алдымен компьютерге осы құрылғымен байланысуға мүмкіндік беретін драйверді жүктеу керек.



#### 

Желілік адаптер картасының драйверлері рұқсат етілген басқару (OSI моделінің арналық деңгейі) ортасында орналасқан. Рұқсат етілген басқару ортасы желі адаптері карталарының физикалық деңгейіне бірлесіп қол жеткізуіне жауап береді, яғни драйверлер компьютер мен тақтаның арасындағы тікелей байланысты қамтамасыз етеді. Бұл, өз кезегінде компьютерді желіге қосады.

Компьютер және сыртқы құрылғылар бір-бірімен байланыса алса, желі компьютерлер арасында деректерді тасымалдауға дайын. Алайда, файлдардың көпшілігі оларды бүкіл кабель арқылы беру үшін тым үлкен. Біріншіден, мұндай блок кабельді толтырады және бүкіл желінің жұмысын «байланыстырады», екіншіден, қателіктердің пайда болуы бүкіл құрылғыны қайта таратуға алып келеді. Деректерді желі арқылы жылдам және оңай беру үшін, оны кішкене басқарылатын блоктарға бөлу керек.



Пакеттер – бұл файлдарға бөлінетін басқарылатын деректер блогы. Пакет компьютерлік желілердегі ақпараттың негізгі бірлігі болып табылады. Деректерді пакеттерге бөлген кезде олардың берілу жылдамдығы өсетіні соншалық, желідегі кез келген компьютер басқа компьютерлермен бір уақытта деректерді қабылдау және беру мүмкіндігін алады.



Пакеттердің құрамдас бөліктері: тақырып, мәліметтер, тіркеме (тіркеме). Тақырыпқа кіреді:

- пакеттің беріліп жатқандығы туралы сигнал;

- бастапқы мекен-жайы;

- белгіленген мекен-жайы;

- беруді синхрондаушы ақпарат.

Трейлер көбінесе қателіктерді тексеру туралы ақпаратты қамтиды, бұл циклдік азайтуды тексеру (Cyclical Redundancy Check, CRC) деп аталады. CRC – бұл пакеттік және бастапқы ақпараттарды математикалық қайта құру нәтижесінде алынған сан. Пакет діттеген жеріне жеткенде, бұл түрленулер қайталанады. Егер нәтиже CRC-пен сәйкес келсе, пакет қатесіз қабылданады.

Байланыс орнатылатын компьютерлер біршама халықаралық ұйымдарды еске түсіреді. Бұл ұйымдар пайдалана алатын көптеген тілдер мен қарым-қатынас әдістері бар. Есте сақтау маңызды: өзара түсіністікке жету үшін қарым-қатынасқа қатысушылардың бәрі бірдей тілде сөйлеуі керек және бірыңғай ережелер мен хаттамаларды ұстануы керек.



Хаттамалар – бұл кейбір байланыстарды жүзеге асыруды реттейтін ережелер мен рәсімдер жиынтығы.

Хаттамаларға қатысты үш негізгі ойды есте сақтаңыз:

1. Көптеген хаттамалар бар. Әр протокол әртүрлі мақсаттарға ие, әртүрлі тапсырмаларды орындайды, өзіндік артықшылықтары мен шектеулері бар.

2. Хаттамалар OSI моделінің әртүрлі деңгейлерінде жұмыс істейді. Хаттама функциялары оның жұмыс жасау деңгейімен анықталады.

3. Бірнеше хаттамалар бірге жұмыс істей алады. Оларды жиынтықтар немесе хаттама жиынтығы деп аталады. Желі бойынша мәліметтерді беру өзгермейтін тәртіптегі қадамдар қатарынан тұрады. ережелері мен рәсімдерін анықтайды. Жіберетін және қабылдайтын компьютерлер келесі процедураларды орындау үшін хаттамаларды қолданады:

- мәліметтерді пакеттерге бөлу;

- пакетке мекен-жай мәліметтерін қосу;

- пакеттерді таратуға дайындау;

- кабель арқылы берілетін пакеттерді қабылдау;

- бастапқы деректер блоктарын жинақтау үшін пакеттен деректерді көшіру;

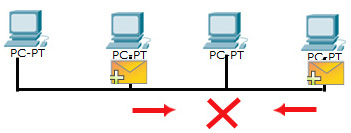
- қалпына келтірілген блоктарды компьютерге беру.



Дұрыс хаттамаларды орнату желінің дұрыс жұмыс істеуінің кепілі емес. Компьютер деректерді кабель арқылы беру үшін әртүрлі қол жетімді болатын әдістерді қолданады.

Рұқсат етілген (қол жетімді) әдіс дегеніміз – компьютердің желілік тора арқылы деректерді қалай жіберіп, қабылдау керектігін анықтайтын ережелер жиынтығы.

Желіде бірнеше компьютер кабельді бірдей бірге бөлісу керек. Алайда, егер екі компьютер бір уақытта деректерді жіберуге тырысса, олардың пакеттері бір-бірімен «соқтығысып», бүлінеді. Бұл соқтығысу (коллизия) деп аталады (1.5 сурет).



1.5 сурет. Екі компьютерден біруақытта деректерді беру соқтығысуға алып келеді

Қол жеткізу тәсілдері бірнеше компьютердің бір уақытта кабельге байланысуға жол бермейді. Қол жеткізудің негізгі әдістері:

* сoll соқтығысуды анықтаумен тасымалдаушының басқаруымен бірнеше рет қол жеткізу;
* сoll соқтығысуды болдырмай тасымалдаушыны басқарумен бірнеше рет қол жеткізу;
* маркерді беру арқылы қол жеткізу;
* басым сұраныс бойынша қол жеткізу.

1. CSMA/CD (Carrier-Sense Multiple Access with Collision Detection) – шина мен жұлдыз топологияларында соқтығысуды анықтаумен тасмалдайтын бақылаушы бірнеше қол жетімділік қолданылады. Станциялар деректерді беру арнасын тыңдайды. Көбінесе, желідегі бірнеше компьютер деректерді беруді «қалайды» (демек, бірнеше), компьютерлер кабельді «тыңдайды» (демек, оператордың басқаруымен). Деректерді жіберген кезде, компьютерлер кабельді тыңдайды, соқтығысуды анықтағаннан кейін біраз уақыт күте тұрыңыз, содан кейін беруді қайта жаңартыңыз, осы жерде – соқтығысулар анықталад.

Сонымен қатар, соқтығысуларды анықтау мүмкіндігі CSMA/CD-нің өзін шектейтін себеп болып табылады. 2,5 км-ден асатын қашықтықтағы сигналдың әлсіреуіне байланысты соқтығысуды анықтау механизмі тиімді емес. CSMA/CD пікірталас әдісі ретінде белгілі, өйткені желілік компьютерлер мәліметтерді жіберу құқығы үшін өзара бәсекелеседі (бәсекелеседі). Бұл өте қиын болып көрінеді, бірақ CSMA/CD-нің қазіргі заманғы енгізілімдері соншалықты тез, сондықтан пайдаланушылар бәсекеге қабілетті қол жетімділік әдісін қолдану туралы ойламайды. Бірақ желідегі компьютерлер көп болған сайын, желілік трафик соғұрлым көп болады. Соқтығысулар саны артады, сәйкесінше бұл желінің баяулауына әкеледі. Сондықтан, кейбір жағдайларда CSMA/CD әдісінің жылдамдығы жеткіліксіз болуы мүмкін.

Әрбір соқтығысқаннан кейін екі компьютер де беруді қайта жаңартуы керек. Егер желіде тұтыну өте көп болса, қайталанған әрекеттер қайтадан қақтығысқа әкелуі мүмкін, бірақ басқа компьютерлермен. Енді төрт компьютер беруді қайта жаңарта бастайды. Осындай қайта беру көшкін тәрізді ұлғайса, онда бүкіл желінің жұмысын бұзуы мүмкін.

2. CSMA/CA (Carrier-Sense-ке бірнеше соқтығысуға қарсы қол жеткізу) – соқтығысуды болдырмайтын тасымалдаушы бақылаушы бірнеше реттік қол жетімділік. CSMA/CA әдісін қолдана отырып, әр компьютер деректерді желіге жібермес бұрын өзінің ниетін білдіреді, сондықтан қалған компьютерлер алдағы тасымал туралы «біледі» және осылайша соқтығысуды болдырмауы мүмкін.

Дегенмен, хабарландыру хабарламасы желінің жалпы трафигін арттырады және оның өткізгіштік қабілетін азайтады, сондықтан желі CSMA/CA әдісі CSMA/CD әдісіне қарағанда баяу жұмыс істейді.

3. Маркермен берілу арқыы қол жеткізу әдісі. Маңыздылығы, бұл пакеттің ерекше түрі (маркер) сақина бойынша айналады. Компьютер маркерді (таңбалауышты) күтіп, оны ұстап алады, ақпаратты толтырады және адресатқа жібереді. Бұл уақытта басқа компьютерлер таңбалауышты босатуды күтуде. Кез келген уақытта бір компьютер маркерді қолданатындықтан, желіде бәсекелестік болмайды, соқтығысулар болмайды және кідірістер болмайды.

4. Сұранымның басымдылығы бойынша қол жетімділік желінің тек концентраторлар (хабтар) мен түйіндерден жасалғанына негізделген. Концентраторлар (хабтар) кабельге қол жеткізуді басқарады, желідегі барлық түйіндерді кезекпен сұрайды және берілу сұраныстарын анықтайды. Концентратор (хаб) барлық мекен-жайларды, байланыстар мен тораптарды біліп, олардың жұмыс істеуін тексеруі керек. Бір уақытта екі сұраныс алғаннан кейін, концентратор (хаб) алдымен сұранысқа басымдық береді. Егер сұраулар бірдей басымдыққа ие болса, оларға кездейсоқ түрде қызмет көрсетіледі. Осылайша, сұраныс басымдықтары бойынша қатынасу тек жіберуші компьютер, концентратор және қабылдаушы компьютер арасында жүзеге асырылады. Концентратор (хаб) деректерді беру арқылы орталықтан басқарылады және ол желідегі барлық басқа компьютерлерге берілмейді.



Тексеру жұмыс №1

**1 жаттығу Сөйлемді аяқтаңыз:**

А бағанынан сөйлемнің басын В бағаннан сөйлемнің соңына сәйкес келтінін қойыңыз. Нұсқаны таңдағаннан кейін, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір затты тек бір рет пайдалануға болады.

**Баған A**

1. Қолданбалы деңгей \_\_\_

2. Арна деңгейі \_\_\_\_\_\_\_\_

3. Желілік деңгей \_\_\_\_\_\_

4. Атқарушы деңгей \_\_\_\_

5. Тасымалдау деңгейі \_\_

6. Физикалық деңгей \_\_\_\_

7. Сеанс деңгейі \_\_\_\_\_\_\_\_

**Баған В**

A. Деректерді қатесіз жіберуді қамтамасыз етеді

B. Компьютерлер арасындағы маршрутты анықтайды

B. Басқару нүктелерін деректер ағынына орналастыру арқылы пайдаланушы тапсырмаларын синхрондауды қамтамасыз етеді

Г. Барлық мекен-жайларды, қатынастардың жұмыс істеуін тексеруді жүргізеді

Д. пайдаланушы қосымшаларын тікелей қолдайтын қызметтерді ұсынады

E. Өңделмеген биттерді физикалық деңгейінен деректер деректер кадрына жинақтайды

Ж. Деректер форматын аударуға жауапты

З. Желілік кабельді адаптерге қосу әдісін анықтайды.

**№2 жаттығу Дұрыс жауапты таңдаңыз**

1.OSI моделі Project 802 стандарттарының қандай деңгейлері үшін анықтайды?

а) Қолданбалы және атқарушы (өкілдік)

б) Физикалық және арналық

в) Желі және арналық

г) Тасымалдау және желілік

2. Қол жеткізуді басқару ішкі деңгейы OSI қандай деңгейіне жатады?

а) Тасымалдау

б) физикалық

в) желілік

г) арналық

3. Компьютер мен принтердің бірге жұмыс істеуіне не көмектеседі?

а)драйверлер

б) пакеттік процессор

в) хаттамалар

г) құрылғылардың барлығы

4. NetBEUI хаттамасына қай мәлімдеме жатады?

a) өз желісі үшін АҚШ қорғаныс министрлігі жасаған

б) Microsoft фирмасының барлық желі өнімдерімен бірге жеткізілетін шағын, жылдам және тиімді тасымалдау деңгейының хаттамалары

в) сеанстық деңгейдегі, желімен қолданбалы интерфейсі ретінде жұмыс істейтін ЛВС бірге IBM интерфейсі

г) Novell желілерінде қолданылатын хаттамалар жиынтығы

5. Деректерді сығу OSI моделінің қай деңгейінде жүзеге асырылады?

а) Желі

б) арна

в) физикалық

г) атқарушы

6. Деректерді жібермес бұрын, компьютер трафиктің болуын анықтау үшін кабельді «тыңдайды». Олар қандай қол жетімді әдісін қолданады?

а) CSMA/CD

б) CSMA/CA

в) маркер берумен

г) сұраныс

7. Маркер берілуімен қол жетімділік әдісі келесілерге байланысты соқтығыстардың алдын алады

а) маркердің соқтығысуын болдырмауға көмектесетін кодты қолдану

б) әртүрлі маршруттар бойынша қозғалатын бірнеше маркерлердің болуы

в) маркерді бір компьютермен бір уақытта қолдану

г) желілік трафиктің қарқындылығын бақылау үшін аймақтарды пайдалану.

8. Драйвер - бұл:

а) аппараттық қамтамасыз ету

б) перифериялық құрылғы

в) плата

г) бағдарламалық қамтамасыз ету

9. Желілік ортада желілік адаптер платасының драйвері қажет:

a) желідегі басқа адаптер платасымен байланыс үшін

б) адаптер палатасы мен компьютердің операциялық жүйесі арасындағы байланыс үшін

c) файлдық сервер мен желідегі басқа компьютерлер арасындағы байланыс үшін

г) желідегі әр түрлі компьютерлер арасындағы байланыс үшін.

10. Принтер драйверлеріне қолданылатын мәлімдемені таңдаңыз:

a) Барлық принтерлердің толыққанды жұмысын қамтамасыз ететін әмбебап принтер драйвері бар

б) Бір өндіруші шығарған барлық принтерлер бірдей драйверді қолдана алады.

в) Әр принтер моделі үшін осы принтер моделінің барлық функцияларын пайдалануға мүмкіндік беретін арнайы драйвер жасалады

г) Бір өндірушінің лазерлік принтер драйвері өндірушіге қарамастан барлық лазерлік принтерлердің толық функционалдығын қамтамасыз етеді.

**№3 жаттығу Мәлімдемені растаңыз немесе жоққа шығарыңыз**

1. OSI моделінде барлық желілік операциялар жеті деңгейге бөлінеді. Иә Жоқ
2. Бір компьютердегі әр деңгей басқа компьютердегі сол деңгейге тікелей қосылады. Иә. Жоқ.
3. Арналық деңгейы желілік жабдықтың қалай жалғанғанын анықтауға арналған. Иә. Жоқ.
4. Желілік деңгей жіберілетін компьютерден қабылдаушы компьютерге дейінгі бағытты анықтайды. Иә. Жоқ.
5. В Project 802 OSI моделінің арналық деңгейі екі ішкі деңгейлерге бөлінеді: Логикалықбайланыстарды басқару және қол жетімді басқару ортасы. Иә. Жоқ.
6. Пакет тақырыптары CRC деп аталатын қателіктерді тексеру туралы ақпараттан тұрады. Иә. Жоқ.
7. Пакеттің құрылымы екі компьютер - жіберуші және алушы қолданатын байланыс әдісімен немесе хаттамамен анықталады. Иә. Жоқ.
8. Әр желілік адаптер платаасы кабель арқылы жіберілген барлық пакеттерді «көреді», бірақ пакеттік мекен-жайы компьютер мекен-жайына сәйкес келген кезде ғана ол оның жұмысын тоқтатады. Иә. Жоқ.
9. Пакет трейлері белгіленген мекен-жайдан тұрады. Иә. Жоқ.
10. Бірнеше хаттамалар бірігіп жұмыс істей алады, бұл хаттамалар жиынтығы деп аталады. Иә. Жоқ.
11. Желілік хатамалар қосымшалар арасында мәліметтер алмасуды қамтамасыз етеді. Иә. Жоқ.
12. TCP / IP маршрутизацияны қолдайтындықтан, ол әдеттежелі арасындағы хатама ретінде қолданылады. Иә. Жоқ.
13. Қол жеткізу әдістері бірнеше компьютердің бір уақытта кабельге кіруіне жол бермейді. Иә. Жоқ.
14. Мәліметтерді беру кезінде CSMA/CD пайдалану бірнеше компьютер деректерін жібере алады. Иә. Жоқ.
15. Қарқынды трафикпен соқтығысулар саны артады, бұл желінің өткізу қабілеттілігінің төмендеуіне әкеледі. Иә. Жоқ.
16. Сұранымның басымдылығы бойынша қол жеткізу әдісімен беріліс желідегі барлық компьютерлерге таратылады. Иә. Жоқ.
17. Маркер (Таңбалауыш) - бұл сақина бойынша айналатын пакеттің ерекше түрі. Иә. Жоқ.
18. Кез-келген уақытта маркермен беру арқылы қол жеткізу әдісі кезінде тек бір компьютер ғана маркерді қолдана алады. Иә. Жоқ.

**№ 4 Қолданбалы тапсырмалар**

1. Бастапқы шарттар: Фирмада серверге негізделе отыра желіге ие. Үш жаңа компьютерді қостық. Әкімшілік желілік ОЖ-ны жаңа компьютерлерге орнатты. Қызметкерлер жаңа компьютерлерді қосқан кезде олар керемет графикті көрді, бірақ желі бойынша ешкіммен байланыса алмады. Олардың компьютерлері желіге мүлдем қосылмаған және автономды режимде жұмыс істейтін сияқты. Ескі компьютерлер ештеңе болмағандай жұмыс істейді. Бұл жағдайдың себебі неде?

Сіздің шешіміңіз.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Баспа құжаты желі арқылы жіберіледі. Тек құжаттың жоғарғы жартысы басылған. Бұл мәселені тек бір қолданушыда болуда, ал басқалары осыған ұқсас құжаттарды сәтті басып шығарады.

Басып шығаруда қиындық тудыратын себептердің бірі неде?\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 1.2. Желілік технологиялар

1.2.1 Ethernet желісінің технологиясы

***Желілік технологиялар*** – бұл компьютерлік желіні құруға жеткілікті болып саналатын, стандартты хаттамалар мен оларды жүзеге асыратын бағдарламалық 0амтамасыз ету мен аппараттық құралдардың (мысалы, желілік адаптерлер, драйверлер, кабельдер мен қосқыштар) жүйелік жиынтығы. «Жеткілікті» эпитеті бұл жиынтық жұмыс істейтін желіні құруға болатын құралдардың ең аз жиынтығы екендігін көрсетеді. Мүмкін бұл желіні, мысалы, Ethernet стандартты хаттамаларына қосымша IP хаттамасын, сонымен қатар арнайы байланыс құрылғыларын – маршрутизаторларды қолдануды қажет ететін қосалқы желілерді бөлу арқылы жетілдіруге болатын шығар. Жақсартылған әрі жетілдірілген желі, желінің негізін құрайтын Ethernet технологиясы арқылы қосымша қондырғылардың көмегімен сенімді және жылдамырақ болады.

Ethernet стандарты 1980 жылы қабылданды. Осы технология негізінде салынған желілердің саны қазіргі уақытта 5 миллионға бағаланады, ал мұндай желілерде жұмыс істейтін компьютерлердің саны 50 миллионға жетеді.

Ethernet негізінде қойылған негізгі міндет – бұл деректер берудің бөлінетін ортасында қол жеткізудің кездейсоқ әдісі. Мұндай орта ретінде қалың немесе жұқа коаксиалды кабель, бұралған жұп, оптикалық талшық немесе радио толқындарын пайдалануға болады.

Ethernet стандарты электр байланыстарының топологиясын қатаң түрде бекітеді. Компьютерлер бөлінетін ортаға «жалпы шина» типтік құрылымына сәйкес қосылады (1.6 сурет). Кез келген екі компьютер уақытты бойынша бөлетін шинаның көмегімен деректерді алмасады. Байланыс желісіне қол жеткізуді арнайы контроллерлер – Ethernet желісінің адаптерлері басқарады. Әр компьютерде, дәлірек айтқанда, әр желілік адаптерде ерекше мекен-жайға ие. Деректер беру 10 Мбит/с жылдамдықпен жүреді. Бұл мән Ethernet желісінің өткізу қабілеттілігі болып табылады.

Ethernet желісінің негізгі сипаттамалары:

-дәстүрлі топология сызықты (желілік) шина

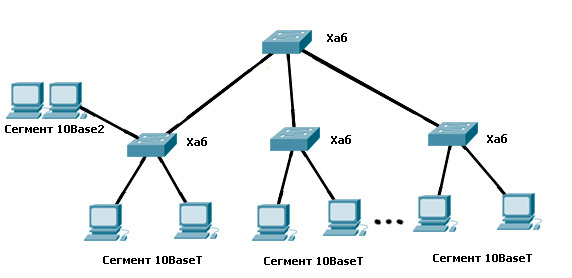
-басқа топологиялар жұлдыз - шина

- берілу түрі тар жолақты

-қол жеткізу әдісі CSMA/CD

-мәліметтер жылдамдығы 10 және 100 Мбит/с

-кабельдік жүйе жуан және жұқа коаксил, UTP



1.6 сурет - Ethernet желісіне мысал.

Кездейсоқ қол жеткізу әдісінің маңызы келесідей. Ethernet желісіндегі компьютер желі бос болған жағдайда, яғни басқа бірде-бір компьютер алмаспаған жағдайда ғана деректерді желі арқылы жібере алады. Сондықтан Ethernet технологиясының маңызды бөлігі - ортаның қол жетімділігін анықтау тәртібі.

Компьютер желі бос екеніне көз жеткізгеннен кейін, ол беруді бастайды және сонымен бірге қоршаған ортаны «түсіреді». Бөлінетін ортаны бір түйінге ерекше пайдалану уақыты бір кадрдың берілу уақытымен шектеледі. Кадр – бұл Ethernet желісінде компьютерлер арасында алмасатын мәліметтердің бірлігі. Кадр бекітілген форматқа ие және деректер өрісімен қатар алушының мекен-жайы және жіберушінің мекен-жайы сияқты қызметтік ақпараттардан тұрады.

Ethernet желісі, кадр деректерді беруде бөлінетін ортаға кірген кезде, барлық желілік адаптерлер бір уақытта осы кадрды ала қабылдап бастайтындай етіп жасалған. Олардың барлығы кадрдың бастапқы өрістерінің бірінде орналасқан мекен-жайды талдайды, егер бұл мекен-жай өзінің адресіне сәйкес келсе, кадр желілік адаптердің ішкі буферіне орналастырылады. Осылайша, тағайындалған компьютер оған арналған мәліметтерді алады.

Кей жағдай бір уақытта екі немесе одан да көп компьютерлер желінің бос екендігі туралы шешім қабылдап, ақпаратты жібере бастағанда мәселе туындауы мүмкін. Соқтығысу деп аталатын бұл жағдай желі арқылы деректердің дұрыс берілуіне жол бермейді. Ethernet стандарты соқтығысуларды анықтау және дұрыс өңдеу алгоритмін қарастырады. Соқтығудың пайда болу ықтималдығы желілік трафиктің қарқындылығына байланысты.

Соқтығысу анықталғаннан кейін, өздерінің кадрларын жіберуге тырысқан желілік адаптерлер беруді тоқтатады және кездейсоқ үзілістен кейін олар қайтадан ортаға кіріп, соқтығысуды тудыруға алып келген кадрды беруге тырысады.

Ethernet желілерінің басты артықшылығы, яғни танымал болуына себеп болған, олардың үнемділігі болып табылады. Желіні құру үшін әр компьютерге бір желілік адаптер, сонымен қатар қалаған ұзындықтағы коаксиалды кабельдің бір физикалық кесіндісі жеткілікті. Сонымен қатар, Ethernet желілерінде ортаға қол жетімді мекен-жай және деректерді берудің қарапайым алгоритмдері енгізілген. Желінің жұмыс жасау логикасының қарапайымдылығы жеңілдетуге алып келеді, сәйкесінше,желілік адаптерлер мен олардың драйверлерінің арзандауына алып келеді. Сол себепті де, Ethernet адаптерлері өте жоғары сенімділікке ие. Сонымен, Ethernet желілерінің тағы бір керемет ерекшелігі - олардың жақсы таралуы, яғни жаңа түйіндерді қосу кезіндегі қарапайымдылығы. Ethernet желілері кабельдік және топологияның әртүрлі нұсқаларын пайдаланады. Біз төрт Ethernet топологиясын қарастырамыз.

1. 1990 жылы 10BaseT бұралған жұп кабелі негізінде Ethernet желісін құруға арналған 802.3 сипаттамасы жарияланды (10 биттік жылдамдығы 10 Мбит/ с, базалық-тар жолақты, Т – бұралған жұп). Осы типтегі желілердің көпшілігі жұлдыз түрінде жасалған, бірақ олар сигнал тарату жүйесі бойынша шинаны ұсынады. Әдетте, 10BaseT желі концентраторы мультипорттық қайталаушы рөлін атқарады. Әр компьютер концентраторға қосылған кабельдің екінші ұшына қосылады және екі жұп сым қолданады: біреуін қабылдау үшін, екіншісін беру үшін. 10BaseT сегментінің максималды ұзындығы – 100 м, минималды кабельдің ұзындығы – 2,5 м. ЛВС 10BaseT 1024 компьютерге дейін қызмет ете алады.

2. 10Base2 (10-биттік жылдамдығы 10 Мбит/с, Base – тар жолақты, 2 - 100 м-ден екі есе асатын қашықтыққа беру). Желінің бұл түрі жұқа коаксиалды кабельге бағытталған, ең аз ұзындығы 0,5 м. Компьютерлердің ең көп саны - 30. Жұқа Ethernet желісі – кішігірім кеңселер мен жұмыс топтарына арналған желілерді іске асыруда үнемді әдіс. Желі төрт репитермен қосылған, ең көп дегенде бес кабельдік сегменттерден тұра алады, бірақ жұмыс станцияларына тек үш сегмент қосыла алады. Осылайша, екі сегмент қайталаушылар үшін сақталған, оларды репитер аралық қосылыстар деп атайды. Бұл конфигурация әдетте 5-4-3 деп аталады.

3. 10Base5 (10 биттік беру жылдамдығы 10 Мбит/с, базалық-тар жолақты, 5 - 500 м болатын бес сегмент) – бұл стандартты Ethernet деп аталады. Қалың коаксиалды кабельдік желілер (қалың Ethernet) шина топологиясын пайдаланады. Қалың Ethernet магистральдық сегментте 100 түйінге дейін қолдана алады. Магистральды сегмент (магистраль) – бұл негізгі кабель, трансиверлерлерге жұмыс станциялары мен репитерлер байланысқан.

4. 100BaseX (100 биттік беру жылдамдығы, 100 Мбит/с, базалық-тар жолақты, X - кеңейту) – бұл қолданыстағы Ethernet стандартының кеңеюі. UTP 5-ші категориясында тұрғызылған, CSMA/CD-ге қол жетімді әдісін және жұлдыз-шина топологиясын қолданады, мұнда барлық кабельдер конентраторға қосылған.

5. Gigabit Ethernet (жылдамдығы 1 Гб/с). Gigabit Ethernet стандарты жақында ғана кәсіпорындар нарығында пайда болды. Оның басты артықшылығы – 10 және 100 мегабиттік Ethernet стандарттарымен бірдей желіні пайдалану мүмкіндігі. Мұнда сонымен қатар қашықтықтағы шектеулер туралы ойлану керек, бірақ ол сервер фермасына қандай артықшылықтар бере алады.

1.2.2 Token Ring желілік технологиясы

Token Ring желісін алғаш IBM компаниясы 1970 жылдары жасаған. Бұл әйгілі Ethernet-тен кейінгі локалды желілер үшін екінші орында тұрған IBM негізгі технологиясы.

Token Ring желісінің негізгі сипаттамалары:

-дәстүрлі топология сақина

-басқа топологиялар жұлдыз-сақина

-берілу түрі тар жолақты

-қол жеткізу әдісі маркер берумен

-деректер беру жылдамдығы 4 және 16 Мбит/с

-кабельдік жүйе UTP және STP

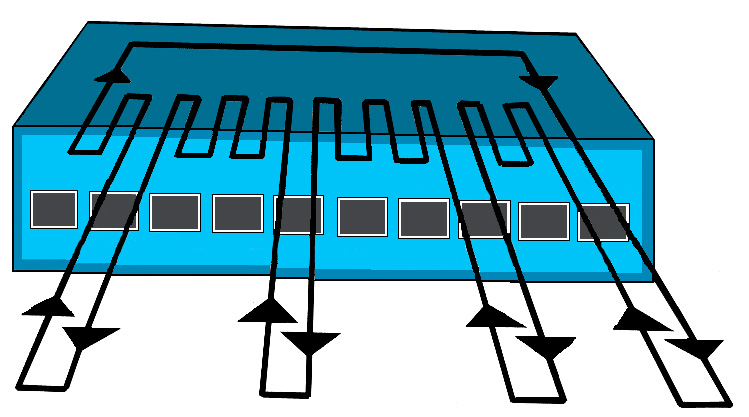
Token Ring желісінде бірінші компьютер жұмыс істей бастағанда, желі маркет өндіреді. Маркер сақина бойынша компьютерден компьютерге өтеді, қашан олардың біреуі деректерді жіберуге дайын екендігі туралы хабарламайынша жүреді және маркермен бақылауды өзіне алады.

**Маркер** – бұл компьютерге деректерді кабель арқылы жіберуге мүмкіндік беретін биттердің (деректер ағынының) алдын-ала реттілігі.

Маркерді түсіріп алғаннан кейін компьютер желіге деректер кадрын жібереді. Кадр қабылдағыштың мекен-жайына сәйкес келетін адресі бар түйінге жеткенге дейін сақина бойынша жүреді. Қабылдағыш-компьютер кадрларды қабылдау буферіне көшіріп алады және кадрдың күйі өрісіне ақпарат алынғандығы туралы жазба жасайды.

Кадр деректер берудің сәтті болғандығын растайтағанша, жіберген компьютерге жеткенше сақина түрінде берілуін жалғастырады. Осыдан кейін компьютер кадрды сақинадан шығарып, маркерді сол жерге қайтарады. Желіде бір уақытта бір ғана маркер берілуі мүмкін және бір бағытта ғана болады. Маркерді беру – детерминистік процесс. Бұл кез келген соңғы станцияның берілуіне дейін өткен максималды уақытты есептеуге болатындығын білдіреді. Бұл сипаттама Token Ring желісін желінің тұрақты жұмыс жасауына маңызды, күту уақытын білу қажет болғанда қолданса өте ыңғайлы етеді. Мұндай қолданыстарға мысал зауыттардағы автоматтандырылған станциялар ортасы болып табылады.

IBM Token Ring желілік станциялары үлкен сақина желісін құру үшін кабельдер көмегімен біріктірілген MAU (Multistation Access Unit) торабына тікелей қосылған (1.7 сурет).



1.7 сурет – Концентраторда сақинаның қалыптасуы (маркердің қозғалысы көрсетілген)

Ажыратқыш кабельдер MAU аралас MAU арқылы қосады. Жапырақшалы – кабельдер MAU-ны станцияларға қосады. МAU құрамына станцияларды сақинадан шығаруға арналған шунттаушы реле кіреді. Осылайша, сәтсіз компьютер (немесе қосылыс) бүкіл Token Ring желісінің жұмысына әсер етпейді. Оған сегіз компьютерге дейін қосуға болады. Алайда, Token Ring желісі бір сақинамен шектелмейді, әр сақинада 33 концентратор есептелген болуы мүмкін.

Сақина толған кезде, яғни әр MAU портына компьютер қосылған, желіні басқа сақина қосу арқылы кеңейтуге болады. Негізгі басты звңдылықты ұстану керек: әрбір MAU сақинаның бөлігі болатындай етіп қосылуы керек. MAU-дегі «кіріс» және «шығу» ұяшықтары кабельдің көмегімен бір сақинада жиналған 12 MAU-ға дейін қосылуға мүмкіндік береді.

1.2.3 Apple Talk және Arc Net желілік технологиялары

Apple Computer, Inc. компаниясы 1983 жылы шағын жұмыс топтары үшін жеке меншік желілік архитектурасы ретінде Apple Talk ұсынды. Желі мүмкіндіктері Macintosh компьютерлерінде құрастырылған, бұл Apple Talk желісін басқа желілермен салыстырғанда оңай іске асырды.

Apple Talk желісінің негізгі сипаттамалары:

-дәстүрлі топология шина немесе ағаш

-берілу түрі тар жолақты

-қол жеткізу әдісі CSMA/CА

-мәліметтер жылдамдығы 2 Кбит/с

-кабельдік жүйе UTP,талшықты-оптикалық кабель

Apple Talk клиент-сервердің таралған желілік жүйесі ретінде жасалды. Басқаша айтқанда, пайдаланушылар желілік ресурстарды (файлдар мен принтерлер сияқты) бірге қолданады. Осы ресурстарды қамтамасыз ететін компьютерлер қызметтік құрылғылар деп аталады; қызметтік құрылғылардың желілік ресурстарын пайдаланатын компьютерлер тұтынушылар (*clients*) деп аталады. Белгілі бір деңгейде сервистік құрылғылармен өзара әрекеттесу қолданушы үшін айқын әрі анық болып табылады, себебі компьютердің сұралған материалдың орналасқан жерін өзі анықтайды және оған пайдаланушыдан қосымша ақпарат алмастан қол жеткізеді. Таратылған жүйелер пайдаланудың қарапайымдылығымен қатар, басқа жүйелерге қарағанда экономикалық артықшылықтарға ие, яғни маңызды материалдарды көптеген жерлерде емес, бірнеше жерде орналастыруға болады.

*LocalTalk –* бұл Apple компаниясының жеке меншік патенттелген тасымалдаушыға қол жеткізу жүйесі. Ол қол жетімділікке жету үшін бәсекелестікке негізделген, шина көмегімен бірігу топологиясы мен базистік сигналдарды беру жолақтарында (baseband signaling) және 230,4 Кбит/с жылдамдықта, бұралған жұп экрандалған болып табылатын тасымалдағышта жұмыс істейді. LocalTalk сегменттерін 300 метрге дейін тасымалдауға және 32 түйінді қамтамасыз етуге болады.

Apple Talk бірнеше желілік құрылымдарды анықтайды. Ең қарапайым – бұл түйін, бұл Apple Talk желісіне қосылған кез-келген құрылғы. Ең көп таралған түйіндер – бұл Macintosh компьютерлері және лазерлік принтерлер, бірақ көптеген басқа компьютерлер Apple Talk-пен байланыс орната алады, соның ішінде IBM компьютерлерімен, сандық жабдықтармен жұмыс істейтін VAX компьютерлерімен және әртүрлі жұмыс станцияларымен байланыс орната алады. Apple Talk анықтаған келесі нысан – бұл желі. Apple Talk желісі – бұл бөлек логикалық кабель. Бұл логикалық кабель көбінесе жеке физикалық кабель болғанымен, кейбір физикалық орталықтар бірнеше физикалық кабельдерді біріктіру үшін көпірлерді пайдаланады. Сонымен, Apple Talk аймағы – бірнеше желілердің логикалық тобы (1.8-сурет, бір-бірінен алыс орналасқан).

Arc Net ортасы 1977 жылы Datapoint корпорациясымен жасалған. Бұл жұмыс топтары желі масштабы үшін қарапайым, икемді, арзан желілік архитектура.

Arc Net желіснің негізгі сипаттамалары:

-дәстүрлі топология жұлдызды -шина

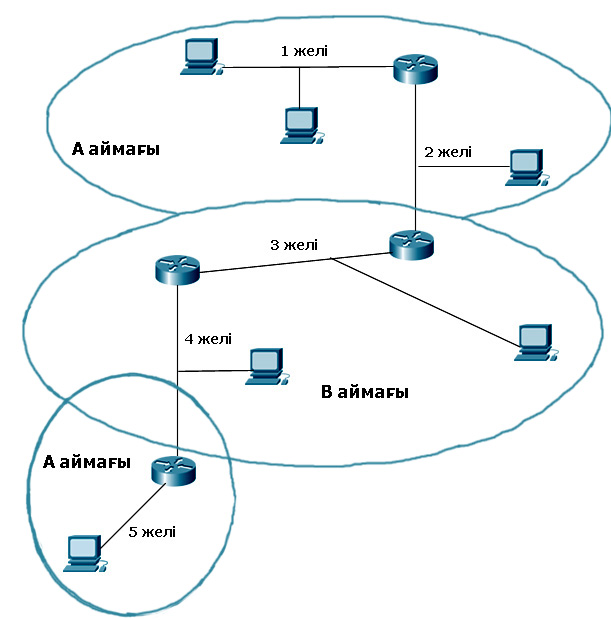
-берілу түрі тар жолақты

-қол жеткізу әдісі маркер берумен

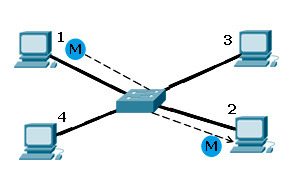
-мәліметтер жылдамдығы 2,5 – 20 Мбит/с

-кабельдік жүйе коаксиалды кабель

Arc Net компаниясы маркерлерді пайдаланатындықтан, Arc Net-дегі компьютерге деректерді жіберуді бастау үшін маркер қажет. Физикалық орналасқан жеріне қарамастан, маркер бір компьютерден екінші компьютерге берілген сериялық нөмірлерге сәйкес өтеді (1.9 сурет).



1.8 сурет – Apple Talk нысандары.



* 1. сурет. Маркер сериялық нөмірлеріне сәйкес компьютерден компьютерге берілуі
     1. Үлкен желілерді құру

Компаниялар өскенде, олардың желілері де дами түседі. Жергілікті желілерде олар бастапқы жобалардан асып түседі. Бұл келесі жағдайлардан көрінеді:

- желілік трафик өткізу қабілеттілігінің шегіне жетті;

- басып шығару тапсырмаларын келесі өңдеуді күту уақыты ұлғайды;

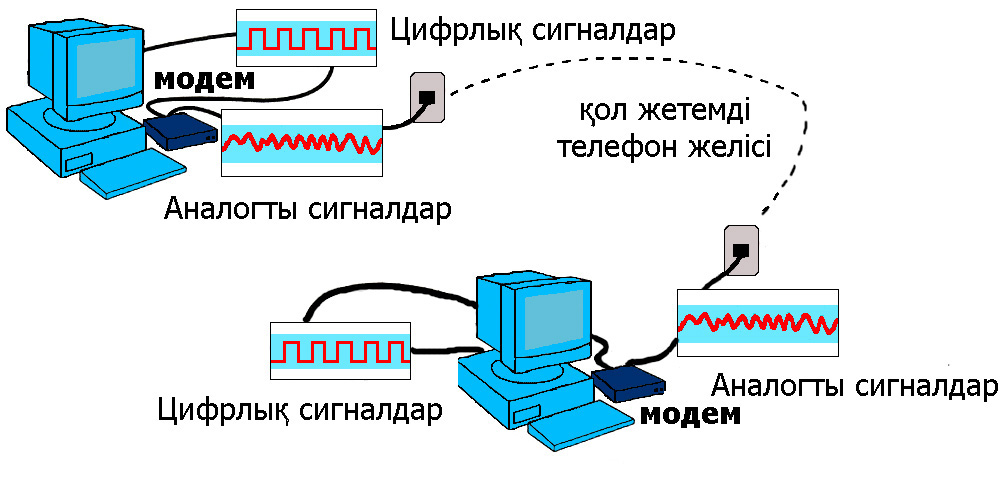
- деректер базасы сияқты желімен қарқынды жұмыс істейтін қосымшалардың жауап беру уақыты артты.

Әрбір әкімшінің жұмысында ерте ме, кеш пе, ол желінің көлемін ұлғайтуға немесе оның жұмысын жақсартуға тура келетін сәт туындайды. Жаңа компьютерлер қосу және қосымша кабель салу арқылы желіні кеңейту мүмкін емес. Кез келген топологияның немесе архитектураның шектеулері бар. Дегенмен, қазіргі жағдайда жұмыс жасап тұрған ортада желінің көлемін ұлғайтуға арналған құрылғылар бар.

**Модем** – бұл компьютерлерге телефон желісі арқылы деректер алмасуға мүмкіндік беретін құрылғы.

Модем функциясы – тасымалдаушы модем цифрлық сигналды аналогқа модульдейді, ал қабылдағыш аналогты цифрлық етіп өзгертеді (1.10 сурет). Қосалқы (1.11 сурет) және сыртқы модем (1.12 сурет) бар. Өндірістік стандарт желілік технологияның барлық салалары үшін бар, модем де солардың бірі. Стандарттар әртүрлі өндірушілердің модемдерінің өзара әрекеттесуін қамтамасыз етеді. 1980 жылдардың басында Hayes Microcomputer Product, Inc. компаниясы Hayes Smartmodem деп аталатын модем жасады. Бұл стандартқа айналды, сол себепті басқа модемдер осы стандартқа бағыттала бастады. Бастапқыда модемнің жылдамдығы секундына немесе бірліктерде «бод» деп аталатын битпен өлшенді. Бод – бұл телефон желісі арқылы деректерді шығаратын дыбыстық толқынның тербеліс жиілігін білдіреді. Бұл бірлік өз атауын француз байланыс офицері Дж.Бодтың атына байланысты алды. 80-жылдардың басында бодтың берілу жылдамдығы модемдердің берілу жылдамдығына тең болды. Содан кейін байланыс инженерлері деректерді сығу және кодтау әдістерін жасады. Нәтижесінде әр дыбыстық модуляцияда бірнеше биттік ақпарат болуы мүмкін. Бұл бит жылдамдығы бод жылдамдығынан жоғары болуы мүмкін дегенді білдіреді.

Модемдердің әр түрлі түрлері бар, өйткені мәліметтерді берудің әртүрлі әдістерін қажет ететін әртүрлі беру ортасы түрлері бар. Бұл жерде орталарды байланыс синхрондалу критерийін ескере отырып, екі түрге бөлуге болады.

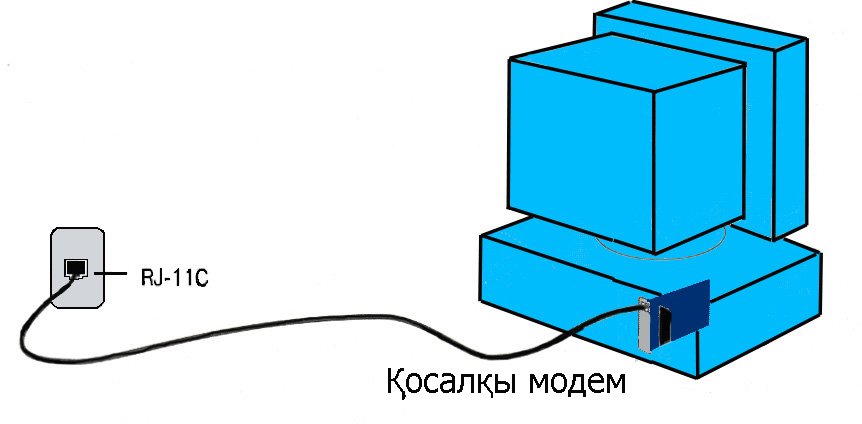


1.10 сурет. Модемдер сандық сигналдарды аналогқа және керісінше түрлендіру

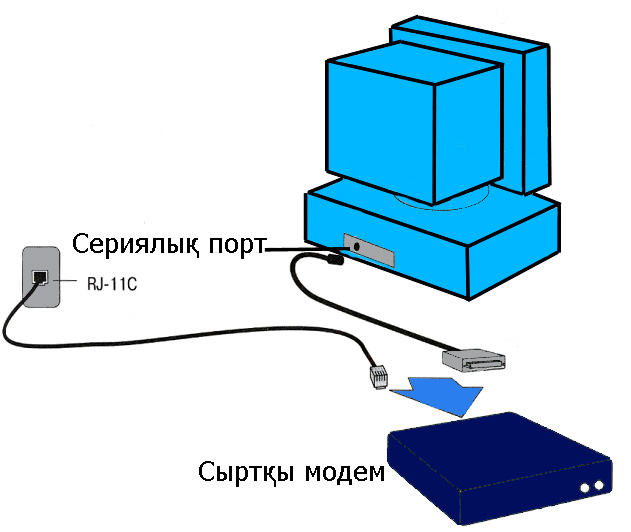
Асинхронды (тізбектей) модем стандартты телефон желілерінде қолданылатын асинхронды байланысты қолдайды. Әр таңба биттер қатарына бөлінеді. Бұл тізбектің әрқайсысы басқалардан басталу және тоқтату биттерімен бөлінген. Беруші және қабылдағыш құрылғылар іске қосу және тоқтату биттерінің комбинациясы туралы келісуі керек. Бұл түрдегі байланыс үндестірілмеген (синхрондалмаған), сондықтан синхрондау үшін арнайы құрылғы жоқ. Деректер жай беріліп, қабылданады, трафиктің 25% -ын басқаратын ақпарат құрайды (1.13 сурет).

Синхронды модем екі құрылғы арасында келісілген синхрондау сұлбасына негізделген. Оның мақсаты – биттерді кадр деп аталатын блогымен беру кезінде топтан оқшаулау. Беріліс бір кадрдың соңында аяқталады және келесі кадрдан басталады. Бұл әдіс асинхронды беріліске қарағанда тиімдірек.

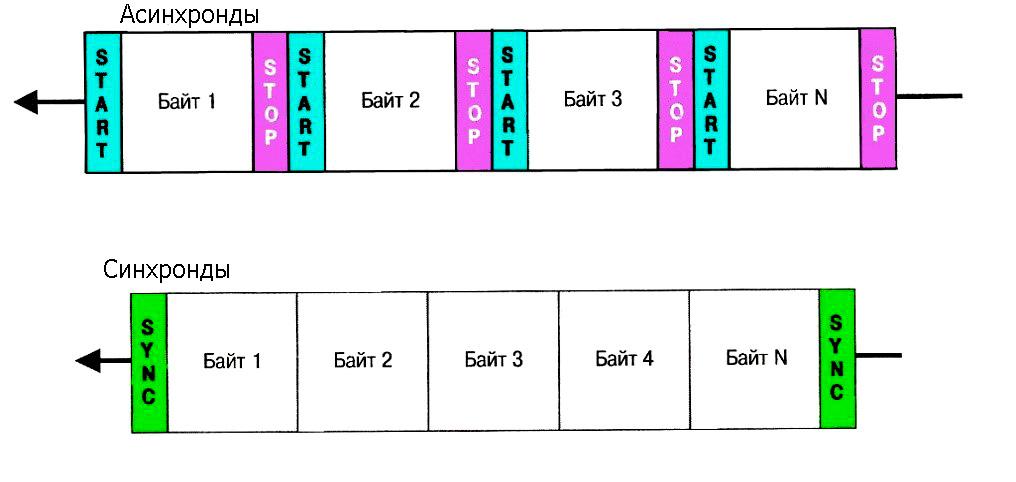
Бағасының қымбат болына және күрделілігіне байланысты синхронды модемдер арнайы үйде пайдалануға ұсынылмайды.



1.11 сурет – Кеңейту ұясына орнатылған қосалқы модем.



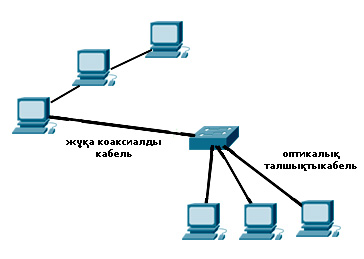
1.12 сурет – Сыртқы модем компьютердің сериялық портына қосылуы.



1.13 сурет – Асинхронды және синхронды деректер ағындары.

**Қайталауыш (репитер)** – электр сигналын күшейтетін құрылғы.

Репитер OSI моделінің физикалық деңгейінде жұмыс істейді, сигналды қалпына келтіреді және оны басқа сегменттерге жібереді. Репитерлер түрлендіру функцияларын және сүзгіден өткізу фукциясын орындамайды. Репитер жұмыс істеуі үшін оған қосылған екі сегментте бірдей қол жетімді әдісіне ие болуы керек. Бұл – желіні кеңейтудің ең арзан әдісі (1.14 сурет). Репитерлерді қолданатын себебіміз, желіні кеңейту кезінде сегменттің ұзындығы немесе түйіндер санына байланысты шектеулерді жоюға негізделген, сонымен қатар сегменттердің ешқайсысы жоғарылаған трафикті тудырмайды, ал құны басты фактор болып табылады.



1.14 сурет – Репиторлар әр түрлі тасымалдағыштарды қоса алады.

**Көпір** – сегменттерді немесе желілерді қосуға арналған құрылғы. Көпірдің міндеттері:



- желінің көлемін ұлғайту;

- желідегі компьютерлердің максималды санын көбейту;

- желілік қиындықтарды жою;

- желіге әр түрлі сегменттерін қосу;

- әр түрлі физикалық ортаны қосу.



Көпірлер OSI моделінің арналық деңгейінде жұмыс істейді, сондықтан олар осы модельдің жоғарғы деңгейлеріндегі ақпаратқа қол жеткізе алмайды. Көпірлер барлық хаттамаларды желіде жібереді, яғни бір хаттаманы келесі хаттамадан ерекшелігін ажыратпастан пайдалануға мүмкіндік береді. Кез келген хаттамалар көпірлер арқылы жұмыс істейтін болғандықтан, әр компьютер қандай Хаттамадармен жұмыс істейтіндігін анықтауы керек. Media Қолжетімді басқару деңгейіндегі көпірлер келесі әрекеттерді орындайды:

- барлық трафикті «тыңдайды»;

- әр пакеттің бастапқы және белгіленген мекен-жайларын тексереді;

- маршруттау кестесін құрастырады;

- пакеттерді береді.

Көпірдің жұмысы әрбір желілік түйіннің өз мекен-жайы болуы принципіне негізделген. Жұмыстың басында көпірдің маршрут кестесі бос болады. Содан кейін, түйіндер пакеттерді жіберген кезде бастапқы мекен-жай маршруттау кестесіне көшіріледі. Осы мәліметтермен көпір компьютерлердің желілік сегменттердегі орналасуын зерттейді.

Пакетті алғаннан кейін көпір маршруттау кестесіндегі бастапқы мекен-жайды іздейді.

Егер бастапқы мекен-жайы табылмаса, оны кестеге қосады. Содан кейін көпір белгіленген мекенжайларды маршруттау кестесінің деректер базасымен салыстырады.

Егер адресаттың адресі маршруттау кестесінде болса және белгіленген мекен-жаймен бастапқы қорек көзімен бірдей сегментте болса, пакет алынп тасталады. Бұл сүзу желілік трафикті азайтады және желі сегменттерін оқшаулайды.

Егер белгіленген мекен-жай маршруттау кестесінде болса, ал белгіленген мекен-жай мен қорек көзі әртүрлі сегменттерде болса, көпір пакетті тиісті порт арқылы белгіленген жерге жібереді. Егер алушының мекен-жайы маршруттау кестесінде болмаса, онда көпір пакет қабылданған жерді қоспағанда, пакетті өзінің барлық порттарына жібереді.

Егер сіз желіні кеңейту үшін көпірлерді қолданамын деп шешсеңіз, келесі ағдайларды ескеріңіз:

-көпірлер репитордың барлық мүмкіндіктеріне ие;

- екі сегментті жалғайды және сигналды пакеттік деңгейде қалпына келтіру;

- OSI модельдерінің арналық деңгейінде жұмыс жасай алады;

- тарату жылдамдығы 56 Кбит/с-тен кем таратылған желілер үшін жарамсыз;

- бір уақытта бірнеше маршрутты қолдана алмайды;

- барлық таратылатын хабарламаларды өткізіп жіберіді, бұл желінің толып кетуіне мүмкіндік береді;

- әр пакеттің бастапқы және белгіленген мекен-жайларын оқып шығады;

- алушының мекен-жайы белгісіз болса да пакеттерді жібереді;

Көпірлердің негізгі мақсаты:

- желі ұзындығын немесе ондағы түйіндердің санын көбейту үшін екі сегментті қосу;

- желіні сегменттеу есебінен трафикті азайту;

- әр түрлі желілерді қосу.



**Маршрутизатор** – бұл әр сегменттің мекен-жайын білетін, ең жақсы маршрутты анықтайтын және кеңінен таратылатын хабарламаларды сүзетін құрылғы. Ол OSI моделінің желілік деңгейінде жұмыс істейді. Бұл олардың бірнеше желілер арқылы пакеттердің мекен – жайларына бағыттауға және маршруттауға болатындығын білдіреді.



Маршрутизация кестесінде желілік мекен-жай көрсетілген. Желіде қолданылатын әрбір хаттама үшін өзінің жеке кестесі құрылады. Ол келесі ақпаратты қамтиды:

- барлық белгілі желілік мекен-жайлар;

- басқа желілермен байланыс әдістері;

- маршрутизаторлар арасындағы мүмкін болатын жолдар;

- осы жолдар бойынша деректерді беру құны.

Маршрутизатор әртүрлі нұсқалардың құны мен қол жетімділігін салыстыра отырып, мәліметтерүшін ең жақсы маршрутын таңдайды.

Маршрутизаторды екі негізгі түрге бөлінеді:

|  |  |
| --- | --- |
| Статикалық | Динамикалық |
| Барлық бағыттарды қолмен орнату және конфигурациялау | Бірінші маршрутты қолмен конфигурациялау. Қосымша желілер мен бағыттарды автоматты түрде анықтау |
| Әрдайым бағыттау кестесінің элементімен анықталған маршрутты қолдану | Олар желі трафигінің құны мен мөлшері сияқты факторларға негізделген маршрутты таңдай алады |
| Пайдаланылған маршрут қатаң берілген және әрқашан ең жақсы бола бермейді. | Таңдалған бағыт бойынша жөнелту туралы шешім қабылдауы мүмкін |
| Статикалық маршрутизаторлар неғұрлым қауіпсіз болып саналады, себебі әкімші өзі әр бағытты белгілейді | Динамикалық маршрутизаторды қорғау үшін оны қолмен конфигурациялау арқылы жақсартуға болады. Мақсаты – анықталған желі мекен-жайларын сүзу және олар арқылы деректердің берілуіне кедергі жасау |

Барлық Хаттамадар маршрутизаторлармен жұмыс істей бермейді. Маршрутизатормен жұмыс жасайтын хаттамалар бағытталған (маршрутталған) деп аталады. Оларға мыналар жатады: DECnet, IP, IPX, OSI, XNS. Бағытталмаған хаттамаларға мыналар кіреді: LAT, NetBEUI.

Маршрутизатор желіні «тыңдап», оның қандай бөліктері қатты жүктелгенін анықтай алады. Ол сонымен қатар, желі сегменттері арасындағы транзит санын анықтайды. Осы ақпаратты пайдалана отырып, маршрутизатор деректерді тасымалдау маршрутын таңдайды. Егер бір жол шамадан тыс жүктелсе, ол балама нұсқаны көрсетеді.

Көпірлер мен маршрутизаторлардың айырмашылығы – олар OSI моделінің әртүрлі деңгейлерінде жұмыс істейді. Маршрутизаторда көбірек ақпарат бар, ол мекен-жайды ғана емес, сонымен қатар хаттаманың түрін де таниды. Көпір желілер арасындағы бір жолды ғана тани алады. Қазіргі уақытта мүмкін болатын бірнеше жолдардың арасынан маршрутизатор ең жақсысын анықтайды.



**Шлюз** – әртүрлі Хаттамадарды қолдана отыра, ақпараттық желілерді біріктіруге арналған құрылғы. Шлюздер OSI моделінің қолданбалы деңгейінде жұмыс істейді.

Шлюздер әртүрлі архитектуралар мен орталардың арасындағы байланысты қамтамасыз етеді. Олар әр ортаның басқа ортадағы деректерді түсінуі үшін бір ортадан екіншіге берілетін деректерді қайта жинақтайды және түрлендіреді. Атап айтқанда, шлюз ақпараттарды тағайындау жүйесінің талаптарына сәйкес қайта өңдейді.



Хабарлама форматын қабылдаушы жақтағы бағдарлама деректерді тануы үшін өзгертеді. Мысалы, электрондық почта шлюздері хабарламаларды бір форматта қабылдап алады, ал оны таратуда және жіберуде басқа форматта болады.

Шлюз әр түрлі қолданылатын екі жүйені қосады:

- коммуникация (байланыс) хаттамаларын;

- мәліметтер құрылымы және форматтарын;

- тілдерді;

- сәулеттерді.

Шлюздер белгілі бір тапсырма түрін орындау үшін жасалады, яғни деректерді белгілі бір түрге түрлендіру үшін. Деректерді өңдей отырып, шлюз келесі операцияларды орындайды:

- кіріс пакеттерден мәліметтерді шығарады, оларды таратушы желіден Хаттамадың толық жинағымен төменнен жоғарыға өткізеді;

- алынған деректерді қайта жинақтайды, оларды белгіленген желінің Хаттама жиынтығы арқылы жоғарыдан төмен қарай жібереді.

Әдетте, желідегі шлюздердің рөлін арнайы серверлер орындайды, сондықтан бұл желіні кеңейту үшін қымбат құрылғы болып саналады.

Осы бөлімде қарастырылған құраушылар (компоненттер) жергілікті және ғаламдық желілерде қолданылады, олардың ішінен сіз өзіңіздің желіңіздің көлемін және өнімділігін арттыру үшін ең қолайлы желіні таңдауыңыз керек.

Тексеру жұмыс №2



**№2 жаттығу Сөйлемді аяқтаңыз:**

А бағанынан сөйлемнің басын В бағанынан ең қолайлы деген сөйлемнің соңымен салыстырыңыз. Дұрыс нұсқасын таңдап, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір сөйлемнің соңын тек бір рет пайдалануға болады.

**Баған А**

1. Token Ring \_\_\_\_\_\_
2. 100Base X\_\_\_\_\_\_\_
3. Шлюздер \_\_\_\_\_\_\_\_\_
4. Көпірлер \_\_\_\_\_\_
5. Маршрутизаторлар \_
6. Хабтар \_\_\_
7. 10BaseТ \_\_\_\_\_

**В бағаны**

A. Таратылатын хабарлардың көп болуын болдырмайды және желі деңгейінде жұмыс жасайды

B. UTP негізінде жұлдыз-шина топологиясын қолданады

B. Әр түрлі хаттамаларды қолданатын желілерді қосады

G. Жұлдыз-сақина топологиясын және маркер беруді қолданады

Д. Көппорттық репитер (қайталаушы) ретінде жұмыс жасады

E. стандартты Ethernet ретінде белгілі

G. Сандық локальды қосылуды қамтамасыз ететін байланыстыратын қызмет

Пакеттік бағыттау қол жетімділікті басқару ортасының қосалқы деңгейына негізделген

**№2 жаттығу Дұрыс жауапты таңдаңыз**

* Әдетте, Ethernet тар жолақты беріліс пен топологияны пайдаланады.

а) жұлдыз

б) шина

в) сақина

г) жұлдызды-сақина

2. Негізгі кабельдік сегменттенде трафикті реттеу үшін Ethernet қол жетімді ортаның қандай әдісін қолданылады?

а) маркер беру көмегімен

б) CSMA/CA

в) СSMA/CD

г) басымдық беру

3. Token Ring желілері маркермен не арқарады?

а) биттердің алдын-ала анықталған реттілігі

б) аналогтық сигнал

в) мәліметтер

г) алушының мекен-жайы

4. Ақаулы компьютер немесе қосылысы бүкіл Token Ring желісінің жұмысына қалай әсер етеді?

а) желіде үзіліс болады

б) маркердің қозғалысын және бүкіл желінің жұмысын тоқтатады

в) компьютер автоматты түрде сақинадан шығарылады

г) ақаулы компьютер желілік сақинадан қолмен ажыратылады

5. AppleTalk желілерін бір үлкен желіге қалай қосуға болады?

а) қайталағышты қолдану

б) қалаған аймақты таңдау арқылы

в) серверлік компьютерді қолдану арқылы

г) желілік адаптерді қолдану арқылы

6. ArcNet желісі жұлдызды-шина топологиясына ие, сондықтан қол жетімді әдісін қолданады:

а) CSMA / CD

б) CSMA / CA

в) маркер берумен

г) сауалнама

7. Модемнің өнімділігін қалай арттыруға болады?

а) деректерді беру жылдамдығын арттыру

б) телефон желісінің өткізу қабілетін арттыру

в) синхронды байланысты пайдалану

г) деректерді сығу және кодтау әдістерін қолдану

8. Репеорлар:

а) Физикалық деңгейдегі функцияланады

б) деректерді сүзгілеу

в) әртүрлі тасымалдағыштардың пайдаланатын сегменттерді жалғау

г) екі бағытта да трафик жаңалғын өткізу

9. Көпірлерге көбірек қолданылатын мәлімдемені таңдаңыз:

а) бір уақытта бірнеше маршрутты қолданады

б) желі сегментациясына байланысты трафикті азайту

в) таратылатын хабарламаларды өткізбей, оларды сүзгіден өткізу

г) белгісіз мекенжайлары бар пакеттерді өткізбейді

10. Маршрутизаторлар келесі функцияларды орындай алады:

а) желіні қосып, пакеттік пакеттерді сүзгіден өткізу

б) қол жеткізуді басқарудың қосалқы деңгейгерінің мекен-жайларын тану

в) белгісіз мекен-жайы бар пакеттерді барлық бағытта тарату

г) желі деңгейінде және кез-келген желілік Хаттамадармен жұмыс істеу

**№3 жаттығу Мәлімдемені растаңыз немесе жоққа шығарыңыз**

Келесі сөйлемдерден Иә немесе Жоқ таңдаңыз.

1. Тез беріліске қол жеткізу үшін Token Ring желісіндегі барлық компьютерлерге бір адрес берілуі керек. Иә. Жоқ.

2. Көлемі, дизайны және деректерді беру жылдамдығы әртүрлі болғандықтан, жұқа және қалың Ethernet кабельдерін бір желіде пайдалануға болмайды. Иә. Жоқ.

3. 100Base VG желісінде жұлдыздар топологиясы қолданылады, барлық компьютерлер концентратормен қосылған. Иә. Жоқ.

4. Бөлгіш пакетте бастапқы адресті көрсетеді. Иә. Жоқ.

5. Сақина толған кезде, желіні басқа MAU қосу арқылы кеңейтуге болады. Иә. Жоқ.

6. Әдетте Ethernet кең жолақты және шина топологиясын пайдаланады. Иә. Жоқ.

7. Жұқа Ethernet желісі төрт репитермен (қайталағышпен) қосылған 8 кабельдік сегменттерден тұруы мүмкін, бірақ жұмыс станцияларын тек үш сегментке қосуға болады. Иә. Жоқ.

8. Token Ring кадрында қол жетімділікті басқару өрісі маркер кадры немесе деректер кадры берілетінін білдіреді. Иә. Жоқ.

9. Телефон байланысында қолданылатын аналогты желілер (стандартты дауыс арналары) байланыстырушы желілері деп те аталады. Иә. Жоқ.

10. Бағыттау кестесі жеке адрестерге жіберілетін хабарларды қолдайды. Иә. Жоқ.

11. Көпірлер мен маршрутизаторлардың ең маңызды айырмашылығы - маршрутизаторлар көптеген маршруттардың ішінен таңдай алу. Иә. Жоқ.

12. Дауыстық байланыстырушы телефон желілері компьютерлерге қол жетімді болу үшін синхронды модемдерді қолданады. Иә. Жоқ.

**№4 Қолданбалы тапсырмалар**

1. Желіні жоспарлау. Оңтайлы желілік қондырғы мен құраушы таңдаңыз:

a) Ethernet 10BaseT желісіне жұқа коаксиалды кабельмен сегментті қосу керек

б) Интернетке жеке байланыс қажет

в) бірнеше сегменттер арасындағы трафикті оқшаулау және сүзу қажет г) әртүрлі желілік архитектурамен сегменттерді қосу қажет

д) әр түрлі жерде орналасқан пайдаланушылармен файлдарды уақытында алмастыру қажет

е) әр түрлі жүйелер арасында байланыс қажет (Microsoft-тың Novell-ге қол жетімді болуыі)

## 1.3. TCP/IP хаттаманының стегі

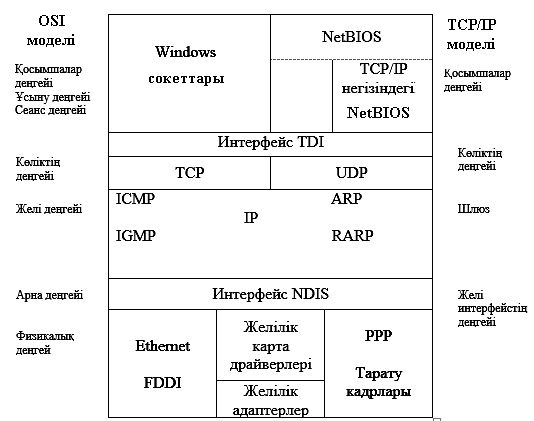
1.3.1 ТСР/IP хаттамасы

Transmission Control Protocol/ Internet Protocol (TCP/IP) – бұл гетерогенді (біртекті емес) ортада байланысты қамтамасыз ететін хаттамалардың өнеркәсіптік жиынтығы, яғни әр түрлі типтегі компьютерлердің үйлесімділігін қамтамасыз етеді. TCP/IP-дің үйлесімділігі оның басты артықшылықтарының бірі, сондықтан көптеген жергілікті желілер оны қолдайды. Сонымен қатар, TCP/IP интернет-ресурстарға қол жеткізуді қамтамасыз етеді, сондай-ақ кәсіпорындардағы желілер үшін бағытталған хаттаманы ұсынады. TCP/IP маршрутизацияны (бағытталуды) қолдайтындықтан, әдетте, оны желіаралық хаттама ретінде қолданылады. TCP/IP танымал болуына байланысты өзара желіаралық әрекеттесудің стандартына айналды. TCP/IP ашық жүйеге негізделген және жүйенің архитектурасы OSI сәйкес келеді.

Microsoft фирмасының TCP/IP жүзеге асыруда төрт деңгейлі модельге ие. 1.15 сурет).

IP хаттамасы желіаралық деңгейде болады және дейтграмма деп аталатын деректер блогын жіберушіден алушыға беру мүмкіндігін қамтамасыз етеді. IP хаттамасы – сенімсіз, байланыс орнатылмаған хаттама, яғни. IP деректердің жеткізілуін растамайды, алынған деректердің тұтастығын бақыламайды және қызметтік ақпаратпен қамтамасыз етілмейді.

IP хаттамасы әр дейтграмманы тәуелсіз бірлік ретінде қарастырады. IP негізгі міндеті – бұл дейтграммаларды бағыттау (деректер торабының түйіннен түйінге бағытын анықтау).



1.15 сурет – Microsoft фирмасының TCP/IP жүзеге асыруда төрт деңгейлі TCP/IP моделінің OSI моделімен сәйкес болуы



**Желінің түйіні** – IP хаттамасын қолдайтын желіге қосылған компьютер. Ол бір немесе бірнеше IP интерфейске ие, әр интерфейсте ерекше IP мекен-жайы болады.

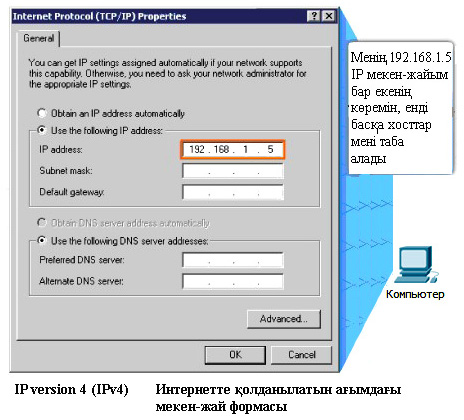
**IP мекенжай –** бұл Интернетте IP интерфейсінің 32 биттік бірегей идентификатор. IP мекенжайы, әдетте, нүктелермен бөлінген ондық сан түрінде октет түрінде жазылады.

**IP мекенжайының форматтары**

|  |  |
| --- | --- |
| Екілік | Ондық |
| 10100000.01010001.00000101.10000011 | 160.81.5.131 |



Интернетте әр IP мекен-жайы немесе оның желісі 1000 немесе 1 000 000 түйіннен тұратындығына қарамастан бірегей болуы керек. Егер сіздің компанияңыздың желісі TCP/IP пайдалануға қалыптасқан болса және Интернетке қосылмаған болса, онда IP мекенжай кеңістігінен қайталанбайтын мекен-жайларды белгілеу және пайдалану үлкен мәселе емес. Сіз бүкіл мекенжай кеңістігінен сіздің қажеттіліктеріңізге сәйкес мекенжайларды таңдай аласыз. Алайда, егер сіздің ұйымыңыздың желісі Интернетке қосылуы керек болса, бұл IP мекенжайды сізден басқа ешкім пайдаланбайтынына көз жеткізу әлдеқайда қиын болады.



InterNIC (Internet Information Centre Интернеттің ақпарат орталығы) интернеттегі мекен-жайларды таратуға және меншіктеуге жауап береді. Интернеттегі барлық желілік мекен-жайларды тағайындауға (меншіктеуге) тек бір топ жауапты болғандықтан, мекенжайлардың қайталанбауын қамтамасыз ету жеткілікті. Алайда, InterNIC интернеттегі барлық мекенжайларды қадағаламайды. Оның орнына, ол сізге берілген қосалқы желіде түйіндердің қажетті санын құруға мүмкіндік беретін желі идентификаторын ұсынады. Ұйым түйіндер идентификаторларын өзінің қосалқы желісіне сәйкес етіп орната алады.



***IP-адрес кластары***

1. А класы

А класы желі идентификаторы үшін тек бірінші октетті және түйін идентификаторы үшін қалған үш октетті пайдаланады. Осы класс мекен-жайының бірінші сегіздігінің (үлкен бит) бөлігі әрқашан нөлге тең болады, бұл сізге А класының адресі екенін анықтауға мүмкіндік береді.

|  |
| --- |
| 0 |
| 0-127 | | Х | Х | Х |
| желі | | түйін | | |

Желілік бөліктің өлшемі - 8 бит, сондықтан А класының 27-1 адресін алуға болады және әр желінің 224-2 мекен-жай кеңістігі болады. Мекенжайлардың бұл класы желідегі түйіндердің осындай көп санын пайдалануға мүмкіндік беретіндіктен, бұл мекенжайлар тек көптеген түйіндерге қол жеткізуді қамтамасыз етуді қажет ететін ұйымдарға ғана беріледі. Шындығында, бұл мекен-жайлардың көпшілігі, кейбіреулері болмаса, көптеген жылдар бұрын қандай да бір ұйымдарға, әдетте әскери немесе университеттерге бөлінген болатын.

2. В класы

В класы желі идентификаторы үшін алғашқы екі октетті және түйін идентификаторы үшін қалған екі октетті қолданады. Осы кластың мекен-жайының бірінші сегіздігінің екі жоғары дәрежелі биттері әрқашан 10 болады, бұл бізге В класының адресі екенін анықтауға мүмкіндік береді. Желі бөлігінің өлшемі – 14 бит, сондықтан В класын 214 мекен-жаймен қарастыруға болады және әрбір желінің 216-2 мекен-жай кеңістігі болады. Бұл мекенжайлар класы орта немесе үлкен желілерге арналған, оларды алу оңай болмаса да, кейбір мекен-жайлар әлі де болса, қол жетімді.

|  |
| --- |
| 10 |
| 128-191 | | N | Х | Х |
| желі | | | түйін | |

1. . С класы

С класы желі идентификаторы үшін алғашқы үш октетті, ал түйін идентификаторы үшін қалған октетті қолданады. Осы кластың мекен-жайының бірінші сегіздігінің жоғары дәрежелі үш биттері әрқашан 110 тең болады, бұл С класының адресі екенін анықтауға мүмкіндік береді. Желі бөлігінің өлшемі – 21 бит, сондықтан C класын мына 221  мекен-жаймен бағыттауға болады және әр желіде 28-2 мекен-жай кеңістік болуы мүмкін. Бұл мекен-жайлар класы түйіндердің шектеулі санын ұстап тұруды қажет ететін шағын желілерге арналған.

|  |
| --- |
| 110 |
| 192-223 | | N | N | Х |
| желі | | | | түйін |

4. D класы

D класы хабар тарату үшін қолданылады, осы класстың мекен-жайының бірінші октетінің ең маңызды биттері әрқашан 1110-ға тең болады, бұл осы D класты мекен-жайдың барын анықтауға мүмкіндік береді.

|  |
| --- |
| 1110 |
| 224> | | Х | Х | Х |
| желі | | Түйіндердің логикалық тобы | | |

1. Е класы

Е класы – болашақта пайдалану үшін сақталған тәжірибелік мекен-жай класы. Осы кластағы мекен-жайлар белгіленген 1111-ге тең жоғары дәрежелі биттермен анықталады.

|  |
| --- |
| 1111 |
| 240> | | Х | Х | Х |
| желі | |  | | |



1 кестесінде мекен-жай кластары, мекен-жайдың ең маңызды (үлкен) биттерінің мәні, осы кластағы бірінші октеттің ондық мәндерінің диапазоны және осы класта қолдау көрсетілетін желілер мен түйіндердің саны көрсетілген. Емтиханда IP-мекен-жай класын, желілер санын және осы класстағы түйіндердің санын бір қарағанда анықтай алуөте құнды болып саналады.

**1 кесте - IP мекенжай кластары**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Класстар | 1-октет | 1 октет биттері | Мекенжайлардың желілік (N) және түйіндік (N) бөлігі | Маска | Желілер мен түйіндердің мүмкін болатын саны |
| А | 1 – 127\* | 00000000 –  01111111 | N.H.H.H | 255.0.0.0 | 128 желілер ()  16,777,214 түйіндер (-2) |
| B | 128-191 | 10000000 –  10111111 | N.N.H.H | 255.255.0.0 | 16,384 желілер ()  65,534 түйіндер (-2) |
| С | 192-223 | 11000000 –  11011111 | N.N.N.H | 255.255.255.0 | 2,097,150 желілер ()  254 түйіндер (-2) |
| D | 224-239 | 11100000 –  11101111 | NA (multicast) |  |  |
| E | 240-255 | 11110000 –  11111111 | NA (experimental) |  |  |

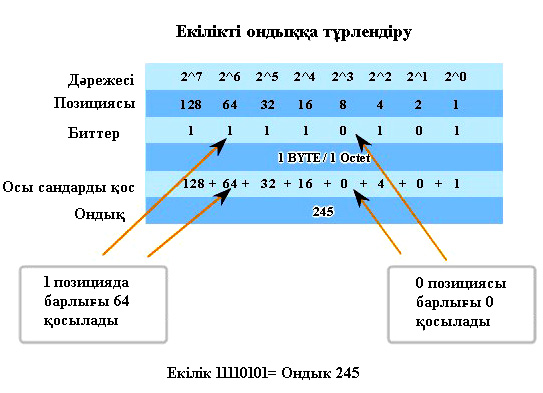
IP мекенжайын таңдау ережелері

1. Болашаққа жоспар құрыңыз. Бірінші және маңыздысы: сіздің желіңіздің одан әрі дамуына мүмкіндік беретін класты таңдаңыз.
2. Бірегейлікті қамтамасыз етіңіз. Маршрутизаторға қосылған желіңіздің әр сегментінде жеке желі идентификаторы болуы керек.
3. Тұтынуға қойылған мекенжайларды пайдаланбаңыз. Кейбір мекенжайлар IP мекен-жайы ретінде Интернетте әдеттегідей пайдалануға келмейді. Мысалы, А класындағы 127 желілік мекен-жайы диагностикалық мақсаттар үшін тұтынуға қойылған. Тұтынуға қойылған мекенжайлардың тізімін http // ds.internic.net мекен-жайы бойынша Халықаралық веб-сайттан табуға болады.

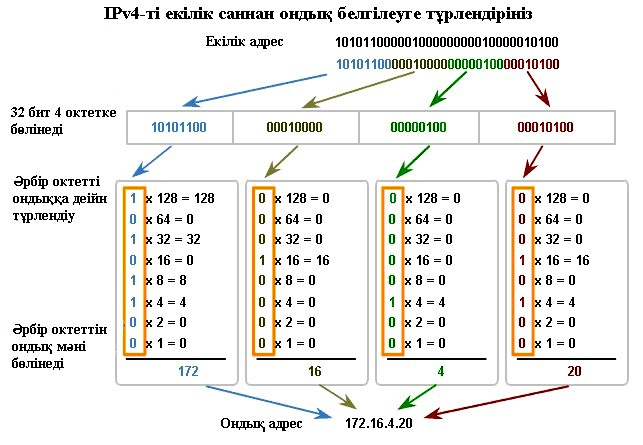
4. Сіз 0 (барлық нөлдердің октеті) және 255 (барлық бірліктегі октет) сандарын IP мекенжайы ретінде пайдалана алмайсыз.

5.

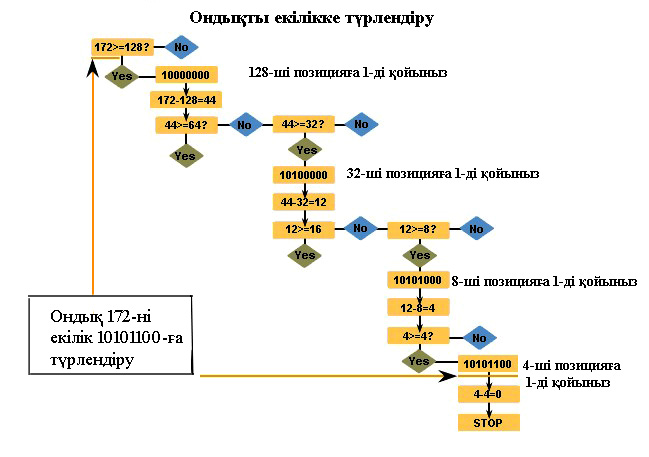
0 позициясы барлығы 0 қосылады



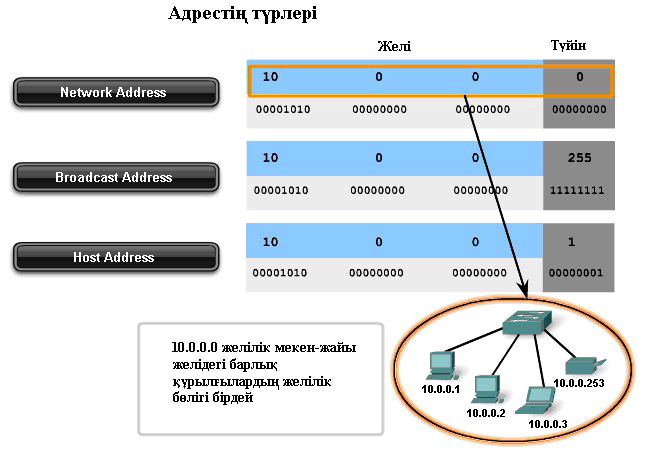
6.



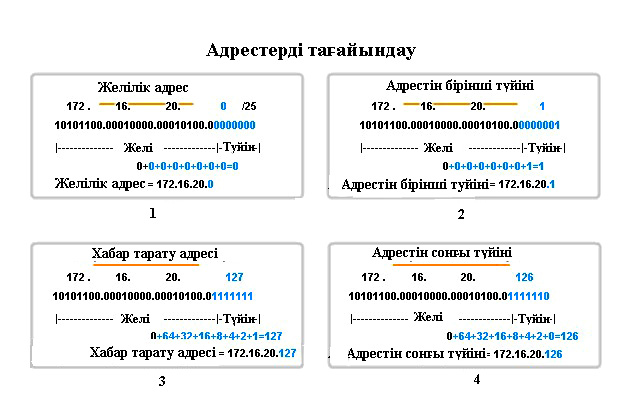
7.



8.



9.



***Класссыз модель***

Қол жетімді мекен-жай кеңістігін тиімді пайдалану қажеттілігі жаңа классыз доменаралық маршрутизация Classless Domain Routing (CIDR) IP мекен-жай кеңістігі сұлбасын құруға алып келді.

Интернетке қосылған жергілікті желіде 2000 компьютер бар делік. Мекенжай кеңістігін қосу үшін сізге 8 класты С немесе В класының бір мекен-жайы керек, бірақ В 65534 түйінге ие – бұл сізге қажет болғаннан әлдеқайда көп (бұл ысырап). Алайда, егер сіз 8 класты С мекенжайын қолдансаңыз, онда осы желілерді қосу кезінде қызметтік ақпаратпен трафиктің шамадан тыс жүктелуі мәселесі туындайды.

Екінші жағынан, біз 32-ді 21-ге және 11-ге бөлуге болады, себебі 211=2046 мекен-жайы, сондықтан 21 биттік мекен-жайы бар бір желі болады және оның қызмет етуі үшін маршрут кестесінде бір ғана жазба қажет болады. Мекенжай кеңістігін бөлу процесін жеңілдету үшін қосалқы желі маскалары қарастырылған.

**Қосалқы желі дегеніміз** – түйін идентификаторынан тұратын IP мекен-жайының бөлігінен желілік идентификаторы бар бөлікке бірнеше битті беру арқылы құрылған желі немесе желінің идентификаторы.

**Қосалқы** **желі маскасы** – бұл 32биттік мекен-жай, бұл желі идентификаторы үшін мекен-жайларда қанша бит қолданылатындығын анықтауға мүмкіндік береді.

Желілік маска келесі ережеге сәйкес жасалады***:***

1) желінің нөміріне сәйкесінше биттер орнатылады (1).

2) түйін нөміріне сәйкесінше биттер қалпына келтіріледі (0).

Жазудың қарапайымдылығы үшін CIDR үлгісіндегі IP мекен-жайлар келесідей түрде ұсынылады: a.b.c.d./n, мұндағы a.b.c.d – IP мекен-жайы; n - желі бөлігіндегі биттердің саны. Мысалы. 137.158.128.0/17 IP мекенжайы берілген, сондықтан қосалқы желі маскасында 17 бірлік (желі идентификаторы) және 15 нөл (түйін идентификаторы) бар және ол 255.255.128.0 тең.

Егер IP-мекен-жайы белгілі болса, онда қосалқы желіден түйін нөмірін қалай табуға болады? Мысал. 205.37.193.134 C класының IP адресі берілсін – түйін нөмірі – 134. Енді желіні қосалқы желіге 205.37.193.134/26 бөліңіз. Бұл жағдайда түйін адресі қандай?

|  |  |  |  |
| --- | --- | --- | --- |
|  | IP адрес | Желі идентификаторы | Түйін идентификаторы |
| Бастапқы түйіннің IP мекенжайы | 205.37.193.134 | 11001101.00100101.11000111. | 10000110 |
| қосалқы желі маскасы | 255.255.255.192 | 11111111.11111111.11111111.11 | 000000 |
| Логикалық ЖӘНЕ элементінің нәтижесі | 205.37.193.128 | 11001101.00100101.11000111.10 | 000110 |

Нәтижесінде қосалқы желінің IP-адресі 205.37.193.128, ал қосалқы желідегі түйін нөмірі – 6.

Әдеттегі маскалар:

- А класы 255.0.0.0;

- В класы 255.255.0.0;

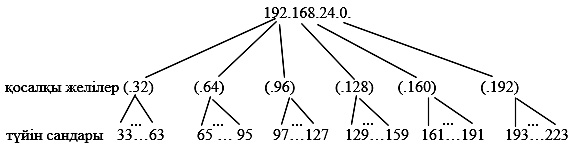
- С класы 255.255.255.0.



*1 жаттығу*. 255.255.240.0 маскасы бар 132.90.132.5 IP адресі 132.90.128.0/20 желідегі 4.5 Түйін нөмірін анықтайтындығын көрсетіңіз.

Қосалқы желілерді адресациялау мысалы.

NIC сізге 192.168.24.0 IP мекенжайын берсін. Сізде үш желі бар. Қосалқы желіге бөлу үшін қандай масканы қолдану керек. 255.255.255.224 маскасы ұсынылады, өйткені бұл жағдайда желілік идентификатор бөлігінде үш блок болады, сондықтан 23-2 = 6 қосалқы желілерге және 25-2 = 30 қосалқы желілерге жүгінуге болады.



Сонымен, қосалқы желіні бөлу келесілер үшін қажет:

- желінің қуатының физикалық шектеулерінен басым болу (желінің архитектуралары желідегі түйіндердің санына шектеулерге ие);

- түйіндерді қосудың әртүрлі әдістерін қолдану (әртүрлі сәулеттері бар желілерді маршрутизатор көмегімен қосуға болады);

Желіні қосалқы желілерге бөлу кезеңдері:

1) Желілік идентификаторлардың жалпы қажетті санын анықтаңыз. Желінің одан әрі дамыту туралы ойлануды ұмытпаңыз.

2) Әрбір қосалқы желі ұстап тұру қажет болатын түйіндер идентификаторларының жалпы санын анықтаңыз. Тағы да, болашақта жаңа түйіндер желіге қосылуы мүмкін екенін ұмытпаңыз.

3) қосалқы желідегі желі идентификаторлары мен түйіндерінің қажетті санын ұстап тұруға мүмкіндік беретін қосалқы желі маскасын анықтаңыз.

4) Қандай желі идентификаторлары қолданылатындығын шешіңіз.

5) Қосалқы желілердегі түйіндерге идентификаторларды белгілеңіз.

*2 жаттығу.* D түйіні 202.12.74.37 IP мекенжайы және 255.255.255.224 қосалқы желі маскасына ие. Түйін D 202.121.74.66 IP мекен-жайы бар Ж түйініне ақпаратты және 255.255.255.224 маскасын жіберуі керек. Д және Ж түйіндерінің бірдей қосалқы желіде екенін және ақпараттың қалай берілетінін анықтаңыз.

*3 жаттығу*. Сіз В класының IP-адресін 128.131.0.0 алған компанияда жұмыс жасайсыз. Қазіргі уақытта 45 жеке желі сегменті бар. Тағы 50 қосалқы желіні енгізу жоспарлануда. Түйіндердің максималды санын ұстап тұру үшін қандай масканы қолдану керек?

*4 жаттығу*. Компания 9 бөлімнен тұрады және 130.121.0.0 IP адресін алды. Бөлмде 3000 түйінді ұста тұруы қажет. Қандай масканы таңдау керек?



**2 БӨЛІМ**

# Коммутация және маршрутизация

## 2.1. IP маршрутизация (бағыттау)

**Бағыттау** – Бұл түйіндерден мекен-жайға деректерді немесе аралық маршрутизаторға беру процесі.

Бағыттау маршрут кестелерге негізделеді, бұл сегменттердің IP мекенжайлары мен маршрутизатор интерфейстерінің IP мекенжайлары арасындағы сәйкестікті сақтайтын мәліметтер базасы. Деректер кандай да бір түйінтан шыққан кезде, маршрутизатор маршрут кестесін тексереді. Егер белгіленген түйін-мекен-жай (немесе оның желілік сегменті) кестеде көрсетілмеген болса, онда деректер әдеттегі мекен-жайға жіберіледі. Егер белгіленген түйін-мекен-жай табылса, деректер белгіленген жерге жіберіледі. Егер белгіленген түйін-мекен-жай табылмаса, жіберуші түйін-жіберушіге қате туралы хабарлама жіберіледі.

Бағыттау процесінің мысалы (2.1 сурет).

Бағыттау кестесінің екі түрі бар: статикалық және динамикалық. Жүйе әкімшілері статикалық бағыттау кестелерін қолмен құрып, жаңартып отыруы керек, себебі кестелерді белгілі бір араласу болмаса өзгерту мүмкін емес. Бағыттаудың динамикалық кестелері бағыттау хаттамасының көмегімен автоматты түрде құрылады.



2.1 сурет – Қарапайым бағыттау

**Статикалық бағыттау**

Статикалық бағыттау – бұл орнатылған IP мүмкіндігі (функциясы) және жұмыс істеу үшін ешқандай қосымша қызметтер қажет етпейді. Статикалық бағыттау кестесі әр маршрутизаторда қолмен жасалуы және сақталуы керек. Статикалық бағыттау кестесі желілер мен оларға кіруге арналған шлюз немесе маршрутизатордың интерфейстерін анықтайды. Статикалық бағыттау кестесі төмендегілерден тұрады:

- Желі мекенжайы. Әр белгілі желінің мекен-жайы, жергілікті мекен-жайы (0.0.0.0) және тарату мекен-жайы (255.255.255.255).

- Желілік маска. Әр желі үшін қолданылатын қосалқы желі маскасы.

- Шлюз мекен-жайы. IP- әр желі үшін кіру нүктесінің адресі (маршрутизатор интерфейсі).

- Интерфейс. Желілік интерфейске белгіленген IP.

- Метрика. Желіге қосылатын қайта беру саны («хоп»).

2 кестесінде бағыттау кестесінің мысалы келтірілген.

2 кесте бағыттау кестесі

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Желі | Маска | Метрика | Интерфейс | Шлюз |
| 0.0.0.0 | 0.0.0.0 | 1 | 10.57.11.169 | 10.57.8.2 |
| 127.0.0.0 | 255.0.0.0 | 1 | 127.0.0.1 | 127.0.0.1 |
| 10.57.8.0 | 255.255.248.0 | 1 | 10.57.11.169 | 10.57.11.169 |
| 10.57.11.169 | 255.255.255.255 | 1 | 127.0.0.1 | 127.0.0.1 |
| 10.57.255.255 | 255.255.255.255 | 1 | 10.57.11.169 | 10.57.11.169 |
| 224.0.0.0 | 224.0.0.0 | 1 | 10.57.11.169 | 10.57.11.169 |

Статикалық маршрутизатор тек маршруттау кестесіне қосылған желілермен байланыс жасай алады.



**Route** пәрмені – бұл статикалық бағыттау кестелерін құру немесе өзгерту үшін қолданылатын TCP/IP утилитасы. Бұл пәрмен келесі синтаксиске ие:

**route** [-f] [-p] [пәрмен [менкен-жай] [маска] [шлюз] [метрика]]

Параметрлер келесі мағыналарға ие:

-f – шлюздер үшін барлық жазбаларды жою. Егер бұл параметр басқалармен бірге қолданылса, онда алдымен шлюздер үшін жазбалар жойылады;

-p – тұрақты жазбалар қосу (қосу пәрменімен). Әдетегідей, жүйе қайта іске қосылған кезде қосылған жазбалар сақталмайды. Барлық тұрақты жолдарды print (басып шығару) пәрменінің көмегімен көрсетуге болады.

-команда – төрт команданың бірін көрсетуге болады: print (жолдарды тізімдеу), add (жолды қосу), delete (жолды жою), change (бар жолды өзгерту);

-мекен-жай белгілеу – көрсетілген пәрменді жіберу керек компьютерді анықтайды;

-маска – көрсетілген жол үшін қосалқы желі маскасын анықтайды. Әдетте, мәні - 255.255.255.255 тең;

-шлюз – көрсетілген жол үшін шлюз;

- метрика – көрсетілген мәнге бағыттау кестесіндегі метрикалық өрісті орнату. 1-ден 9999-ға дейінгі кез келген мәнді көрсетуге болады.

**Тracert** **командасы** – бұл маршруттық тексеруді және пакеттік транзит уақыттарын өлшеу үшін пәрмен жолынан пайдаланылатын TCP/IP утилитасы. Бұл пәрмен келесі синтаксиске ие:

tracert [-d] [-h ретрансляция\_саны] [- j жүйелер\_тізімі] [- w таум\_аут] жүйе\_аты

Параметрлер келесі мағыналарға ие:

* d – IP мекен-жайын жүйелік атауларға аудармайды;
* h – ретрансляция саны – жүйені іздеген кезде ретрансляцияның (хоп) ең көп рұқсат етілген саны («хоп»);
* j – жүйелер\_тізімі – көрсетілген тізімдегі жүйелер арасынан еркін таңдау;
* w – таим\_аут – әрбір жауаптың көрсетілген миллисекунд санын күту;
* жүйелердің\_аты – ізделетін жүйенің атауы.

Tracert – жолды тексерудің тамаша тәсілі. Сондай-ақ, оны жолдардың жылдамдығын анықтау үшін пайдалануға болады.

**Динамикалық бағыттау**

Динамикалық маршрутизация күрделі архитектурасы бар үлкен желілерде статикалық маршруттауды қарағанда ыңғайлы, өйткені ол көптеген бағыттау кестелерін қолмен ұстап тұруды қажет етпейтін мүмкіндікке ие. Динамикалық бағыттау кезінде желі әкімшісінде жүктеме аз болады және көбінесе әр маршрутизатор үшін шлюздің көрсетумен шектеледі. Бағыттау кестесінің құрылуы мен барлық басқа келтірулер маршруттау хаттамасының көмегімен автоматты түрде жүзеге асады.

2.1.1 Бағыттау хаттамалары

Әртүрлі бағыттау хаттамалары бірнеше ондаған жылдардан бері белгілі екі қарапайым алгоритмге негізделген:

- қашықтық векторының алгоритмдері (Distance vector protocols);

- арна күйінің хаттамасы (Link state protocol);

Негізгі функциясын орындау үшін – трафиктің ауысп-қосылуы – әр маршрутизатор белгілі бір уақытта желі топологиясын көрсететін кестені пайдаланады.

Бағыттау хаттамасының функциялары:

- бағыттау кестесін ұстап тұру

- желілік топология және оның өзгерістері туралы ақпаратты уақтылы тарату.

Хаттамаларда сипатталған:

- желіні өзгерту туралы хабарламалар қалай жіберіледі

- өзгертулерде желілік топология туралы қандай ақпарат бар

- желілік ақпарат қаншалықты жиі жіберіледі

- желідегі өзгерістер туралы алушылардың орналасқан жерін қалай анықтауға болады.

TCP/IP бағыттауы үшін жиі қолданылатын екі хаттама: RIP (Routing Information Protocol, бағыттауды басқару хаттамасы) және OSPF (Open Shortest Path First) алдымен ең қысқа жолды ашу. Осы екі хаттама маршрутизация кестелерін жаңарту кезінде желілік трафикті жасайды, бірақ RIP – OSPF-пен салыстырғанда анағұрлым көп сөйлесетін хаттама (ол барлық бағыттау кестелерін желі арқылы жүйелі түрде жібереді, ал OSPF желідегі кесте өзгерістерін ғана жібереді).

**Қашықтық векторлық алгоритмдер**

Қашықтық векторлық хаттамалар (distance vector protocols) келесі жағдайларда қолданылады:

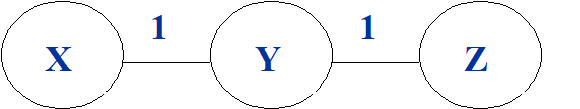
- **RIP** (Routing Information Protocol).;

- **IGRP** (Interior Gateway Routing Protocol).;

- **EIGRP** (Enhanced Interior Gateway Routing Protocol);

Қашықтық векторын пайдалану кезінде барлық «көршілерге» бағыттаудың толық кестесі жіберіледі, яғни түйіндердің шектеулі санына көптеген ақпарат жіберіледі. Әдістің мәні – пакет арқылы өтетін түйіндердің санын азайту болып табылады. Бұл қарапайым және аз жадты қажет етеді. Орнату кезінде барлық көршілерді және олардың әрқайсысына арналардың «құнын» көрсету керек. Беллман-Форд алгоритмдері деп те аталатын векторлық алгоритмдер баяу жинақталады және «шексіздікке кету мәселесіне» ұшырайды.

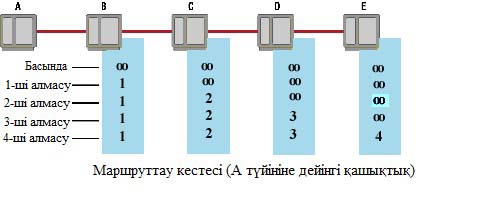
Мысал: X, Y және Z үш түйіндері 1 тұратын арналар арқылы қосылған.



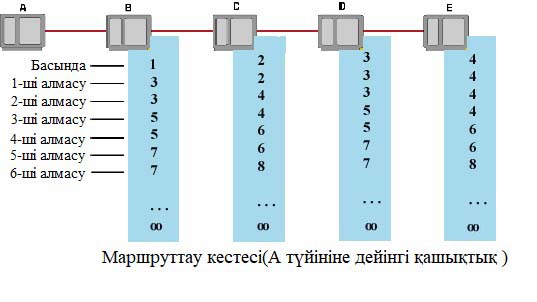
Егер X және Y арасындағы арна сәтсіздікке ұшыраса, онда Y «3» (1-ден Z-ге және Z-ден X-2-ге дейін) құны бар X-тен Z-ге жететін нәрсені шешеді.

Бұл алгоритмнің басты артықшылығы – оның қарапайымдылығы. Процесс барысында, маршрутизатор тек көршілерімен байланыс орнатады, олармен үнемі кесте көшірмелерімен алмасады. Маршрутизатор ең аз шығын болатын жолды таңдап, оны кестеге енгізеді. Бұл алгоритмнің артықшылығы жақсы жаңалықтарға тез әсер етеді (желіде жаңа маршрутизатордың пайда болуы), ал кемшілігі – жаман жаңалықтарға өте баяу әсер етеді (көршілердің бірінің жоғалып кетуі).

«Жақсы» жаңалықтарды таратудың мысалы. А маршрутизаторы қол жетімді болсын.



«Жақсы» жаңалықтардың таралуына мысал. A маршрутизаторды қол жетімсіз болсын.



Қашықтық векторы алгоритмінің мәселесін шешу. Мысалы, RIP хаттамасында ұзындығы 15-тен асатын транзиттік түйіннің бағыты шексіздікке тең деп саналады. Бұл жол маршруттау кестесінен дереу алынып тасталады. Хаттама кіші және орта желілер үшін өте қолайлы. Өткізудің максималды саны 16-мен шектелген. Хаттама желілік қасиеттердің өзгеруін дереу ескере алмайды (мысалы, кідірген уақыт пен арнаның жүктемесі). RIP неғұрлым жетілдірілген хаттамамен алмастыру үрдісі бар. RIP-дің екі нұсқасы бар: RIPv1 және RIPv2. RIPv2 қосалқы желі маскасы туралы ақпаратты ұстап тұрады, сондықтан ол қазіргі заманның талаптарына сәйкес келеді.

2.1.2 RIP хаттамасы

RIP - іске асырудың қарапайымдылығына байланысты ертерек жасалған хаттама. RIP қолдайтын бағыттау кестесі келесі ақпараттардан тұрады:

- белгіленген түйіннің IP мекенжайы;

- ретрансляция (тарату) саны 1 ден 15 дейін.;

- жолдағы келесі маршрутизатордың IP-мекен-жайы;

- әр жол үшін жеткізу уақыты;

- маршруттау кезіндегі ақпараттың өзгеру уақыты.

RIP – бұл қосалқы маршруттауға арналған қашықтық-векторлық хаттама. RIP анықталған жолдардың әрқайсысы үшін ретрансляция санын анықтайды және осы ақпаратты ең тиімді жолды таңдау үшін пайдаланады. Егер RIP ретрансляция санын есепке алмаса, шексіздікті санау мәселесі туындауы мүмкін. Кейбір желілерде, арна қол жетімді болмаған кезде, RIP логикалық циклге алып келетін жақсы альтернативті (тиімді) жолды іздеуді бастайды. Мұндай цикл шексіз қайталануы мүмкін. Осындай жағдайлардың алдын алу үшін RIP ретрансляция есептегішін қолдайды, ол 1 ден 15 дейінгі мәнге ие болуы мүмкін.

**RIP метрикасының түрлері**

Әр түрлі метрикаларға рұқсат береді:

-Хоптар;

-Енгізілген кешігу;

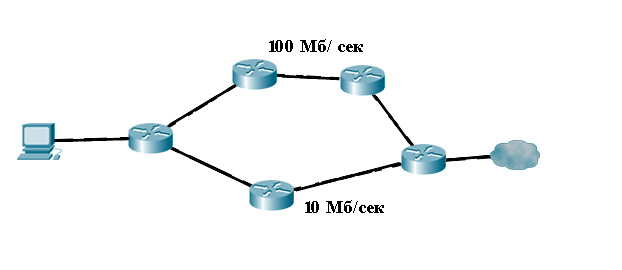
-Желілердің сенімділігі;

-Өткізу қабілеті;

-Осы өлшемдердің кез-келген комбинациясы.

Көп жағдайда қарапайым метрика қолданылады - хоптар саны, яғни аралық маршрутизаторлардың саны. Маршрутизаторлар хабарламаларды 30 секунд сайын ауыстырады. RIP хаттамасы 6 хабарландыру келгенше күтуге арналған, барлығы 180 сек құрайды. Бұл пайдаланушылар үшін тым ұзаққа созылу болып саналатын, тұтынуға сақталған маршрутты табуға кем дегенде 3 минут кететінін білдіреді. RIP-тегі негізгі мәселелердің бірі – беру жылдамдығын, арнаның өткізу қабілеттілігін есермеу.

**Тапсырма.** Екі арна бар: 1. Әрқайсысы 100 Мб/с болатын екі қосқыш. 2. 10 Мб/с жылдамдықтағы бір қосқыш. Беріліс қай жолмен жүреді?



Бұл сұлбада жоғарғы канал жылдамдығына қарамастан, маршрут төменгі, төмен жылдамдықты канал бойымен таңдалады.

1. кесте - RIPv1 және RIPv2 салыстыру

|  |  |
| --- | --- |
| RIPv1 | RIPv2 |
| Аутентификацияға қолдау көрсетілмейді | Аутентификацияға қолдау көрсетіледі |
| Маскаларға қолдау көрсетіледі | VLSM және CIDR қолдайды |
| Жаңартулар таратылады | Көп мекен-жайға жаңартулар жіберіледі |
| ұстап тұру уақыты 30 секунд | ұстап тұру уақыты 180 секунд |
| Ілмектер қалыатасады | Горизонтты бөлу әдісі қолданылады |

**RIP хаттамасын орнату**

Маршрутизаторда RIP қосу үшін алдымен маршрутизатордың конфигурациясына RIP қосу керек, содан кейін ол қай желілерде жұмыс істейтінін көрсету керек. Мысалы, 172.16.0.0 желі үшін RIP орнату қажет болса, конфигурация режиміне кіру керек:

Router(config)#**router rip**

Router(config-router)#**network 172.16.0.0**.

***Статикалық бағыттау***

Статикалық бағыттауы бар кестелер қолмен жасалады және жаңартылады. Осы бағдарлаумен маршрутты өзгерту басқа бағыттауларға осы оқиға туралы автоматты түрде хабарламайды. Осындай өзгертулер кезінде әкімшінің өзі бағыттау кестелеріне қажетті өзгертулер енгізуі керек.

Статикалық бағыттаудың артықшылығы – өткізу қабілеттілігі тұрақты, себебі бағыттаудың өзгеруі туралы таратылатын хабарламалар жоқ. Тағы бір жағымды қасиет – қауіпсіздік. Статикалық бағыттау кезінде бағыттаулар әкімші хабарлаған желілер туралы біледі.

Статикалық бағыттауды конфигурациялау үшін конфигурация режимінде ip route пәрменін (командасын) қолданыңыз***:***

**Ip route** желі маска мекен-жай / интерфейс [арақашықтық],

мұнда: желі – алушының желісі немесе қосалқы желісі; маска – қосалқы желі маскасы; мекен-жай – келесі өтулер үшін маршрутизатордың IP мекенжайы; интерфейс - алушы желісіне кіру үшін қолданылатын интерфейс атауы; арақашықтық – әкімшілік қашықтық.

Мысалы, 172.16.40.0 жойылған желіге статикалық бағыттауды орнату үшін келесі пәрменді енгізу керек:

**ip route 172.16.40.0 255.255.255.0 172.16.20.2**

немесе

**ip route 172.16.40.0 255.255.255.0 serial0.**

Сонымен, маршрутизатор 172.16.40.0 желіге арналған пакетті алған кезде, оларды serial0 интерфейс арқылы жіберу керек, оған маршрутизатор 172.16.20.2 IP мекен-жайы қосылған.

***Бағыттау***

Әдеттегі маршрут әр маршрутизаторда көрсетілуі керек, болмаса белгіленген желісі анықталмаған пакеттер алынып тасталады. Әдеттегі маршруттың тапсырмасы статикалық бағыттау кезінде орындалатын командамен бірдей орындалады, бірақ желінің адресі мен желілік маска (қосалқы желі) нөлге тең. Мысалы, егер маршрутизатордың соңғы желілері белгісіз барлық пакеттерді 172.16.20.2 IP мекенжайына жібергенін қаласаңыз, онда келесіні енгізу керек

**ip route 0.0.0.0 0.0.0.0 172.16.20.2.**

***passive и neighbor*** пәрмендер

***Passive*** командасы көрсетілген интерфейс арқылы кез келген өзгертулердің алдын-алу үшін қолданылады. Атап айтқанда, бұл пәрмен ғаламдық Интернетке қосылған интерфейске қолданылады. Мысалы, serial0 интерфейсі Интернетке қосылған делік, онда ол келесідей орындалады:

Router(config)#**router rip**

Router(config-router)#**network 172.16.0.0**

Router(config-router)#**passive serial0**

Router(config-router)#**^Z**

Router#.

Егер бір фирманың екі кеңсесі Frame Relay желісімен қосылған болса, онда RIP хабарламалары ол арқылы берілмейді. Осыған жол бермеу үшін neighbor пәрменін қолданады.

Router(config)#**router rip**

Router(config-router)#**network 172.16.0.0**

Router(config-router)#**neighbor 172.44.51.2**

Router(config-router)#**exit**

Router(config)#**^Z**

Router#.

Бұл мысалда, маршрутизатор таратылатын RIP хабарламаларын осы WAN форматында (біздің жағдайда, Frame Relay) инкапсуляциялайды және оларды мекен-жайы 172.44.51.2 болатын маршрутизаторға жібереді.

*RIP бақылау*

Жұмыстың дұрыс екендігін тексеру және RIP хаттамасын келтіру үшін кестеде көрсетілген пәрмендер қолданылады.

4 кесте - RIP хаттамаларының бақылау командалары

|  |  |
| --- | --- |
| Пәрмен (Команда) | Сипаттамасы |
| show ip route | Бағыттау кестесін көрсету. |
| show ip protocol | Таймерлерді, RIP желісі туралы ақпаратты және маршруттық ақпарат көздерін көрсету. |
| show ip interface | Интерфейс конфигурациясын көрсету. |
| debug ip rip | RIP күйін келтіруді қосыңыз. |
| trace | Бағытты қадағалаңыз. |

**Жалған маршруттарды қалыптастыру мәселесін шешу**

Жалған маршруттардың пайда болуын болдырмау үшін келесі әдістер қолданылады: «бөлек ақпараттандыру ережелері» горизонтты ыдырату (split-horizon) әдісі. «Бөлек ақпараттандыру ережелері» горизонтты ыдырату (split-horizon) әдісі – маршруттау кестесінде сақталған кейбір желілердің бағыттау туралы ақпараты ешқашан алынған маршрутизаторға берілмейді.

*Мысал.* Статикалық бағытты алып тастау және R маршрутизаторындағы бағыттау протоколын конфигурациялау.

1. 192.168.3.0 мекен-жайы бойынша статикалық бағытты жою.

R(config)#no ip route 192.168.3.0 255.255.255.0 192.168.2.2

1. RIP v2 бағыттауды қосыңыз және қатысушы желілерді жарнамалаңыз.

R(config)#router rip

R(config-router)#version 2

R(config-router)#network 192.168.1.0

R(config-router)#network 192.168.2.0

2.1.3 OSPF (Open Shortest Path First) хаттамасы

TCP/IP желілерінде ең танымалы OSPF болып табылады. OSPF белгілі бір қызмет түрі үшін маршруттарды есептеу мүмкіндігін ұсынады. OSPF – дейін хаттама ешбір протокол осы өрістің мәнін пайдаланбаған.

-Минималды кідіріс.

-Максималды өткізу қабілеті.

-Максималды сенімділік.

-Минималды шығындар (құны төмен).

RIP салыстырғанда, OSPF «екінші буын хаттамасы» болып табылады және оның көптеген артықшылықтары бар: OSPF желілерже аз жүктеме құрады, едәуір үлкен желілерді қолдайды, сөйлесуі аз және жіберуші мен тағайындалған менкен-жай арасындағы бірнеше жолды қолдайды.

Әрбір каналға өзінің салмағын беруге болады (ретрансляция саны);

- Қайта беру санына шектеу - 65535;

- Әрбір түйінде ағаш түріндегі желілік жолдар туралы мәліметтер базасы болады, оның жоғарғы жағында берілген түйін болады;

- Егер салмағы бірдей жолдар болса, онда жүктеме олардың арасында бөлінеді;

- Бағыттау кестелерін тарату тек өзгерістер болған кезде жүзеге асырылады;

- Бағыттау кестесіндегі өзгерістер туралы хабарламаны тек «өзіңіз оқып шығыңыз және өткізіңіз» әдісімен тікелей байланысты маршрутизатор жібереді, ол желідегі жүктемені азайтады.

Желінің жұмысын тиімді басқару үшін OSPF желілері аймақтар деп аталатын бөліктерге бөлінеді. Негізгі аймақ нөл деп аталады (area 0). Барлық OSPF желілерінде 0 аймақ бар. Әр аймақта осы сегмент үшін ақпарат көзі болып табылатын DR (Designated Router) маршрутзатор белгіленеді.



**-** Арна жағдайының хаттамасы қашықтық векторының хаттамасына қарағанда әлдеқайда жылдам жұмыс істейді.

- Егер арна жағдайының хаттамасы желінің сәйкестілігінен (жинақтылығынан) де әлдеқайда жылдам болады.

- Сәйкестілік (жинақтылық) (converge) түсінігі кез-келген өзгерістен кейін желінің күйін тұрақтандыруды білдіреді, мысалы, маршрутизатордың бұзылуы немесе каналдың істен шығуы.



Сонымен қатар, OSPF IP-ны тікелей қолдануына байланысты RIP-тен ерекшеленеді (басқа бағыттау хаттамалары сияқты). Бұл UDP немесе TCP пайдаланбайтындығын білдіреді. OSPF хаттама өрісінде IP тақырыбында орнатылатын өзіндік мәні бар. OSPF – бұл ішкі маршруттауға арналған бір ғана стандартты көп платформалы хаттама. Ол талғампаз иерархиялық құрылымға ие, сонымен қатар ақпаратты бағыттауды бұзылудан қорғайды. Қазіргі уақытта IPv6 үшін OSPF нұсқасы бойынша жұмыс жүргізілуде. Бұл ішкібағыттауларда алі де ұзақ уақыт пайдаланылатындығын білдіреді.

**Арна жағдайы хаттамасының жұмыс істеу принципі**

1. DVA (Distance Vector Algorithms) хаттамасынан айырмашылығы, LSA (Link State Algorithms) хаттамасының байланыс жағдайы туралы хабарлау кезеңді түрде қайталанбайды, тек HELLO хабарламалары көмегімен қандай да бір байланыс жағдайының өзгерісін орнау болған кезде беріледі.

2. Нәтижесінде, LSA хаттамаларымен тудырылатын трафик DVA хаттамасымен салыстырғанда әлдеқайда аз қарқынды.

3. Желіге қосқан кезде сіз көршілеріңіз туралы ақпарат алуыңыз керек. Көршілердің әрқайсысына дейінгі жолдың құнын біліңіз, яғни, арнаның жағдайы туралы біліңіз. Алынған ақпараты бар HELLO жарнамалық пакетін дайындаңыз. Бұл пакетті барлық көршілерге жіберіңіз. Барлық басқа маршрутизаторларға ең қысқа жол ағашын жасаңыз.

4. Арна күйіне негізделген бағыттау хаттамалары қашықтық векторлық хаттамалардың кемшіліктерінен бағынбайды. Осы хаттамаларда барлық белсенді байланыс арналарын көрсететін желілік карта жасалады. Бір маршрутизатор оңтайлы маршрутты құруды болжайтын жағдай жоқ, барлық маршрутизаторлар бірдей картаны пайдаланады, сондықтан бар маршруттар оларға «оңтайлы» болып көрінеді.

5. Топологиялық өзгерістер болған кезде, осы өзгерісті анықтайтын маршрутизатор ақпаратты барлық көршілеріне жібереді, басқалары да өз кезегінде солай істейді. Сондықтан маршрутизаторлар өздерінің дерекқорларын тез қалпына келтіре алады және процесс тез жинақталады. Әр өзгеріс уақыт белгісімен қамтамасыз етіледі; егер осылай орындалмаса, желінің кездейсоқ кідіруіне байланысты жаңа нұсқадан ерте шыққан ескі нұсқалар мәліметтер базасының маңыздылығын бұзуы мүмкін.

**OSPF метрикасы**

Метрика - белгілі бір желідегі (белгілі бір физикалық арнада) байланыс сапасын бағалау;

- Метрика неғұрлым аз болса, қосылымның сапасы соғұрлым жақсы болады.

- Маршруттың метрикасы маршрутқа кіретін барлық байланыстардың (желілердің) метрикаларының қосындысына тең.

- Қарапайым жағдайда (RIP хаттамасында кездесетіндей) әр желінің метрикасы бірге тең болады, ал маршруттық метрика – бұл оның хоптағы ұзындығымен бірдей.

- FTP және SMTP хаттамаларымен командаларды минималды кідіріспен жіберуі керек, ал деректерді беру үшін үлкен өткізу қабілеті болуы керек;

- DNS сұранысы UDP арқылы жіберіледі және жауап тезірек алынады, бірақ егер TCP арқылы болса, кідіріспен жіберу талабы қажет емес;

- Алайда, көп мүмкіндіктерді теріс пайдалану маршрутизатордың жадының шамадан тыс жүктелуіне және дұрыс жұмыс істемеуіне әкеледі.

- OSPF қызмет ету түріне байланысты кез-келген желі үшін әртүрлі метрикалық мәндерді анықтауға мүмкіндік береді. (Қызмет түрін TOS өрісінің оның тақырыбындағы мәніне сәйкес дейтаграмманы сұрайды).

Қызметтің әр түрі үшін өзінің бағыты және жылдам арнаны көп қажет ететін дейтаграмма есептелінеді, бір маршрут бойынша жіберу мүмкін болады, ал ең аз қымбат арнаны сұрағандарды басқасына жіберуге болады.

Өткізу қабілеттілігін бағалайтын желінің метрикасы берілген желінің физикалық ортасы арқылы 100 Мбит жіберуге қажетті секундтар саны ретінде анықталады. Мысалы, 10Base-T Ethernet негізіндегі желінің метрикасы 10, ал 56 кбит/с жалданған желінің метрикасы 1785 құрайды. 100 Мбит/с және одан жоғары деректерді беру жылдамдығы бар каналдың метрикасы бірге тең.

**OSPF хаттамасы** (Open Shortest Path First, RFC-1245-1248, RFC-1583-1587, Дикстрой ұсынған SPF алгоритмі) - IP желілеріндегі стандартты бағыттау хаттамасы. OSPF маршруттау хаттамасының заманауи нұсқасын ұйымдастырудың негізгі қағидалары RFC 2328-де сипатталған. OSPF – бұл маршруттық күйдің хаттамасы (метрика ретінде қызмет көрсету коэффициентінің сапасы қолданылады). OSPF қызметтің әр түрі type-of-service үшін жеке маршрутизаторлар жиынтығын есептей алады. Бұл кез келген бағытта бағыттау кестесінде бірнеше нүкте болуы мүмкін екендігін, IP қызметінің әр түрі үшін біреу болуы мүмкін екендігін білдіреді. Әр интерфейске баға белгіленеді. Оны өткізу қабілеттілігі, қайтару уақыты, сенімділігі немесе басқа параметрлер бойынша тағайындауға болады. IP қызметінің әр түрі үшін бөлек баға белгіленуі мүмкін. Егер сол бағытқа бірдей бағамен бірнеше маршрут болса, OSPF трафикті (деректер ағынын) осы бағыттар арасында теңдей таратады. Мұндай жағдайды жұмыс жүктемесінің балансы деп атайды.

OSPF қосалқы желілерді қолдайды: қосалқы желі маскасы әрбір хабарланған бағытқа сәйкес келеді. Бұл кез-келген кластың IP-мекен-жайын әртүрлі көлемдегі бірнеше қосалқы желіге бөлуге мүмкіндік береді (өзгермелі ішкі желі – VLSM).

Маршрутизаторлар арасындағы нүкте-нүкте сілтемелерінің соңында IP мекенжайы болмайды. Бұл мекенжайсыз желілер unnumbered деп аталады. Бұл тәсіл сізге IP-мекен-жайларды үнемдеуге мүмкіндік береді – қазіргі уақытта өте құнды ресурс! Аутентификацияның қарапайым схемасы қолданылады. Құпия сөз RIPv2 схемасында көрсетілгендей, анық мәтінмен көрсетілуі мүмкін.

OSPF кең хабарландыру орнына топтық мекенжайды қолданады, бұл OSPF танымайтын жүйелердегі жүктемені азайтады. OSPF – бұл Link–State класстағы маршруттаудың классикалық хаттамасы, ол мыналарды қамтамасыз етеді:

-желінің көлеміне шектеулердің болмауын;

-кластан тыс желілерді қолдау;

-типтегі мекенжайларын пайдалану арқылы маршруттардың жаңартуларын беру;

-маршрутты құрудың жеткілікті жоғары жылдамдығы;

- маршрут жаңартуларын беру және алу кезінде authentication процедурасын қолдану.

OSPF маршрутизаторының жұмысы барлық қосылған порттар арқылы «сәлемдесу» пакеттерін жіберуден басталады. Көрші маршрутизатор анықталған кезде, құрылғылар аутентификация үшін ақпаратпен алмасады. Егер бұл операция сәтті болса, олар бір-біріне өздерінің жүйелік нөмірлерін береді. Маршрутизаторлар тобы бір-бірімен жұмыс істеуге болатындығын анықтағаннан кейін олардың біреуі жауапты маршрутизаторға (designated router, DR) айналады, ал екіншісі резервтік жауапты маршрутизаторға айналады (backup designated roter – BDR). DR осы аймақтағы барлық маршрутизаторларға сілтеменің мемлекеттік деректер базасын және мультимедиялық желіні өзгерту туралы хабарламаны ұстауға жауап береді. Арнаның күйі өзгерген кезде, осы арна тиесілі маршрутизатор сәйкес DR және BDR хабарламаларын жібереді. Деректер базасының көшірмесі BDR-де сақталады. Бұл маршрутизатор DR рұқсат алу мүмкін болмаған кезде күшіне енеді. Әрі қарай алмасу хаттамасы күшіне енеді. Осы кезде маршрутизаторлар өздері қолдайтын арналардың нұсқа нөмірін DR-де сақталған нұсқа нөмірлерімен салыстырады. Әрі қарай, су тасқыны (flooding) хаттамасын қолдана отырып, маршрутизаторлар қызығушылық танытатын арналармен алмасады, олардың дерекқорлары мен DR дерекқорларының маңыздылыңын қолдап отырады.

**OSPF артықшылықтары**

-Иерархиялық бағыттау.

-Параллель арналар арасындағы жүктемелерді теңестіру (Load balancing).

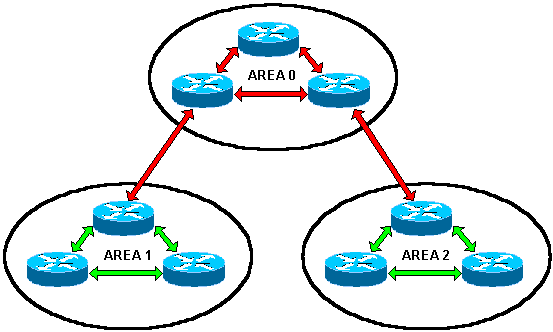
-Ақпарат көзінің түпнұсқасын анықтау тәртібі.

-Маршруттар туралы ақпарат алмасуды ұйымдастырудың ерекше тәсілдері.

**Иерархиялық бағыттау**

-Иерархиялық маршрутизацияны пайдалану олар арқылы берілетін трафиктің үлесін азайту арқылы деректерді беру арналарын пайдалану тиімділігін едәуір арттырады.

-Аймақ ішіндегі деректерді беру маршрутын анықтау үшін маршрутизаторлар іске асыратын ақпарат алмасу басқаларға берілмейді (2.2 суреттегі жасыл түспен көрсетілген).



2.2 сурет – Маршрутизаторлар арасындағы байланыс.

**Load balancing**

-OSPF кезінде бірнеше бағыт рұқсат етіледі.

-Егер бұл маршруттар мәліметтерді берудің бірдей сапасын қамтамасыз етсе, маршруттар бір уақытта пайдаланылады, бұл деректерді беру жылдамдығын едәуір арттыруды қамтамасыз етеді.

-Параллельді каналдар арасындағы трафикті динамикалық түрде қайта бөлу, яғни осы каналдардағы жүктеме деңгейіне пропорционал түрде орындалса Load balancing деп аталады.

**Authentication процедурасы**

-Түпнұсқасын анықтау процедурасын қолдану ақпараттық қауіпсіздікке сәйкес келеді.

-Маршрутизаторлар қабылдағышқа берілетін деректер көзінің түпнұсқалығын анықтау үшін қажетті әрекеттер жиынтығын орындауы керек (authentication procedure).

-Егер, берілген мәліметтердің көзі аутентификация процедурасын сәтті аяқтаса, онда маршруттар туралы мәліметтер өңдеуге қабылданады.

**Маршрут туралы ақпаратпен алмасу**

-OSPF маршруттау хаттамасының айрықша ерекшелігі – маршрутты анықтау процесінде маршрутизаторлар арасында ақпарат алмасу үшін multicast типті мекен-жайларды пайдалану.

-Мұндай адрестерді пайдалану broadcast түріндегі мекен-жайларды пайдалануды жояды, бұл өз кезегінде желінің есептеу ресурстарын пайдалану тиімділігінің артуына әкеледі.

-OSPF маршруттау хаттамасында ақпарат алмасуды ұйымдастырудың тағы бір маңызды ерекшелігі - «тағайындалған» (designated) маршрутизаторларды пайдалану.

-Бұл мүмкіндікті бірнеше маршрутизаторлар бір желіге қосылған кезде пайдалану қызметік трафик көлемін едәуір азайтуға мүмкіндік береді.

**OSPF кемшіліктері:**

-Басқа хаттамаларды қолдайтын немесе статикалық бағыттауы бар түйіндер үшін арнаны таңдау туралы ақпарат алу қиын.

-OSPF – бұл тек қосалқы хаттама.

*Бір аймақта OSPF хаттамасы қалпына келтіру*

OSPF (Open Shortest Path First – бірінші болып қысқа жолды ашу). IGP маршруттаудың иерархикалық алгоритмі ең аз шығындар көрсеткіші бағытымен, бірнеше маршрутты бағыттау және жүктемелерді бірдей бөлу сияқты функциялармен жабдықталған.

Маршрутизаторда OSPF бапталған кезде OSPF процесі оның сәйкестендіру нөмірімен (ID процесстері) анықталады. Сәйкестендіру нөмірлері автономды жүйелік нөмірлер емес, сондықтан белгілі бір OSPF аумағында бірегей болмауы керек. Процесс нөмірі тек OSPF жұмыс істеп тұрғандығы туралы маршрутизаторға хабарлау үшін қызмет етеді. Процесс идентификаторы бойынша ауданды анықтаудың орнына сеансқа қосылған желілер OSPF аймақтарымен салыстырылады. Бұл осы аймаққа салыстырылған барлық желілер осы ауданды құрайды дегенді білдіреді. OSPF аймақтары желілік нөмірлермен анықталатындықтан, OSPF процесі маршрутизатор интерфейсімен байланысқан желілік нөмірлерді талдайды, содан кейін оларды интерфейстердің конфигурацияланған IP мекен-жайларымен байланыстыра отырып, осы аймақта қандай желілер немесе ішкі желілер ұсынылатындығын анықтайды. Пәрмен синтаксисі төменде көрсетілген.

***router ospf ID-процесі***

***network үлгі-маска мекенжай area ID-аймағы,***

мұндағы: ID процесс – ID процесс, 1-ден 65535-ке дейінгі бүтін сан;

Аймақтың идентификаторы – аймақтың идентификаторы, 0 ден 4294967295 аралығындағы бүтін сан.

***Мысалы:***

**Router#configure terminal**

Router(config)#router ospf 1

Router(config-router)#**network 172.16.10.0 0.0.0.255 area 20**

Router(config-router)#**network 10.1.2.0 0.0.0.255 area 20**

Router(config-router)#^**Z.**

1 процестің ID мысалында 172.16.10.0 және 10.1.2.0 қосалқы желілері 20 - салыстырылған.

OSPF жұмысын және дұрыс қалпына келтірілгенін тексеру келесі командалармен жүзеге асырылады:

show ip ospf – OSPF жұмысы туралы жалпы ақпарат береді: сәлемдемелер қаншалықты жиі жіберілетіндігін анықтайтын SPF алгоритмдерінің санын және жаңарту таймерінің мәні.

- show ip ospf interface интерфейстер мен аудандардың сәйкестігін тексеруге мүмкіндік береді, сонымен қатар сәлемдесу пакеттерінің таймері мен берілу аралығын көрсетеді.

- show ip ospf border-routers шекаралық маршрутизаторлары аймаққа және автономды жүйенің шекаралық маршрутизаторларына қатысты кесте жазбаларын көруге мүмкіндік береді. Сонымен қатар, пәрменде берілген маршрутизатордың аймақта орналасқандығы немесе әртүрлі аймақтарды қосатындығы туралы ақпарат көрсетіледі.

***Мысалы.*** OSPF аутентификациясын қалпына келтіру және тексеру

OSPF хаттамасы шифрланбаған және шифрланған парольді пайдалану арқылы аутентификацияны пайдалануға мүмкіндік береді. Шифрланбаған аутентификация паролі қауіпсіз емес болғандықтан, Message Digest 5 (MD5) аутентификация алгоритмі қолданылады.

OSPF аутентификациясыy қалпына келтіру екі кезеңмен іске асырылады. Біріншіден, ол осы аймақтың маршрутизаторында қосылады, содан кейін ол осы аймақтағы интерфейстер конфигурациясын қалпына келтіруге беріледі.

Екі бағыттағышта 0 аймағында MD5 аутентификациясын қосыңыз.

R1(config)#**router ospf 1**

R1(config-router)#**area 0 authentication message-digest**

R2(config)#**router ospf 1**

R2(config-router)#**area 0 authentication message-digest**

R1 бағыттауышында s0/0/0 интерфейсінде OSPF аутентификациясын қосыңыз.

R1(config)#**interface s0/0/0**

R1(config-if)#**ip ospf message-digest-key 10 md5 secretpassword**

show ip ospf neighbor команданы R1-ге белгілі көрші маршрутизаторларды көру үшін қолданыңыз.

R1#**show ip ospf neighbor**

4) Сол сияқты R2 маршрутизаторында 2) және 3) қадамдарды орындаңыз.

***Мысал***: 0 магистральдық аймаққа IPv6 интеграциялау.

RTA-да IPv6 мекен-жайларын және OSPFv3 бағыттауды конфигурациялау.

RTA(config)#**ipv6 unicast-routing**

RTA(config)#**ipv6 router ospf 10**

RTA(config-rtr)#**router-id 1.1.1.1**

RTA(config-rtr)#**exit**

RTA(config)#**interface serial 0/0/0**

RTA(config-if)#**ipv6 address 2001:DB8:CAFE:A001::2/64**

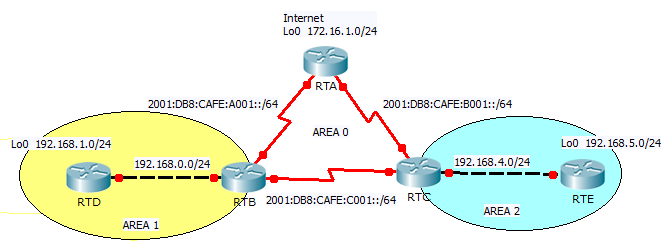
RTA(config-if)#**ipv6 ospf 10 area 0**

RTA(config-if)#**interface serial 0/0/1**

RTA(config-if)#**ipv6 address 2001:DB8:CAFE:B001::2/64**

RTA(config-if)#**ipv6 ospf 10 area 0**

RTA(config-if)#**end**



0 аймақтың бірізді интерфейсінде OSPFv3 конфугурацияланғанын тексеріңіз.

RTA#**show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "static

IPv6 Routing Protocol is "ospf 10"

Interfaces (Area 0)

Serial0/0/0

Serial0/0/1

RTB-де IPv6 мекенжайын және OSPFv3 бағыттауды конфигурациялаңыз.

RTB(config)#**ipv6 unicast-routing**

RTB(config)#**ipv6 router ospf 10**

RTB(config-rtr)#**router-id 2.2.2.2**

RTB(config-rtr)#**interface serial 0/0/0**

RTB(config-if)#**ipv6 address 2001:DB8:CAFE:A001::1/64**

RTB(config-if)#**ipv6 ospf 10 area 0**

RTB(config-if)#**interface serial 0/0/1**

RTB(config-if)#**ipv6 address 2001:DB8:CAFE:C001::1/64**

RTB(config-if)#**ipv6 ospf 10 area 0**

RTB(config-if)#**end**

OSPFv3 хаттамасы бойынша RTB мен RTА арасында көршілес қатынастар орната алғанына көз жеткізіңіз.

RTB#**show ipv6 ospf neighbor**

Neighbor ID Pri State Dead Time Interface ID Interface

1.1.1.1 0 FULL/ - 00:00:32 4 Serial0/0/0

5) RTC- те IPv6 мекенжай мен OSPFv3 бағыттауын қалпына келтіріңіз.

RTC(config)#**ipv6 unicast-routing**

RTC(config)#**ipv6 router ospf 10**

RTC(config-rtr)#**router-id 3.3.3.3**

RTC(config-rtr)#**interface serial 0/0/0**

RTC(config-if)#**ipv6 address 2001:DB8:CAFE:C001::2/64**

RTC(config-if)#**ipv6 ospf 10 area 0**

RTC(config-if)#**interface serial 0/0/1**

RTC(config-if)#**ipv6 address 2001:DB8:CAFE:B001::1/64**

RTC(config-if)#**ipv6 ospf 10 area 0**

RTC(config-if)#**end**

6) RTC маршрутизаторының OSPFv3 бойынша RTA және RTB арасындағы 2001: DB8: CAFE: A001 :: / 64 желісіне бағыт алғанын тексеріңіз.

RTC#**show ipv6 route**

IPv6 Routing Table - 6 entries

<output omitted>

O 2001:DB8:CAFE:A001::/64 [110/128]

via FE80::201:C7FF:FEC5:B002, Serial0/0/0

via FE80::2D0:FFFF:FE09:9102, Serial0/0/1

C 2001:DB8:CAFE:B001::/64 [0/0]

via ::, Serial0/0/1

L 2001:DB8:CAFE:B001::1/128 [0/0]

via ::, Serial0/0/1

C 2001:DB8:CAFE:C001::/64 [0/0]

via ::, Serial0/0/0

L 2001:DB8:CAFE:C001::2/128 [0/0]

via ::, Serial0/0/0

L FF00::/8 [0/0]

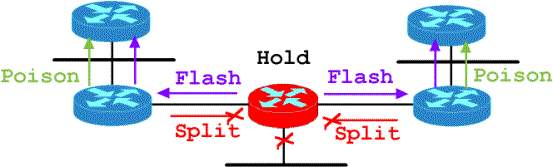
via ::, Null0

7) 2001:DB8:CAFE:A001::/64 желісінің қол жетімді екендігін тексеріңіз.

RTC#**ping ipv6 2001:DB8:CAFE:A001::1**

2.1.4 IGRP хаттамасы

IGRP хаттамасы автономды жүйелердің ішінде орналасқан маршруттарды анықтауға арналған, сондықтан Interior Gateway Protocol хаттамалар түріне жатады. Автономды жүйе ішіндегі маршруттар туралы ақпарат жинау әдісіне сәйкес бұл хаттама distant-vector түріне жатады. Poison reverse – маршрут көрсеткіштерінің жоғарылауы, әдетте, келесі маршруттау циклінің бар болуын білдіреді. Метрика біртіндеп өсе бастайтын бағыттарды бұғаттау (блоктау) үшін оларға, әдетте, шексіздікке сәйкес келетін метрикалық мән белгіленеді.



2.3 сурет – Блоктау маршруттары.

Қызыл түспен белгіленген маршрутизаторды орталық желімен қосатын арна жоғалса (2.3-сурет), бұл маршрутизатор осы желі үшін басқарылатын жаңартуларды қалыптастырады және hold down ауысады, яғни, бұл кезде ол осы желі үшін маршрут жайлы ақпарат қабылдай алмайды. Split Horizon принципіне сәйкес, оның жақын көршілері оған осы маршрут бойынша жаңартуларды жібермеуі керек. Бұл бағытты көрші маршруттық кестелерден алып тастау үшін маршрутизаторлар Poison Reverse функциясын қолдана алады.

2.1.5 EIGRP хаттамасы

EIGRP (Enhanced Interior Gateway Routing Protocol) – бұл сол фирманың IGRP хаттамасы негізінде Cisco фирмасы жасаған қашықтық-векторлық бағыттау хаттамасы. Қашықтық-векторлық алгоритмнің кемшілігі жойылады:

- Диффузиялық жаңарту алгоритмі көмегімен;

- Бағыттау кестесі тек белгіленген желілерге баратын жолдағы келесі түйіннің мекен-жайын ғана емес, сол қысқа жолды білетін көршілердің тізімін де сақтайды.

- EIGRP маршрутизаторы белгілі бір уақыт мезетінде «Hello» хабарламаларын жіберу арқылы көршілерін анықтайды.

- Дәл осындай хабарламалар көршімен байланыс жағдайын бақылау үшін қолданылады (олар әр 5 секунд сайын өткізу қабілеті жоғары желілерде жіберіледі - мысалы, Ethernet және әр 60 секунд сайын «баяу жұмыс жасайтын» желілерде).

- Мұндай мониторинг сізге желіге қашықтық векторларын белгілі бір уақыт мезетінде емес, тек желілік топология өзгерген кезде жіберуге мүмкіндік береді.

- EIGRP желі арқылы мәліметтерді беру үшін өткізгіштік қабілеті және кідіріс өлшемдері негізінде есептелген күрделі метрикалық мәнді қолданады.

- Сондай-ақ, метрикалық есептеу желі жүктемесі мен сенімділік көрсеткіштерін қамтуы мүмкін.

EIGRP-тегі метриканың RIP хаттамасынан айырмашылығы жүйенің өлшемін шектейтін фактор болып саналмайды. EIGRP-те бірнеше бағыттардың арасындағы жүктемелердің тепе-теңдігін жүзеге асырады. Маршрутизацияның инкременттік (тек өзгертілген) жаңартулары. Ресми көршілік қарым-қатынас. Бұл хаттама IGRP сияқты бірдей қашықтықтағы және бағыттағы ақпаратпен жұмыс істейді, бірақ оны басқа алгоритммен өңдейді. EIGRP метрикаларды есептеу үшін диффузиялық жаңарту алгоритмін (DUAL) қолданады. Ресми түрде EIGRP хаттамасы distant – vector маршруттау алгоритмдеріне жатады. Алайда, бұл хаттама link-state түріндегі хаттамасының ең жақсы қасиеттерін біріктіреді. Сондықтан оны маршруттау хаттамаларының ерекше түріне – гибридтік хаттамаларға жатқызуға болады. EIGRP хаттамасы сонымен қатар IGRP ретінде қалпына келтіруге болады, яғни желілік процесс және автономды жүйе қалпына келтіріледі. EIGRP хаттамасы RIP және IGRP салыстырғанда жетілдірілген және OSPF қарағанда оңай қалпына келтіруге болады. EIGRP негізіндегі желілер өте сенімді және кеңейтілген.

EIGRP жұмыс істеу принципі

Маршрутизатордағы EIGRP дерекқоры көршілерден алынған барлық маршруттар мен метрикаларды сақтайды. Әрбір жеке желі үшін 6 маршрутты сақтауға болады. Олардың ішінен маршрутизатор негізгі және қосымша (резервтік) көшірмелерді таңдау керек (негізгі маршрут маршруттау кестесіне енгізілген). Межелі жерге баратын ең жақсы маршрутты таңдау кезінде маршрут активті (белсенді) күйде, таңдаудан кейін - ол пассивті күйге өтеді. Жергілікті маршрутизатордағы және көршілерден алынған метрика туралы ақпарат негізінде (мысалы, өткізу қабілеті, кідіріс) біріктірілген метрика есептеледі (метрика құны қосылады).

Ең жақсы көрсеткішке ие маршрут (ең төменгі құнымен) негізгі, ал келесі көрсеткішке – қосымша (егер бар болса) болып жарияланады. Негізгі маршруттар бөлінгеннен кейін маршруттау кестесіне енгізіледі. EIGRP-де маршрутизатор көршілерге бүкіл маршруттау кестесін бермейді, тек ондағы өзгерістер ғана береді. Тікелей қосылған маршрутизаторлар арасындағы тең құқықты байланыстарды орнату және қолдау үшін HELLO хаттамасы қолданылады. Сәлемдесулер қарым-қатынас жағдайын анықтау үшін алмастырылады. Әр маршрутизатор көршілер кестесін жасайды, онда оған тікелей қосылған көршілер туралы маңызды ақпарат сақталады:

-көршілердің IP мекенжайлары;

-блоктау аралықтары;

-SRTT таймерінің мәні;

-кезек туралы ақпарат.

Бұл деректер байланыс күйіндегі өзгерістердің нақты қай жерде болғанын анықтау үшін қажет.

Екі маршрутизатор байланыс орнатқан кезде, олар толық кестелермен алмасады. Осыдан кейін, барлық тікелей қосылған маршрутизаторларға ғана тән өзгерістер беріледі. Байланыс орнату келесі түрде орнатылады:

-сәлемдер барлық M интерфейстерінен жіберіледі;

-көрші М-нен деректер базасына (ДБ) енгізілген маршруттар туралы ақпаратпен келеді;

-бастапқы M пакет ACK растауын береді;

-топология базасы жаңадан алынған ақпарат негізінде жаңартылады.

-жаңартудан кейін, түпнұсқа М өзінің барлық кестесін барлық жаңа көршілерге жібереді;

Көршілер ACK пакетінен ақпарат алғандарын растайды.

Ең жақсы маршрутты және жүктеменің біркелкі таралуын анықтау үшін бірнеше мәліметтер базасын құрады:

-ең жақсы маршруттар туралы ДБ;

-топология бойынша мәліметтер базасы (маршруттар туралы барлық ақпарат;

- көршілер кестесі.

Бұл ДБ әрқайсысы IP, IPX, AppleTalk үшін бөлек, сондықтан егер 3 хаттама жұмыс істесе, онда 9 дерекқорды М-да сақтауға болады.

***Кеңес.*** EIGRP-ны Cisco құрылғыларына негізделген өте үлкен (немесе метрикалардың күрделі есептеулері мен жүктемелерді тепе-теңдігін қажет ететін) желісі бар кез келген адамға ұсынуға болады.

Қалған барлық басқа жағдайларда OSPF қолданған жөн.

Жалпы алғанда, байланыстырушы күйлердің хаттамалары (OSPF) желілік топологиядағы өзгерістерді EIGRP-ге қарағанда тезірек өңдейтіндігіне қарамастан, OSPF бірқатар қосымша мүмкіндіктерге ие, EIGRP қарапайым және маршрутизатордың есептеу ресурстарына аз талап қояды.

***Мысал***. EIGRP бағыттауды қалпына келтіру.

R маршруттау хаттамасына маршруттау хаттамасы ретінде аты-жөні көрсетілмеген жүйелік нөмірі бар EIGRP көрсетіңіз және тиісті желілерді жариялаңыз:

R(config)#**router eigrp 100**

R(config-router)#**network 10.0.0.0**

R(config-router)#**network 10.0.0.4**

2) MD5 аутентификациясын қалпына келтіру. Dischain деп аталатын кілттер жиынтығын жасаңыз. 1 кілт ретінде san-fran кілтін енгізіңіз. Әр көрші EIGRP маршрутизаторы үшін жұмыс тобының маршрутизаторында EIGRP MD5 аутентификациясын пайдалануды қосыңыз және icndchain кілтінің жиынтығын қолдануды көрсетіңіз.

R(config)#**key chain discchain**

R(config-keychain)#**key 1**

R(config-keychain-key)#**key-string san-fran**

R(config-keychain-key)#**end**

R#**config terminal**

R(config)#**interface serial0/1/1**

R(config-if)#**ip authentication mode eigrp 100 md5**

R(config-if)#**ip authentication key-chain eigrp 100 discchain**

3) Маршруттарды автоматты түрде қосуды өшіру

R(config)#**router eigrp 100**

R(config-router)# **no auto-summary**

Қалыпқа келтірулердің дұрыс орындалғанын тексеру

1) show ip eigrp neighbors командаларын пайдаланып, көршілес EIGRP маршрутизаторларының кестесін шығарыңыз.

2) Show ip Protocol Protocol командасымен динамикалық бағыттау хаттамасында пайдаланылатын нақты ақпаратты көрсетуге болады.

3) Бағыттау кестесін көру үшін show ip route командасын қолданыңыз.

**EIGRP-Metrics қалпына келтіру.**

show interfaces Serial0/0 команда нәтижесінен R маршрутизаторының Serial 0/0 интерфейсі үшін EIGRP-Metric құраушыларының мәндерін алу.

R маршрутизаторының Serial интерфейстері үшін bandwidth мәндерін орнату.

R(config)#interface Serial0/0

R(config-if)#bandwidth 64

## 2.2 Мекен-жайларды анықтау

2.2.1 ARP мекен-жайын анықтау хаттамасы

Мәселе мынада, IP мекенжайлары тек TCP/IP хаттамалар тобында ғана қандай жа бір мағынаға ие болады. Арналық деңгейлер өзіндік мекенжай сұлбасына ие (негізінен маршрутизаторының 48 биттік мекенжайлар); желілік деңгейлер, өз кезегінде, осы арналық деңгейлерді пайдаланады. Әр түрлі желілік хаттамаларды қолданатын компьютерлер бірдей физикалық кабельде болуы мүмкін. Желілік адаптердің драйвері ешқашан IP-датаграммадағы тағайындалған IP мекен-жайына қарамайды. Басқаша айтқанда, екі түрлі мекенжай арасындағы сәйкестікті құру қажет болады: 32 биттік IP мекенжайлар мен қандай да бір арналық деңгейлер мекен-жайларын. Біз екі хаттаманы қарастырамыз: мекенжайды анықтау хаттамасы (ARP – address resolution protocol) және (RARP – reverse address resolution protocol) кері мекенжайды анықтау хаттамасы (RARP). 2.4 суретте екі хаттама ARP және RARP көрсетілген.

ARP

RARP

32 – битный адрес Internet

48 – битный адрес Ethernet

2.4 сурет – Мекенжайды анықтау хаттамасы: ARP және RARP.

ARP мекенжайды анықтау хаттамасы IP мекенжайларын және соған байланысты аппараттық мекенжайларды динамикалық картаға түсіруді қамтамасыз етеді. Біз динамикалық терминді қолданамыз, өйткені бұл автоматты түрде жүреді және, әдетте, қолданбалы бағдарламалармен пайдаланылатын немесе жүйе әкімшісінің еркіне байланысты тәуелді болмайды.

RARP негізінен қатты дискілері жоқ жүйелер қолданылады (дисксіз жұмыс станциялары немесе X терминалдары), бірақ мұнда жүйелік әкімшінің қатысуымен қолмен қалпына келтіру қажет.

Мысал. Егер біз% ftp bsdi командасын енгізсек, келесі әрекеттер орындалады:

1. Бағдарлама, FTP тұтынушы хост атауын (bsdi) 32 биттік IP мекен-жайға түрлендіру үшін DNS функциясын шақырады.

2. FTP тұтынушы көрсетілген IP мекен-жайы бойынша TCP байланысын орнатуды талап етеді.

3. TCP көрсетілген IP мекен-жай бойынша IP датаграмманы жіберу арқылы қашықтағы хостқа қосылу сұраныс жібереді.

4. Егер белгіленген хост желіге қосылған болса (Ethernet, Token ring немесе нүкте-нүкте арнасының екінші ұшына), IP датаграмманы тікелей хостқа жіберу мүмкін болады. Егер белгіленген хост қашықтағы желіде болса, IP маршрутизаторы IP датаграмманы жіберу үшін тікелей қосылған келесі маршрутизатордың Internet мекенжайын анықтайды. Екі жағдайда да, IP датаграмма тікелей желіге қосылған хостқа немесе маршрутизаторға жіберіледі.

5. Егер Ethernet қолданылса, жіберуші хост 32 биттік мекенжайды 48 биттік Ethernet мекенжайына түрлендіруі керек. Немесе басқаша айтқанда, интернеттегі логикалық Ethernet мекен-жайдан сәйкес келетін физикалық аппараттық мекен-жайға ауысыңыз. Бұл жағдайда, ARP жұмыс жасайды. ARP бір желіге қосылған көптеген хосттар немесе маршрутизаторлардың тарату желілерінде жұмыс істейді.

6. ARP желідегі әрбір хостқа ARP сұранысы (ARP request) деп аталатын фрейм Ethernet жібереді. Мұндай тарату әдісі хабар тарату сұранысы (broadcast) деп аталады. ARP сұрауында белгіленген хосттың (bsdi атауы) IP-мекен-жайы және «егер сіз осы IP мекен-жайдың иесі болсаңыз, маған өзіңіздің аппараттық мекен-жайыңызды айтыңыз» деген сұраныстан тұрады.

7. ARP деңгейіндегі белгіленген хост осы хабар тарату сұранысын қабылдайды, жіберушінің IP мекенжайын сұрайтынын анықтайды және ARP жауабымен (ARP reply) жауап береді. Бұл жауапта IP мекенжайы және сәйкес аппараттық мекенжайы болады.

8. ARP жауабы қабылданады, соның арқасында ARP сұранысы алмастырыла бастаған IP датаграмманы жіберуге болады.

9. IP-датаграмма белгіленген хостқа жіберіледі.

ARP-де тұжырымдалған негізгі тұжырымдама келесідей қорытындыланады. Желі интерфейсі аппараттық деңгейде алмастырылған аппараттық мекен-жай Фреймдерге ие, дұрыс интерфейске бағытталуы керек. Алайда, TCP / IP өзінің мекенжай сұлбасын қолданады: 32 биттік IP мекенжайлары. Хосттың IP мекенжайын білу ядроға осы хостқа деректер кестесін жіберуге мүмкіндік бермейді. Ethernet драйвері мәліметтерді сол жерге жіберу үшін белгіленген құрылғының мекен-жайын білуі керек. ARP міндеті - 32 биттік IP мекенжайлары мен әртүрлі желілік технологиялар пайдаланатын аппараттық мекенжай арасындағы динамикалық сәйкестікті қамтамасыз ету.

ARP жұмысының тиімділігі көбінесе әр хостта болатын ARP кэшіне (ARP cache) байланысты. Кэште Интернет мекен-жайы және олардың сәйкес аппараттық мекен-жайы болады. Әр кэштегі жазбаның стандартты мерзімі жазба жазылған сәттен бастап 20 минутты құрайды.

ARP кэшінің мазмұнын arp командасының көмегімен көруге болады.



**Arp командасы.** Команда параметрлері:

-a - барлық ARP кэш жазбаларын көрсету.

-d, жазбаны ARP кэшінен жою.

-s, ARP кэшіне жазба қосыңыз. Бұл опцияны пайдалану кезінде сіз хост атауын және Ethernet мекенжайын, хост атауына сәйкес IP мекенжайын және Ethernet мекенжайын кэшке қосуыңыз керек. Мұндай жазба тұрақты түрде жүзеге асырылады (ол күту уақытында кэштен жойылмайды), егер пәрмен жолының соңында temp құпия сөзі қолданылмаса.

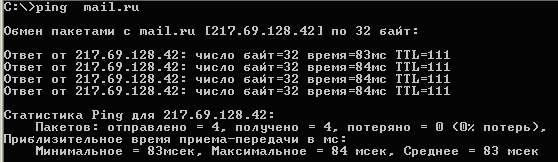


ARP – бұл барлық TCP/IP хаттамарда қолданылатын негізгі хаттама. Әдетте, оның жұмыс істеуі қолданылған қолданбаларға немесе жүйе әкімшісінің еркіне байланысты емес. ARP кэші – бұл жұмыстың негізі. Arp командасын кэшті қарау немесе өзгерту үшін қолдандық. Кэштегі әр жазбада таймер бар, ол аяқталмаған немесе аяқталған жазбаларды жою үшін қолданылады. ARP командасы өзгертілген жазбаларды ARP кэшінде көрсетеді.

Ping бағдарламасы. Ping бағдрламасы қашықтағы хосттың қол жетімділігін тексеруге арналған. Бағдарлама хостқа ICMP жаңғырық сұрауын жібереді және ICMP жаңғырық жауапының қайтарылуын күтеді.

Әдетте, егер сіз Ping-ді хостқа жібере алмасаңыз, Telnet немесе FTP көмегі арқылы осы хостқа қол жеткізе алмайсыз. Екінші жағынан, егер сіз Telnet көмегімен хостқа кіре алмасаңыз, онда, ережеге сәйкес Ping мәселені бастайтын бастапқы нүкте болып табылады. Сонымен қатар, Ping көмегімен сіз хосттан пакеттің қайтарылу уақытын есептей аласыз, бұл хосттың қаншалықты алыс екендігі туралы түсінік береді. Реттік нөмір 0-ден басталады және келесі жаңғырту сұранысы жіберілген сайын пинг әр қайтарылған пакеттің реттік нөмірін басып шығарады, пакеттің жоғалған-жоғалмағанын, пакеттің реттілігі өзгергенін немесе пакеттің қайталанғанын көруге мүмкіндік береді. IP – бұл датаграмманы жеткізуде сенімсіз қызмет болғандықтан, жоғарыда аталған үш шарттың кез-келгені Ping бағдарламасы жұмыс істеп тұрған кезде пайда болуы мүмкін.

Ping бағдарламасы – TCP/IP қолданатын жүйелер арасында байланыс бар-жоғын анықтауға мүмкіндік беретін негізгі тестілеу құралы. Ол ICMP эхо-сұранысын және эхо-жауапты қолданады және тасымалдау деңгейлерін (TCP немесе UDP) қолданбайды. Ping қызметі, әдетте, ICMP негізгі ядроның іске асыру бөлігі болып табылады (2.5 сурет).



2.5 сурет – Ping командасын қолдануға мысал.

2.2.2 TCP хаттамасы

TCP (Transmission Control Protocol) хаттамасы әр түрлі компьютерлік байланыс желілеріне қосылған, бір жүйеге біріктірілген негізгі компьютерлердегі процесс жұбы арасында сенімді тікелей байланысты қамтамасыз етуге арналған. Ол IP хаттамалары мен қосымшаның арасындағы тасымалдау деңгейінде орналасқан.

**TCP негізгі функциялары**

1. Негізгі деректерді беру. TCP модулі деректердің үздіксіз ағындарын екі бағытта да жібереді. Бұл TCP ағыны октеттер ағыны ретінде қарастырылады. TCP деректерін жіберу үшін IP модулін шақырып бұл ағынды бөліктерге (дейтграммалар) бөледі.

2. Сенімділікті қамтамасыз ету. TCP модулі мәліметтердің реттілігін бұзудан, жоғалудан, қайталанудан және бұзудан қорғауды қамтамасыз етеді. Ол үшін барлық октеттер өсу ретіне қарай нөмірленеді. Әр сегменттің тақырыбында октеттер саны және бірінші октеттің сериялық нөмірі бар. Одан кейін әрбір сегментте мәліметтердің бүлінуі тексерілетін тексеру мәні бар болады (2.6 сурет).

3. Арналарды бөлу. TCP хаттамасы бірнеше қосылыстардың бір уақытта жұмыс істеуіне мүмкіндік береді. Сондықтан TCP сегментінің тақырыбында порт нөмірлері бар. Барлық жалпы Интернет қызметтерінде стандартты порт нөмірлері бар. Мысалы, электрондық пошта - 25, FTP - 21, т.б. IP мекенжайы мен порт нөмірінің жиынтығы сокет деп аталады. Сокет Интернеттің қолданбалы процесін ерекше анықтайды.

4. Қосылысды басқару. Қосылыс дегеніміз - деректер ағынының жай-күйі, соның ішінде сокеттерді, жіберілген нөмерлерді, қабылданған және расталған октеттер санын, терезе өлшемдері туралы ақпарат жиынтығы.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |
| Source Port | | | | | | | | | | | | | | | | Destination Port | | | | | | | | | | | | | | | |
| Sequence Number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Acknowledgment Number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Data Offset | | | | Reserved | | | | | | U R G | A C K | P S H | P S T | S Y N | F I N | Window | | | | | | | | | | | | | | | |
| Checksum | | | | | | | | | | | | | | | | Urgent Pointer | | | | | | | | | | | | | | | |
| Options | | | | | | | | | | | | | | | | | | | | | | | | Padding | | | | | | | |
| Data | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

2.6 сурет – TCP тақырып түрі.

Назар аударыңыз, мұнда әр белгі тиісті биттің орнын көрсетеді.

Source Port (жіберушінің порты)16-биттік порт жіберуші порт нөмірі

Destination Port (алушының порты) 16 биттік алушының порт нөмірі

32 биттің Sequence Number (кезек нөмір). Осы сегменттегі деректердің бірінші октетіне арналған кезек нөмірі (SYN синхрондау жалаушасы болмаса). Егер SYN жалаушасы болса, онда кезек нөмірі инициализацияланған (ISN), ал бірінші мәліметтер октетінің нөмірі -ISN + 1 болады.

32 биттің Acknowledgment Number (растау нөмірі). Егер ACK тексеру биті орнатылса, онда бұл өрісте осы датаграмманы жіберуші қарсы бағытта алғысы келетін келесі кезек нөмірі болады. Растау нөмірлері байланыс орнатылғаннан кейін үздіксіз жіберіледі.

4 биттің Data Offset (деректердің араласуы).

Деректер офсеті 4 бит. TCP тақырыбындағы 32 биттік сөздер саны. Деректер өрісінің басталуын көрсетеді. TCP тақырыбы әрдайым 32 биттік сөз шекарасында аяқталады, тіпті егер ол опцияларды қамтыған жағдайда да.

6 бит Reserved. Бұл сақтық көшірме өрісі нөлдермен толтырылуы керек.

Control Bits (бақылау биттері) 6 бит. Бұл өрістің биттері солдан оңға қарай.

|  |  |
| --- | --- |
| URG: | жедел көрсеткіш өрісі қосылған |
| ACK: | растау өрісі қосылған |
| PSH: | итеру функциясы |
| RST: | осы байланысты қайта қосыңыз |
| SYN: | кезек нөмірін синхрондау |
| FIN: | басқа деректер жіберілмейді |

Window (терезе) 16 бит. Растау жолында нөмірі көрсетілген октеттен басталатын мәліметтердің октет саны. Осы сегментті жіберуші күткен октеттер саны.

Checksum (бақылау суммасы) 16 бит. Бақылау суммасы – бұл 16 биттік барлық тақырыптар мен мәтін сөздерінің қосындысы. Егер сегментте бақылау суммасының есебіне кіретін тақырып пен мәтінде октет тақ саны болса, онда 16 биттік сөзді құру үшін оң жақтағы соңғы октет нөлдермен толтырылады. Осы түзету нәтижесінде пайда болған октет желі арқылы сегментпен бірге берілмейді. Бақылау суммасын есептемес бұрын, осы бақылау суммасының өрісі нөлдермен толтырылады.

Urgent Pointer (жедел көрсеткіш) 16 бит. Бұл өріс жедел көрсеткіштің ағымдағы мәнін хабарлайды. Соңғысы оң мән – бұл сегменттің кезек санына қатысты орнын толтыру. Шұғыл көрсеткіш жедел мәліметтерден кейін октеттің кезек нөмірін хабарлайды. Бұл өріс URG бақылау биті сегментте орнатылған кезде ғана түсіндіріледі.

Options (опция) айнымалы ұзындық. Опциялар TCP тақырыбының соңында орналасуы мүмкін, ал олардың ұзындығы 8 биттен тұрады. Бақылау суммасын есептеу кезінде барлық параметрлер ескеріледі.

Padding (түзету) айнымалы ұзындық. TCP тақырыбын түзету TCP тақырыбының аяқталуын және сегменттік деректер өрісінің 32 биттік шекарадан басталуын қамтамасыз ету үшін түзетіледі. Түзету нөлдермен орындалады.

***Байланысты орнату тәртібі***

TCP хаттамасын қолданатын серіктестердің өзара әрекеті үш кезеңнен тұрады:

- логикалық байланыс орнату;

- мәліметтермен алмасу;

- байланысты жабу.

Қосылымды орнату кезеңі «үш жақты қол алмасу» (three-way handshake) түрінде жүзеге асырылады. 1) TCP А модулі тұтынушының рөлін атқара отырып, TCP B модуліне SYN жалаушасы және мәліметтер тізбегіндегі нөмірдің бастапқы мәні бар пакет жібереді. 2) TCP модулі В, өз кезегінде, байланыс орнатуға дайын бола отырып, TCP пакетімен жауап береді және сұраныстың дұрыс қабылданғанын және байланыс орнатуға дайын екендігі туралы хабарлайды; 3) Үшінші қадамда TCP модулі А, TCP пакеті В дұрыс қабылдағанын растайды.

TCP хаттамасы бір жағынан қолданушымен немесе қолданбалы бағдарламамен, екінші жағынан Internet хаттамасы сияқты төменгі деңгейдегі хаттамамен байланысады. Қолданбалы процесс пен TCP хаттамасы арасындағы интерфейсін қолайлы егжей-тегжеймен түсіндіреміз. Бұл интерфейс файлдарды басқаруға арналған қосымшалар процесінде қарастырылған операциялық жүйелік қоңырауларға ұқсас қоңыраулар жиынтығынан тұрады. Мысалы, бұл жағдайда байланыстарды ашуға және жабуға, орнатылған байланыстар туралы мәліметтерді жіберуге және алуға шақырулар болады. TCP хаттамасы қосымшалармен асинхронды түрде әрекеттесе алады деген болжам бар. TCP хаттамасын жасаушыларға белгілі бір амалдық жүйенің қасиеттеріне сәйкес келетін интерфейстерді құруда айтарлықтай еркіндік берілгенімен, TCP хаттамасы мен қолданушы арасындағы интерфейстің қажетті минималды функциялары қажет.

***Сырғымалы терезе механизмі***

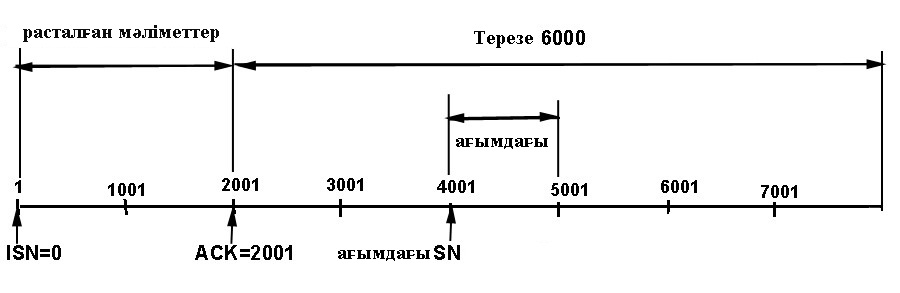
Байданысты орнату арқылы сенімді деректерді берудің кең тараған жалпы түрінде, пакеттер алушы тарапқа олар берілген тәртіпте жеткізілуі керек. Бұл мәселенің қарапайым шешімі – әр егменттің деректерді қабылдағандығы туралы алушы растауын қолдану.

Алайда, егер жіберуші әр сегментті жібергеннен кейін растауды күтуге мәжбүр болса, онда осы әдіс кезінде берілу жылдамдығы айтарлықтай төмендейді. Растауды алуды қажет етпей, жіберушіге жіберуге рұқсат етілген деректер пакеттері терезе деп аталады.

TCP хаттамасында күтілетін растау қолданылады; олар келесі күтілетін октеттің санын қамтиды. Сырғымалы терезенің механизмі TCP сеансы кезінде терезенің өлшемін үйлестіру динамикалық түрде жүреді. Сырғымалы терезе механизмі - бұл деректердің белгілі бір көлемін жібергеннен кейін қабылдаушыдан жіберушіден растауды талап ететін мәліметтер ағынын басқару механизмі.

Екі құрылғы арасында берілетін мәліметтер ағынын басқару үшін TCP хаттамасында ағынды басқару механизмі қолданылады. Терезе ағымдағы растау нөмірінен есептелген октет санын анықтайды, оны TCP құрылғысы белгілі бір уақытта ала алады.

Мысалы, 2.7 суретте терезе 6000 байтқа тең. Бұл деректер алушыға беріледі. Жіберуші алушыдан растауды күтуі керек. Осыдан кейін ол келесі мәліметтер терезесін жібере алады. TCP терезесінің өлшемі екі желілік құрылғылар арасында деректер ағынын беру кезінде өзгеруі мүмкін. Қабылдаушыдан жіберілген әрбір растау алушының алатын байт саны туралы ақпаратты қамтиды. Терезенің үлкен өлшемі бір уақытта көп мөлшердегі октерді жіберуге мүмкіндік береді.



2.7 сурет – Сырғымалы терезе механизмі

2.2.3 UDP хаттамасы

Пайдаланушы дейтаграммасының хаттамасы UDP (User Datagram Protocol) – бұл транспорттық деңгейдің хаттамасы және IP желіаралық хаттаманы қамтамасыз ететін мүмкіндіктерге негізделген. UDP негізгі мақсаты – желіде мәліметтердің «жылдам» берілуін қамтамасыз ету.

Оның негізгі ерекшеліктері төменде келтірілген:

-логикалық (виртуалды) байланыс орнатылмаған режимде өзара әрекеттесуді жүзеге асырады;

-мәліметтерді берудің блоктық (дейтаграммалық, пакеттік) түрін ұйымдастырады;

-транспорттық деңгейде байланыс серіктестерін анықтау үшін 16-биттік «порт нөмірлерін» қолданады;

- деректердің сенімді жеткізілуіне кепілдік бермейді (UDP пакеттерінің жоғалуы да, олардың қайталануы да мүмкін);

- UDP пакеттің мекенжайын қабылдаған кезде оның дұрыстығы / дұрыс еместігі туралы хабарлау мүмкіндігі жоқ;

- UDP пакеттерін алушыға дұрыс жеткізудің тәртібі қамтамасыз етілмеген;

- UDP пакетіндегі мәліметтердің тұтастығына бақылау суммасын қолдану арқылы кепілдік бере алады;

- өте қарапайым (TCP хаттамасымен салыстырғанда).

Айта кету керек, іс жүзінде IP желіаралық деңгейдегі хаттама құралдарының қолданбалы бағдарламасы үшін UDP транспорттық деңгейінің хаттамасы интерфейс рөлін атқарады. 2.8 суретте UDP пакет тақырыбының түрі көрсетілген.

|  |  |
| --- | --- |
| 0 15 | 31 |
| Бастапқы порт | Қабылдағыш порт |
| Ұзындығы | Бақылау суммасы |
| Деректер октеті | |

2.8 сурет – UDP хаттамасының дейтаграммалар үшін тақырып түрі.

Бастапқы порт және қабылдағыш порты – порт нөмірлерінен тұратын 16-биттік өрістер, сәйкесінше UDP пакетінің мекенжайы мен бастапқы көздер болып табылады.

Ұзындығы – тақырыпты және деректерді қосқанда, бүкіл UDP пакеттің ұзындығын (байтпен) қамтитын 16 биттік өріс.

Бақылау суммасы – UDP тақырыбы үшін есептелген, Internet бақылау суммасы бар 16 биттік өріс.

UDP хаттамасында сырғымалы терезе механизмін пайдаланбайды, сондықтан деректерді беру сенімділігі қосымша деңгейі хаттамасымен қамтамасыз етілуі керек. UDP хаттамасы тапсырыс берілген сегменттерді бірге қосудың қажеті жоқ қосымшалар үшін жасалды.

UDP хаттамасы осындай қызметтермен және жоғарғы деңгейдегі хаттамалармен қолданылады:

- TFTP (Trivial File Transfer Protocol) – файлдарды жіберудің қарапайым хаттамасы;

- SNMP (Simple Network Management Protocol) – желіні басқарудың қарапайым хаттамасы;

- DHCP (Dynamic Host Configuration Protocol) – түйіннің динамикалық конфигурациялау хаттамасы;

- DNS (Domain Name System) – домендік атаулар қызметі.

2.2.4 TCP және UDP хаттамаларының порт нөмірлері

TCP және UDP хаттамаларының деректерді жоғарғы деңгейге жіберу үшін порт нөмірлерін қолданады. Порт нөмірлері желіде бір уақытта болатын түрлі әрекеттесулерді бақылау үшін қолданылады.

Қолданбалы бағдарламаларды қамтамасыз етуді жасаушылар мен Internet Assigned Numbers Authority (IANA) хаттамаларының бірегей параметрлері мен атауларын ерекшелеу бойынша агенствоны басқарушы белгілеуімен арқылы басқаратын резервтік порт нөмірлерін пайдалануға келісті. Белгілі порт нөмірі бар, қосымшалармен байланыссыз желілік өзара әрекеттесулер порт нөмірін өздігінен береді, бірақ олар белгілі бір мәндер диапазонынан таңдалады - 1023-тен жоғары. 5 кестесінде жиі қолданылатын TCP және UDP хаттамаларының порт нөмірлері берілген.

Алушының порт нөмірі соңғы түйінді қолданатын бағдарламаға сәйкес келеді. Жіберуші портының нөмірі – әдетте жіберуші түйінмен динамикалық түрде тағайындалған, 1023-тен асатын нөмір. Мысалы, түйін FTP арқылы байланысады, қабылдағыштың 21 (FTP) портының нөмірін көрсететін пакеттерді жібереді және 1028 жіберушінің порт нөмірін динамикалық түрде қалыптастырады. Мұндай порттардың жұбы (жіберуші және қабылдағыш) түйіндердің өзара әрекеттесуінің бірегейлігін анықтайды. Егер дәл сол түйін үшінші түйінменн FTP байланысын бастаса, алушы порты 21-ге тең болады, бірақ жіберуші порты екі байланыс сеансын бөлу үшін алдыңғыдан (мысалы, 1030) ерекшеленеді.

5 кесте Сақталған TCP және UDP хаттамалар портының нөмірлері

|  |  |  |
| --- | --- | --- |
| Порт нөмірі | Құпия сөздер | Сипаттамасы |
| 0 | - | Сақталған |
| 1-4 | - | Белгіленбеген |
| 5 | Rje | Жұмысты қашықтан орындау |
| 7 | Echo | Эхо |
| 9 | Discard | Сегментті жою |
| 11 | Users | Белсенді пайдаланушылар |
| 13 | Daytime | Уақыт |
| 15 | Netstat | Белсенді байланыстар немесе желі статистикасы |
| 17 | Quote | Күн халамалары |
| 19 | Chargen | Таңба генераторы |
| 20 | ftp-data | FTP хаттамасы (мәліметтер) |
| 21 | ftp | FTP хаттамасы (басқару) |
| 23 | telnet | байланыс |
| 25 | Smtp | Пошталық хабарламалардың берілуінің (SMTP) қарапайым хаттамасы |
| 37 | Time | Тәулік уақыты |
| 39 | Rlp | Ресурстарды орналастыру хаттамасы(RLP) |
| 42 | Nameserver | Атау қызметі |
| 43 | nickname | Пайдаланушы атаулар қызметі |
| 53 | Domain | Домен атауларының қызметі (DNS) |
| 67 | Bootps | Бастапқы жүктеме хаттамасының қызметі |
| 68 | Bootpс | Бастапқы жүктеме хаттамасының тұтынушысы |
| 69 | Tftp | TFTP хаттамасы |
| 75 | - | Телефон желісі бойынша сыртқы жүйелерге кез-келген жеке қызмет байланысы |
| 77 | - | Тапсырмамен қашықтықтан басқарудың кез-келген жеке қызмет байланысы |
| 79 | Finger | Желідегі белсенді тұтынушыларды анықтау қызметі |
| 80 | HTTP | Гипермәтінді беру хаттамасы |
| 95 | SUPDUP | SUPDUP хаттамасы |
| 101 | HOTNAME | Түйін атауы қызметі |
| 102 | ISO-TSAP | ISO-TSAP хаттамасы |
| 113 | AUTH | Аутентификация қызметі |
| 117 | UUCP-PATH | UUCP маршрут қызметі |
| 123 | Ntp | Уақытты синхрондау хаттамасы (NTP) |
| 133-159 | - | Белгіленбеген |
| 160-223 | - | Сақталған |
| 224-241 | - | Белгіленбеген |
| 242-255 | - | Белгіленбеген |



**Тексеру жұмысы №3**

**№1 жаттығу Сөйлемді аяқтаңыз:**

А бағанынан сөйлемнің басын В бағанынан ең қолайлы соңымен салыстырыңыз. Параметрді таңдап, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір затты тек бір рет пайдалануға болады.

|  |  |
| --- | --- |
| **Баған А** | **В бағаны** |
| 1. TCP/IP пакет \_\_\_\_ 2. IP хаттама \_\_\_\_\_ 3. IP мекенжайы\_\_\_\_\_\_ 4. ТСР хаттамасы\_\_\_\_\_\_\_\_ 5. ARP хатамасы\_\_\_\_\_\_\_\_ 6. UDP хаттамасы \_\_\_\_\_\_\_ 7. OSPF\_\_\_\_\_\_\_\_ | A. Байланыссыз мәліметтерді беруге арналған хаттама  Б. Арналар жағдайын қолданатын маршруттау алгоритмі (link-state). OSI ішіндегі домендік бағыттау хаттамасының негізінде жасалған.  B. IP мекенжайы бойынша аппараттық құралдың мекен-жайын анықтауға арналған хаттама  Г. Аппараттық құралдың мекен-жайын бойынша IP мекенжайы анықтауға арналған хаттама  D. Біртұтас жұмыс істейтін хаттамалар тобы және төрт деңгейлі модельді қолдайды  E. Деректерді бір желіден екінші желіге жіберуге және байланыс орнатуға арналған хаттама  Ж. Процестер арасындағы сенімді тікелей байланысты қамтамасыз ету үшін хаттама  З. TCP/IP түйінін бірегей түрде анықтайтын сан |

**№2 жаттығу Дұрыс жауапты таңдаңыз**

1. В класының желісі қанша түйінге қолдау көрсетеді

а) 65534

б) 254

в) 2097152

г) 16384

2. TCP / IP деген не? (ең жақсы жауапты таңдаңыз)

a) Microsoft корпорациясы қарапайым пайдаланушыларға Интернеттегі ресурстарға қол жеткізуге мүмкіндік беру үшін әзірлеген хаттамалардың жиынтығы

б) әртүрлі аппараттық платформаларда және әртүрлі типтегі желілерде жұмыс істейтін әртүрлі қосымшалармен өзара әрекеттесуге мүмкіндік беретін хаттамалар жиынтығы

в) әр текті желілер арасында ақпаратты бағыттау үшін Microsoft жасаған хаттама

г) IAB әртүрлі бағдарламалық жасақтама мен аппараттық құрал өндірушілері Интернетке қол жеткізе алатындай етіп жасалған хаттама.

3. Жергілікті желідегі адресті анықтаған кезде кэшті тексергеннен кейін компьютер не істейді?

а) маршрутизаторға сұраныс жібереді

б) ARP серверіне сұрау жібереді

в) HOSTS файлына жатады

г) кең таралымды сұраныс жібереді

4. TCP/IP моделінің қай деңгейінде UDP хаттамасы? (ең жақсы жауапты таңдаңыз)

а) желілік интерфейс деңгейінде

б) желілік деңгейінде

в) көлік деңгейінде

г) қосымша деңгейінде

5. ARP кэш жазбасы қанша уақытқа созылады?

а) 10 минут

б) 20 минут

в) 5 минут

г) 1 минуту

6. Төмендегі тұжырымдардың қайсысы сокетті ең жақсы сипаттайды?

a) Қашықтағы тораптағы процестің орналасқан жерін көрсетуге арналған сан

б) қашықтағы түйінде процестің орналасқан жерін көрсету үшін пайдаланылатын порт нөмірі

в) Сервер құратын кездейсоқ сан, бұл қосымшаларға қашықтағы түйіндегі процеске қол жеткізуге мүмкіндік береді

г) қашықтағы түйінде қосымшаны немесе қызметке кіруді қамтамасыз ету үшін пайдаланылатын порт нөмірі мен IP мекен-жайының тіркесімі

7. Төмендегі жауаптардың қайсысы ARP функцияларын дұрыс сипаттайды?

а) NetBIOS атауларының сәйкес IP мекенжайларын анықтау

б) желіге пакеттерді жіберу

в) биттерді байтқа түрлендіру

г) IP мекенжайларына сәйкес келетін аппараттық құралдарды анықтау

8. Ішкі желі маскасының ерекшеліктерін сипаттайтын жауапты таңдаңыз

a) Желілік маска TCP/IP желісіндегі IP мекенжайының бір бөлігін жасыру үшін қолданылады

б) ішкі желі маскасы басқа TCP/IP түйіндерінің орналасуын анықтауға мүмкіндік береді

в) ішкі желі маскасы TCP/IP хост идентификаторынан желі идентификаторын анықтауға көмектесу үшін қолданылады. Бұл басқа TCP/IP түйіндерін табуға көмектеседі.

г) Ішкі желі маскасы TCP/IP желі идентификаторын түйін идентификаторынан бөлуге көмектесу үшін қолданылады. Бұл басқа TCP/IP түйіндерінің IP мекенжайларын анықтауға көмектеседі.

9. Егер тағайындалған мекен-жайы белгісіз болса, деректер қайда жіберіледі?

a) Бағыттау кестесіндегі бірінші желілік мекен-жайға

б) Маршрутизатор кэшіне

в) шлюзге

г) RIP түйініне

10. Неліктен RIP бағыттау хаттамасында 15 ретрансляция максималды ұзындықтағы жолдар жүреді?

а) маршруттау кестесінде таратудың санын сақтау үшін он алтылық код қолданылады

б) шексіз циклдердің пайда болуына жол бермеу

в) үлкен желілер ішкі желіге бөлінетін ету үшін

г) үлкен ұзындықтығы маршруттарды пайдаланатын желілер жоқ

**№3 жаттығу Мәлімдемені растаңыз немесе жоққа шығарыңыз**

Келесі сөйлемдерден Иә немесе Жоқ таңдаңыз.

1. Тек NetBIOS пайдалану үшін қалпына келтірілген Windows NT Server түйіні үшін бірегей TCP/IP мекенжайы қажет емес. Иә. Жоқ.

2. Түйіннің орналасу мекен-жайына қарамастан қосалқы желілерге бөлу IP мекен-жайын еркін тағайындауға мүмкіндік береді. Иә. Жоқ.

3. Утилит route көмегімен маршруттау кестесіне жаңа жолдар қосуға болады. Иә. Жоқ.

4. Әдетте, жүйені қайта жүктегеннен кейін жаңадан анықталған жолдар маршруттау кестесінде сақталады. Иә. Жоқ.

5. Жөнелтуші мен қабылдағыштың аппараттық мекен-жай пакеті шлюз арқылы өткен сайын өзгереді. Иә. Жоқ.

6. OSPF желілік аз жүктеме тудырады, едәуір үлкен желілерді қолдайды, сөзі аз және жіберуші мен тағайындалған түйін арасындағы бірнеше жолды қолдайды. Иә. Жоқ.

7. ICMP TCP/IP анықтамалық моделініңжеліаралық деңгейінде орналасқан. Иә. Жоқ.

8. Келесі мәлімдеме қосылудың ашылу сатысын сипаттайды: «Жоқ, мен қазір бос емеспін, менде сізге уақыт жоқ, бірнеше минуттан кейін қайталап көріңіз.» Иә. Жоқ.

9. IP TCP/IP хаттамалар тобының шлюз деңгейінде орналасқан. Иә .Жоқ.

10. Динамикалық маршруттау жағдайында маршруттау кестелері қолмен қолданылады. Иә. Жоқ.

**№ 4 Қолданбалы тапсырмалар**

1. Бастапқы шарттар: Фирма 9 бөлімшеден тұрады, олардың әрқайсысы өзінің ішкі желісін қажет етеді. Фирма 130.121.0.0 желі идентификаторын алды. Құрылғыдағы 3000 түйінге дейін қолдауды қажет етеді. Қандай қосалқы желі маскасын қолдануды ұсынар едіңіз?

Сіздің шешіміңіз. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Сіз Windows NT Server-де TCP / IP қолдауын орнатқыңыз келеді. Сізге не орнату керек? (Барлық дұрыс жауаптарды көрсетіңіз).

a) Сіз орнатқан компьютердегі жергілікті әкімшілер тобының мүшесі болуыңыз керек

б) Сіз жеке компьютер орнатылған доменнің әкімшісі болуыңыз керек

в) Жүйені таратуға рұқсатыңыз болуы керек

г) Сіз қандай параметрлерді жасау керектігін жақсы түсінуіңіз керек.

3. ARP кэшінен статикалық жазбаны қалай жоя аламын? (Барлық дұрыс жауаптарды көрсетіңіз).

а) көмпьютерді өшіру

б) осы жазба үшін **arp-а** командасын іске қосыңыз

в) кең таратылған хабарламадан алынған ақпарат пен жазба арасындағы қарама-қайшылық кезінде жазба жойылады

г) осы жазба үшін **arp-d** командасын іске қосыңыз

4. Сіздің ішкі желіңізде 3 ішкі желі бар. Сіз А қосалқы желіде DNS қызметін қалпына келтірдіңіз, бірақ бұл сәтсіздікке ұшырайды, нәтижесінде бүкіл желідегі атаудың рұқсат етуі жұмыс істемейді. Болашақта бұған жол бермеу үшін не істеу керек?

## 2.3. Қолданбалы деңгейдің хаттамалары

OSI және TCP/IP модельдерінің соңғы деңгейі қосымша деңгейі болып табылады. Бұл пайдаланушыларға ең жақын. Тұтынушы-қызмет қосымшалары, домендік атаулардың қызметтері, түрлі желілік қосымшалар және көптеген басқа қызметтер (тұтынушы-қызмет технологиялары; домендік атау жүйесі; электрондық пошта; Telnet қызметі; FTP хаттама қызметтері мен тұтынушылары; HTTP хаттамалары) қосымшалар деңгейіне тәуелді.

2.3.1 DHCP хаттамасы

***DHCP хаттамаға шолу жасау***

DHCP (Dynamic Host Configuration Protocol) – бұл желілік қызмет және қолданбалы деңгей хаттамасы. TCP/IP, желілік әкімшілерге бекітілген IP мекенжайын қажет етпейтін жұмыс станциялары, жұмыс үстелі және басқа клиенттік машиналар үшін IP мекенжайларының топтарын таратуға және басқаруға серверлерді қалпына келтіруге мүмкіндік береді. Ұйымдар өсіп, басқаруды қажет ететін компьютерлердің саны өскен сайын, DHCP тез сәнді зат болудан бас тартып, қажетті құралға айналады.

Майкрософт әрдайым DHCP-ге қомақты қаржы салды, өйткені оны көптеген жүйелер үшін IP қалпына келтіруде басқарудың негізгі құрамдас бөлігі ретінде қарастырды. DHCP қызметтері IP мекенжайларының бір немесе бірнеше ауқымын басқаруға қабілетті, олардың әрқайсысын мекенжай пулы немесе мекен-жай аймағы деп атауға болады. Әрбір жеке IP-адрес аймағында DHCP қызметі клиенттік машиналар арасында таратылмауы керек жеке мекен-жайларды немесе мекенжайлар жиынтығын бөле алады. Бұл DHCP-ге IP-мекен-жайлардың бірнеше ауқымын үйлестіруге мүмкіндік береді, олардың кейбіреулері маршрутизаторлар мен қызметтерге белгіленген болуы мүмкін. Клиенттердің өтініші бойынша DHCP қызметі қалған белгіленбеген мекенжайларды тарата алады, және мұндай тапсырмалардың әрқайсысы мекен-жайларды ерекшелеу немесе жай ерекшелеу деп аталады.

2.3.2 Желіге DHCP хаттамасын орнату

Желілік жобалардың көпшілігі IP хаттамалары негізінде жасалады. Осы хаттамамен жұмыс істеу үшін барлық компьютерлер сәйкесінше қалпына келтірілген болуы керек. Желідегі компьютерлердің саны көп жағдайында IP қалпына келтірудегі қателіктердің ықтималдығы артып, қалпына келтіру мен басқару уақыты артады. Жобаның негізгі мақсаты – ұйымның жеке желісіндегі барлық компьютерлерде дұрыс IP қалпына келтіруін қамтамасыз ету. Жобаны құрмас бұрын әр компьютерде IP қалпына келтіру әдісін анықтау керек. Бұл үшін бірнеше әдістер дайындалды:

a) файлдық қызметтерге, баспа қызметтеріне, маршрутизаторларға, шлюздерге және клиенттерге ресурстар мен тұтынушыға қызмет көрсететін басқа желілік құрылғыларға қолмен қалпына келтіру қолайлы. Автоматты IP конфигурациясы желілік ресурстарды басқармайтын компьютерлерде, мысалы жұмыс үстелі компьютерлері сияқты үшін қолданылады. Бұл қалпына келтіру қателіктерін азайтады және әкімшілік үстеме шығындарды азайтады.

б) үшінші тараптың операциялық жүйелерінің DHCP қызметтері. DHCP сервері Novell Netware және Unix сияқты көптеген заманауи операциялық жүйелердің бөлігіне кіретін болып табылады.

в) Windows жүйесінің құрамындағы DHCP қызметтері. Әр түрлі операциялық жүйемен тұтынушыларға қолдау көрсете алады. Олар келесі жағдайларда қолданылады:

- Windows 2000 – бұл кәсіпорынның стандарты;

- рұқсат етілмеген DHCP серверлерінен туындаған қалпына келтіру қателерін болдырмау қажет;

- Active Directory қызметін каталог қызметі ретінде пайдалану керек;

- DNS серверлерімен және RRAS қызметімен біріктіруді қажет етеді.

Автоматты IP конфигурациясы кез-келген желілік қызметтер жобасының маңызды бөлігі болып табылады. Жобаның сәттілігі немесе сәтсіздігі көбінесе оны қолдауға қажетті ресурстарға байланысты. Сондықтан, IP конфигурациясындағы қателіктердің ықтималдығын азайту және басқару уақытын қысқарту жобаның құнын айтарлықтай арттырады. Бұл нәтижеге жетудің бір әдісі – IP-ны автоматты түрде конфигурациялау. DHCP – бұл компьютерлердің IP конфигурациясын автоматты түрде теңшеуге мүмкіндік беретін салалық стандартты хаттама. Windows DHCP қызметі үш құрамнан тұрады:

a) DHCP тұтынушысы Windows-да IP хаттамасын енгізудің ажырамас бөлігі болып табылады. Ол DHCP серверінен алынған IP параметрлеріне сәйкес компьютер конфигурациясын өзгертеді және кез-келген амалдық жүйенің бөлігі болып табылады.

б) DHCP сервері – IP параметрлерін DHCP клиенттеріне тағайындайды. Бұл тұрақты Windows қызметі. Ол өзінің IP адрестерінің жергілікті деректер қорын басқарады.

в) DHCP ретрансляция агенті – RRAS қызметінің құрамдас бөлігі болып табылатын хаттама. Ол DHCP хабарламаларын роутер арқылы жіберуді қамтамасыз етеді. Ретрансляция агенті бар компьютерге тіркелген IP мекен-жайы берілуі керек. Бір компьютерге DHCP серверін және ретрансляция агентін орнатуға болмайды.

2.3.3 DHCP хаттамасының функциялары және конфигурациясы

1) Автоматты IP конфигурациясын қажет етушілер үшін сегменттерді анықтаңыз.

Автоматты IP конфигурациясы желінің барлық сегменттерінде қолданылуы керек, тек:

- желілік ресурстарды басқаратын компьютерлер ғана болатын желі сегменттері. Файлдық серверлер, баспа серверлері, дерекқор серверлері және веб-серверлер сияқты желілік ресурстарды басқаратын компьютерлерде тіркелген IP мекенжайлары болуы керек. Олар қолмен тағайындалады.

- тіректі желілермен басқа да сегменттерді қосатын тек маршрутизаторлардан тұратын тіректі сегменттер.

- жаһандық (WAN) желілер арқылы қосылатын сегменттер. WAN қосылымының өткізу қабілеттілігін сақтау үшін оны қажетсіз трафикпен артық жүктемеу керек.

- қосалқы желілерден қорғалған. Олар тек нақты пайдаланушыларға қол жетімді ресурстардан тұрады. Қауіпсіздік мақсатында DHCP серверлері қорғалған қосалқы желілерде орналаспаған.

Басқа жағдайларда, жұмыс үстелінің компьютерлері үшін автоматты IP конфигурациясын пайдалануға болады.

2) Автоматты IP-баптау әдісін анықтау. Автоматты IP конфигурациясын қамтамасыз ету үшін әр желі сегменті үшін сіз әдістердің бірін таңдауыңыз керек:

а) DHCP сервері. Әрбір географиялық сегментте кемінде бір DHCP сервері болуы керек. Бір DHCP сервері 15000 санын ұстай алады. Қосымша серверлерді, әдетте, қол жетімділік пен өнімділікті арттыру үшін орнатады.

б) DHCP ретрансляция агенттері. Олар DHCP серверіне тікелей қосылмаған сегменттерде орнатылады. Олар кең таралымды пакеттерді алады, сұраныстарды бір мекен-жайлы пакеттерге аударады және оларды нақты DHCP серверіне жібереді. Бір агент 1000 компьютер тұтынушысын қолдайды.

в) Маршрутизаторда DHCP/BOOTP қайта жіберуді қосу. BOOTP – Bootstrap Protocol - жүктеу протоколы - жүктелу кезінде желіге қол жетімділік пен операциялық жүйенің кескінін алуға мүмкіндік беретін дискісіз жұмыс станцияларын ұсынады. DHCP/BOOTP қайта жіберу DHCP серверіне тікелей қосылмаған желілік сегменттердегі маршрутизаторларда қосылады. Ол тек DHCP тарату трафигін беру арқылы таратылатын трафикті азайтады. Бұл әдістің басты артықшылығы – қосымша жабдық немесе бағдарламалық жасақтама сатып алудың қажеті жоқ.

3) DHCP аймағын және олардың параметрлерін анықтау. Аймақ – бұл DHCP сервері басқаратын IP мекенжайларының аймағы. Windows жүйесінде DHCP енгізудің ерекшелігі – DHCP серверінің бірнеше аймағын біріктіретін кушті аймақтардың болуы. Олар жобада қолданылады, егер:

- DHCP/BOOTP қайта бағыттау арқылы ретрансляция агенттері немесе маршрутизаторлар арқылы IP параметрлерін алатын желілік сегменттерге қолдау қажет;

- қолданыстағы диапазондары таусылған сегменттер үшін IP мекенжайларының қосымша аймағын ұсыну қажет;

- қолданыстағы IP-мекен-жай сұлбасын және қосалқы желі маскаларын сақтау кезінде бірнеше ішкі желілерді бір-біріне біріктіру қажет.

Аймақ үшін сіз жалға алу мерзімін – IP мекенжайын қайта тағайындауға рұқсат етілетін уақыт кезеңін көрсетуіңіз керек. Ол компьютерлердің қозғалыс жиілігіне байланысты орнатылады. Егер жиі болса, онда ұзақтығы қысқа болады. Егер сирек кездесетін болса, онда ұзағырақ. Аймақ параметрлері – DHCP тұтынушыларының конфигурациясын анықтайды. Қолмен тағайындалған IP мекенжайларын DHCP аймағынан шығару керек. Бұл:

- IP маршрутизаторлары;

- брандмауэрлер;

- серверлер (файл, басып шығару, қосымшалар);

- шлюздер;

- кез келген операциялық жүйелер немесе DHCP көмегімен конфигурацияланбайтын құрылғылар.

DHCP аймағының параметрлерінде IP тұтынушыларының конфигурация ерекшеліктерін көрсету керек:

- маршрутизаторлар;

- DNS серверлері;

- DNS домен атауы;

- WINS торабының түрі;

- WINS сервері.

DHCP әкімшісі басқаруға қол жетімді DHCP аймағының параметрлерін анықтауға мүмкіндік болады (сонымен қатар құра аласыз, өзгерте және жоя аласыз). DHCP тұтынушыларының әр түрлі деңгейлері немесе деңгейлері үшін әр түрлі DHCP параметрлерін тағайындауға болады. Әр түрлі деңгейдегі аймақ параметрлерін тағайындау себептері:

|  |  |
| --- | --- |
| Деңгейі | Тағайындау себебі |
| Сервер параметрлері | Параметрлер DHCP серверінің барлық аймақтары үшін жарамды. Осы деңгейде параметрлерді тағайындау кезінде сақ болу керек, өйткені бұл параметрлер осы DHCP серверінің барлық тұтынушыларының келтірулеріне әсер етеді. |
| Аймақтың параметрлері | Барлық DHCP тұтынушылары үшін жарамды. DHCP аймағымен анықталған IP мекенжайлары (желілік сегмент) ауқымындағы параметрлер аймақ параметрлері. |
| Кластық параметрлер | DHCP тұтынушыларының белгілі бір санатына арналған параметрлер. Белгілі бір критерийлер негізінде DHCP тұтынушыларын ерікті түрдегі кластарға топтастыра аласыз. Мысалы, Windows басқаруымен DHCP тұтынушыларына арналған класс. Бұл класс үшін тек Windows-те орнатылған арнайы параметрлерді тағайындауға рұқсат етіледі. |
| Тұтынушы параметрлері | Жеке тұтынушылық компьютерлер үшін аймақ параметрлері. Мысалы, WINS түйіннің белгілі бір түрі ұйымдағы бір ғана компьютерге арналған. |

4) DHCP бар жобаларда конфигурацияны қорғау. IP конфигурациясының тұтастығын қамтамасыз ету DHCP көмегімен жобаны құру кезіндегі маңызды міндет болып табылады. Сонымен қатар, DHCP тұтынушыларын автоматты түрде конфигурациялайтын ұйымның кез-келген сыртқы DHCP серверлері тұтынушылық компьютерлердің IP-конфигурациясында қателіктер мен сәйкессіздіктерді тудыруы мүмкін, нәтижесінде желілік қосылыстарды бұзуы мүмкін. Бұл жағдайда қорғау әдісі - рұқсат етілмеген DHCP серверлерінің пайда болуын болдырмау.

Егер желіде бір DHCP сервері болса:

a) DHCP сервер қызметі DHCPINFORM сұранысын жергілікті ішкі желіге жіберіп, DHCP серверлерінен Active Directory түбірлік домені туралы ақпарат алуға тырысады. Бұл сервер жалғыз болғандықтан, ол сұрауға жауап алмайды.

б) жауап алмағаннан кейін DHCP серверінің қызметі Active Directory каталогынан авторизацияны растауды сұрайды.

в) Рұқсат алғаннан кейін, DHCP сервері DHCP тұтынушыларының IP хаттамасын конфигурациялау функциясын жалғастырады.

г) егер DHCP сервері рұқсат алмаған болса, онда DHCP сервер қызметі тиісті оқиғаны оқиға журналына жазады және тоқтайды.

Егер желіде бірнеше DHCP серверлер болса:

a) DHCP сервер қызметі DHCPINFORM сұранысты жергілікті желіге жібереді, бар DHCP серверлерінен Active Directory түбірлік домен ақпаратын алуға тырысады.

б) бар DHCP серверлері сұранысқа DHCPACK растау хабарламасымен жауап береді және түбірлік домен туралы ақпаратты қайтарады (әр түрлі DHCP серверлері әртүрлі түбірлік домендер туралы ақпаратты қайтара алады).

в) түбірлік домендердің тізімі және белсенді DHCP серверлерінің тізімі жасалады.

г) егер DHCP сервері қызметі домен бақылауында немесе мүше серверінде орнатылған болса, DHCP сервері оның компьютерінің түпнұсқалық доменіндегі Active Directory каталогында авторизацияны растауды сұрайды.

д) Егер DHCP сервері автономды компьютерде жұмыс істейтін болса, онда DHCP сервері растауды алғанға дейін кез келген түбірлік домендердің тізімінде оның авторизациясын растауды сұрайды.

е) Рұқсат алғаннан кейін DHCP сервері DHCP тұтынушыларының IP хаттамасын конфигурациялау функциялары жұмыстарын жалғастырады.

ж) Егер DHCP сервері рұқсат алмаса, DHCP сервер қызметі Windows 2000 оқиғалар журналына тиісті оқиғаны жазады және жұмысын тоқтатады.

Windows 2000 жүйесінде Active Directory каталог қызметінде жұмыс істейтін DHCP серверлері авторизациясы желіде сыртқы DHCP серверлерінің пайда болуына жол бермейді. Рұқсат етілмеген DHCP серверлерін тану және бұғаттау үшін бірқатар шаралар қабылдау қажет:

* Бір немесе бірнеше DHCP серверлерінің қызметін домен бақылауына немесе жобадағы мүше серверіне орнатуды қарастырыңыз (DHCP серверінің домендік бақылаушысы болып табылатын компьютердің істен шығуы жағдайында домен контроллерінде немесе мүше серверлерінде орнатылған бірнеше DHCP серверлері ақаулыққа төзімділікті қамтамасыз етуі керек).
* Active Directory каталогқа кіруге рұқсат етілген DHCP серверлерінің тізімін жасаңыз (тізімде көрсетілмеген DHCP серверлері басталмайды).
* DHCP ретрансляция агенттерін орнатыңыз немесе DHCP/BOOTP бағыттауыштарға бағыттауды қосыңыз (DHCРформинг, DHCPACK хабарламалары таратылатын хабарламалар болып табылады, сондықтан оларды оңай қабылдап, желінің барлық сегменттеріне жіберуді қамтамасыз ету керек).

DHCP дерекқорының тұтастығын қамтамасыз ету үшін рұқсаты жоқ пайдаланушылардың DHCP серверіне тікелей кіруіне жол бермеу керек. Рұқсат етілмеген пайдаланушылардың DHCP дерекқорына нұқсан келтірмеуінің бірнеше жолы бар:

- Ұйымдағы DHCP серверлерін басқаруға рұқсат етілген пайдаланушылар санын шектеу.

- DHCP серверлерін ортақ желіден оқшаулау. DHCP серверлері Интернет сияқты ашық желілерден қол жетімді емес желілік сегменттерде орналасуы керек.

5) DHCP қол жетімділігінің артуы. DHCP жобаларында қол жетімділікті арттыру жолдары:

а) Windows Clustering сервер кластерлері. DHCP сервер қызметі Windows Clustering серверлер кластерлінің жұмысын қолдайды. Кластер кем дегенде екі компьютерден тұрады, олар кластердің ортақ дискісін қолданады. Кластер дискісі кластерлік компьютерлердің немесе кластер түйіндерінің ортақ SCSI шинасына қосылады. Мысалы, кез-келген уақытта DHCP қызметі түйіндердің біреуінде жұмыс істейді. Деректер кластердің ортақ дискісінде сақталады. Қазіргі уақытта DHCP сервері қызметі жұмыс істеп тұрған кластер түйіні белсенді түйін деп аталады. Егер белсенді (активный) түйін істен шықса, белсенді емес (неактивный) түйін автоматты түрде қосылады.

б) DHCP-нің бірнеше серверлері арасында аудандарды бөлу. Кейде бір DHCP аймағының IP мекенжайларының аймағы екі (немесе одан да көп) DHCP серверлер арасында бөлінеді. Бұл жағдайда осы аймақтың әр бөлігі серверлердің бірінде басқарылады. Егер DHCP серверлерінің біреуі істен шықса, екінші сервер қалған конфигурацияның мекен-жайларын бере отырып, IP конфигурация функцияларын алады. Мысалы, 172.16.01-172.16.0.254 диапазоны берілген. 172.16.01.-172.16.0.128 диапазоны әр серверге орнатылады. Басқа серверге - 172.16.0.129-172.16.0.054. Бұл әдістің басты артықшылығы - оны енгізу үшін қосымша аппараттық және бағдарламалық ресурстарды қажет етпейді. Егер бір DHCP сервері шықса, оның мекенжайлары қол жетімсіз болады, бірақ басқа мекенжайларды тағайындауға болады.

в) арнайы компьютердегі DHCP сервері. Бұл жағдайда басқа қосымшалар мен қызметтердің тұрақсыз жұмысы компьютерді қайта қосу қажеттілігіне әкелмейді.

6) DHCP жұмысын жақсарту. DHCP өнімділігін жақсарту жолдары:

а) бірнеше DHCP серверлерінің арасындағы жүктемелерді теңестіру. Егер қолданыстағы DHCP серверлері қайта жүктелген болса және оларды жаңарту мүмкін болмаса, қосымша DHCP серверлерін орналастырған жөн, DHCP сұраулары қосымша серверлер арасында таратылады, яғни IP конфигурациясының уақыты қысқарады.

б) жалдау мерзімінің өзгеруі. Тұтынушылардың IP мекенжайларын жалға алу мерзімін ұзарту жалдау мерзіміне байланысты болады. Ол ұлғайған кезде тұтынушылар DHCP серверіне азырақ қатынайды, бұл DHCP трафигін азайтады.

в) арнайы компьютерде DHCP серверінің орналасуы. Өнімділік жоғарылайды, өйткені жүйелік ресурстар бір уақытта жұмыс істейтін қосымшалар мен қызметтерді пайдаланбайды.

2.3.4 BOOTP және DHCP хаттамалары арасындағы айырмашылықтар

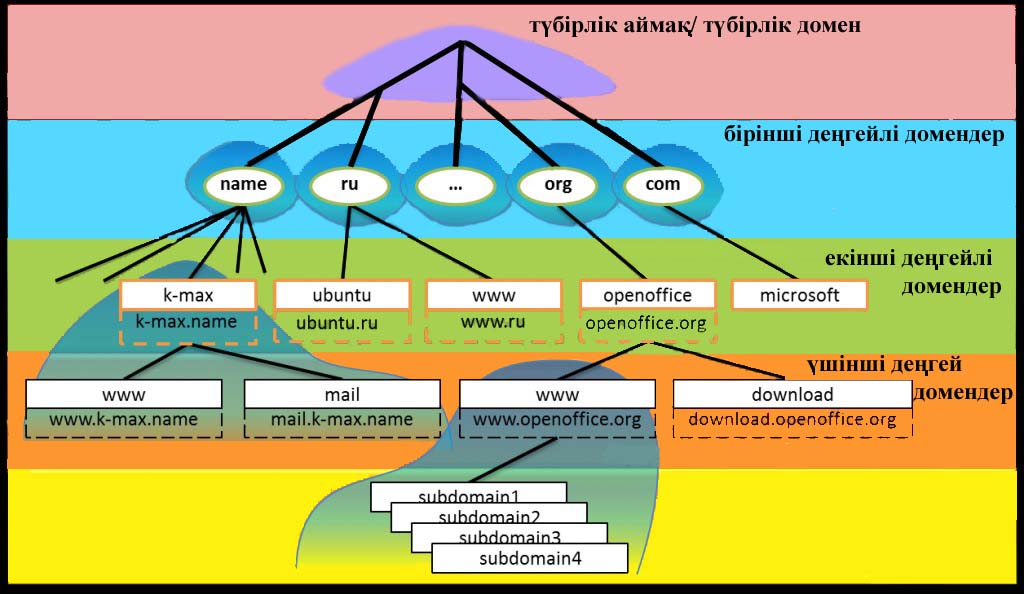
DHCP хаттамасы – BOOTP (Bootstrap Protocol, жүктеу хаттамасы) кеңейтуге ықпал жасайтын болып табылады. Ол алғашында желілік интерфейс платаларында орналасқан, бағдарламанатын тұрақты еск сақтауға арналған жадтыы (PROM) және өшірілетін бағдарламаланатын тұрақты жадты (EPROM) дискісіз жұмыс станцияларын жүктеу мүмкіндігін қамтамасыз ету үшін жасалған. Іске қосылған жүктеу коды осы машиналарға желіге операциялық жүйе конфигурациясының деректерін және желінің басқа жерде орналасқан серверден желі конфигурациясын жүктеуге мүмкіндік беретін қатты кодталған процедураны орындайды.

Бастапқылармен салыстырғанда, DHCP хаттамасы көптеген мүмкіндіктерді ұсынады, алайда DHCP және BOOTP хаттамаларының пішіндері сәйкес болып қалады. Осылайша, ешқандай DHCP сервері қосылмаған кабельдік сегментте DHCP трансляторын қолданудың орнына BOOTP сұраныстарын әртүрлі кабельдік сегменттерге жіберуге бағыттауды қалпына келтіруге болады.

2.3.5 DNS қызметі

Домендік атаулар жүйесі (DNS – Domain Name System) - бұл IP мекенжайлары мен түйін атаулары арасындағы сәйкестікті орнату үшін TCP / IP қосымшаларында қолданылатын таратылған мәліметтер базасы. Сондай-ақ, DNS электрондық поштаны бағыттау үшін қолданылады. Біз таратылған терминді қолданамыз, өйткені барлық қажетті ақпарат бір Интернет желісінде сақталмайды. Әрбір түйін (университет, кампус, серіктестік немесе компания ішіндегі бөлім) өзінің ақпараттық базасын сақтайды және Интернет арқылы басқа жүйелерге сұрау жібере алатын серверлік бағдарламаны іске қосады. DNS тұтынушылар мен серверлердің бір-бірімен байланысуына мүмкіндік беретін хаттамар.

DNS атаулар кеңістігі иерархиялық құрылымға ие, 2.9 суретте DNS иерархиялық ұйымы көрсетілген.



2.9 сурет – DNS иерархиялық ұйымы.

Әрбір түйіннің (2.9 суреттегі шеңберлер) ұзындығы 63 таңбаға дейін тұрады. Ағаш тамыры – бұл белгісіз арнайы түйін. Белгілеулер үлкен немесе кіші әріптерден тұруы мүмкін. Ағаштағы кез-келген түйіннің домендік атауы (domain name) – бұл түбір ретінде әрекет ететін түйіннен басталып, белгілер нүктелермен бөлінетін белгілер тізбегі. Әрбір ағаш түйінінде ерекше домен атауы болуы керек, алайда бірдей белгілерді ағаштың әртүрлі нүктелерінде пайдалануға болады.

Нуктемен аяқталатын домендік атау абсолютті домендік атау (absolute domain name) немесе толық домендік атау (FQDN– fully qualified domain name) деп аталады. Мысалы, sun.tuc.noao.edu. Егер домендік атау нүктемен аяқталмаса, атауды аяқтау керек деп болжанады.

2.10 суретте жеті негізгі домендердің әдеттегі жіктелуінің тізімі көрсетілген.

2.9 суретте көрсетілмеген DNS-тің маңызды сипаттамалары, DNS ішіндегі жауапкершілікті беру болып табылады. Барлық ағашты тұтасымен және әр белгімен жеке-жеке басқаратын ұйым жоқ. Оның орнына бір ұйым (NIC) ағаштың бір бөлігіне ғана қызмет етеді (жоғары деңгейлі домендер) және белгілі бір аймақтар үшін жауапкершілікті басқа ұйымдарға жүктейді.



Аймақ (zone) – бұл DNS ағашының бөлек басқарылатын бөлігі. Мысалы, noao.edu екінші деңгейлі домен - бұл бөлек аймақ. Екінші деңгейдегі көптеген домендер кіші аймақтарға бөлінеді. Мысалы, университет өз аймағын факультет бойынша өзінің аймақтарына бөле алады, ал компания филиалдарға немесе бөлімдерге бөліну қағидаты бойынша аймақтарға бөлінеді.

|  |  |
| --- | --- |
| Домен | Сипаттамасы |
| com | Коммерциялық ұйымдар |
| edu | Білім беру ұйымдары |
| gov | АҚШ үкіметтік ұйымдары |
| int | Халықаралық ұйымдар |
| mil | АҚШ әскери ұйымдары |
| net | Желілер |
| org | Басқа ұйымдар |

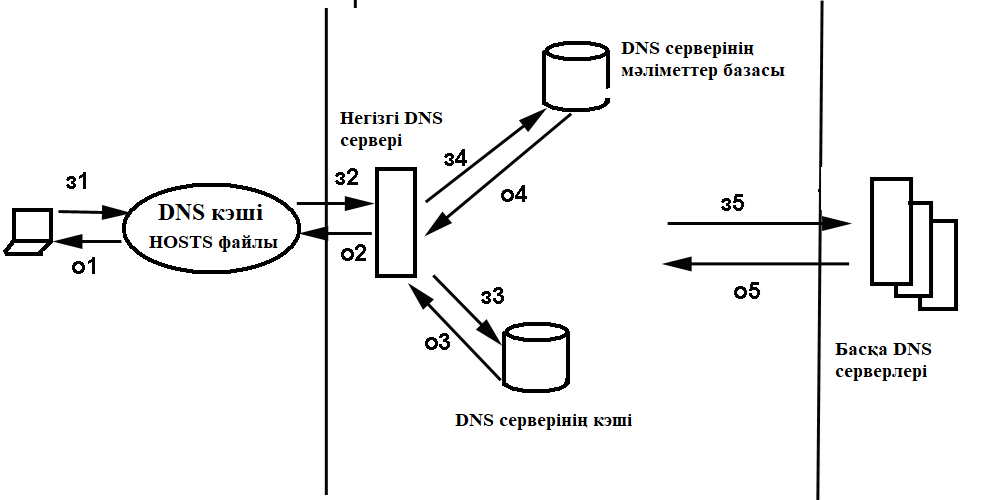
2.10 сурет-3 таңбалы жалпы домендер.

Сіз аймақты басқаруға жауапты ұйымды немесе адамды таңдаған сәттен бастап бұл ұйым немесе адам осы аймақ үшін бірнеше DNS (name servers) серверлерін ұйымдастыруы керек. Аймақта жаңа жүйе пайда болғаннан кейін, осы аймақтың әкімшісі жаңа түйіннің аты мен IP мекенжайын DNS серверінің дерекқорына орналастырады. Шағын университеттерде, мысалы, жаңа жүйе пайда болған сайын бір адам мұны істей алады, бірақ үлкен университеттерде жауапкершілікті бөлу керек (мысалы, кафедра бойынша), өйткені бір адам бұл жұмысты толығымен орындай алмайды.

Егер DNS серверінде қажетті ақпарат болмаса не болады? Ол басқа DNS серверімен байланыс орнатуы керек. (Бұл DNS-тің таратылған сипаты.) Алайда, кез келген DNS сервері басқа серверге кіруді білмейді. Оның орнына әрбір DNS сервері түбірлік DNS серверлерімен байланыс жасауды білуі керек. 1993 жылы сәуірде сегіз түбірлік серверлер болды, барлық бастапқы серверлер әр түбірлік сервердің IP мекен-жайларын білуі керек. (Бұл IP мекенжайлар бастапқы сервердің конфигурация файлдарында орналасқан. Бастапқы серверлер олардың DNS аттарын емес, түбірлік серверлердің IP мекенжайларын дәл білуі керек.) Түбірлік сервер, өз кезегінде, барлық домендер үшін әр екінші деңгейлі ресми DNS серверінің аттары мен позицияларын (IP мекен-жайларын) біледі. Нәтижесінде бірізді процесс жүреді: сұралған сервер түбірлік сервермен байланыс орнатуы керек. Түбірлік сервер сұралған серверге басқа сервермен байланысуды хабарлайды және т.б.

DNS – Internet-ке қосылған кез-келген түйіннің маңызды бөліктерінің бірі, бұл жүйе жеке өзара байланысты желілерде де кеңінен қолданылады. Ұйымның негізі – DNS атаулар кеңістігін құрайтын иерархиялық ағаш.

IP мекен-жайындағы түйін атауын және керісінше өзгерту үшін қосымшалар талдаушыларға жүгінеді. Талдаушылар жергілікті DNS серверлеріне жүгінеді, ал олар өз кезегінде сұрауға жауап алу үшін түбірлік серверлердің біріне немесе басқа серверлерге жүгіне алады (2.11 сурет).



2.11 сурет – Домен атауларын рұқсат ету кезінде сұрау және жауап сұлбасы

Барлық DNS сұраулары мен жауаптары бірдей форматта болады. Бұл хабарламалар сұрақтардың және мүмкін жауаптардың, RR тіркелген деректерінің және қосымша ақпараттың RR жазбаларын қамтиды.

Интернет арқылы әртүрлі қызметтерді ұсынатын барлық серверлердің IP мекен-жайларын есте сақтау мүмкін емес. Оның орнына, серверді іздеудің оңай әдісі – атауды кейбір IP мекенжайымен сәйкестендіру. Домендегі түйін аттарын тиісті IP мекен-жайымен байланыстыратын DNS серверінде арнайы кесте жазылады. Егер тұтынушы сервердің атауын білетін болса, мысалы, веб-сервер, бірақ IP-мекен-жайын табу керек болса, ол 53-порт арқылы DNS серверіне сұрау жібереді. Тұтынушы осы түйіннің IP-конфигурациясының DNS параметрлерінде көрсетілген DNS серверінің осы IP мекенжайын пайдаланады .

Сұранысты алғаннан кейін DNS сервері оның кестесінен сұралған IP мекенжайы мен веб-сервер арасында сәйкестіктің бар-жоғын анықтайды. Егер DNS серверінде сұралған аттың жазбасы болмаса, ол өз доменіндегі басқа DNS серверін сұрайды. IP мекенжайын танығаннан кейін DNS сервері нәтижені тұтынушыға қайта жібереді. Егер DNS сервері IP мекенжайын анықтай алмаса, тұтынушы осы веб-сервермен байланыса алмайды және күту уақыты туралы хабарлама алады.

2.3.6 FTP хаттамасы

Файлдарды беру хаттамасы (File Transfer Protocol (FTP)) – файлдарды бір компьютерлік жүйеден екіншісіне ауыстыру алгоритмі болып табылады, TCP қолданады және қосымша ID пайдаланушы мен пароль көмегімен қолданушының аутентификациясын қамтамасыз етеді. FTP – бұл қашықтағы компьютерге қосылуға, файлдарды көшіруге және беру аяқталғаннан кейін байланыс желісін жабуға қызмет ететін интерактивті қызмет. Бұл әрекеттерді орындау үшін келесі негізгі пәрмендер қолданылады:

-Open (Ашық) – қашықтағы компьютерге қосылу;

- Get (алу) – байланыс орнатқаннан кейін файлды компьютерден алу;

-Bye (жабу) – байланысты өшіру және FTP бағдарламасын аяқтаңыз.

-FTP – бұл компьютерлер арасында кең таралған файлдарды жіберу хаттамасы. FTP тұтынушылық бағдарламалық жасақтамасын басқаратын түйін файлды басқарудың әртүрлі функцияларын, соның ішінде жүктеу және жүктеуді орындайтын FTP серверіне кіреді. Бұл сізге мәтіндік және екілік файлдарды тасымалдауға мүмкіндік береді. Деректерді беру аяқталғаннан кейін қосылыс автоматты түрде аяқталады, яғни бағдарлама файлдарды көшіру немесе жылжытудың ағымдағы сеанс аяқтағаннан кейін жүйеден шығады, сеанс аяқтау үшін осы жеткілікті.

FTP сервері тұтынушы мен құрылғылар арасында файл алмасуды қамтамасыз етеді. FTP серверінің көмегімен тұтынушы файлдарды қашықтықтан басқара алады, мысалы, жою немесе атын өзгерту пәрмендерін қолдана отыра. Бұл үшін FTP қызметі тұтынушы мен сервер арасындағы екі байланыс портын қолданады.

FTP сеансын бастау туралы сұраныс серверге 21-ші порт арқылы жіберіледі. Байланыс сеансын ашқаннан кейін сервер деректер порттары жіберілетін 20 портқа ауысады.

FTP тұтынушы бағдарламасы компьютердің операциялық жүйесіне, сонымен қатар көптеген веб-браузерге енеді. Автономды FTP тұтынушылары графикалық интерфейс арқылы басқарудың көптеген ыңғайлы мүмкіндіктерін ұсынады.

2.3.7 TFTP хаттамасы

Хаттама – TFTP (Trivial File Transfer Protocol – файлдарды қарапайым жіберу хаттамасы) UDP механизмін қолданатын байланыссыз хаттама болып табылады. TFTP конфигурация файлдары мен Cisco IOS операциялық жүйелерінің суреттерін маршрутизаторлар мен коммутаторларға беру үшін қолданылады. Хаттама қолдануға және орнатуға кішкентай және оңай жасалған, сондықтан FTP хаттамасының көптеген мүмкіндіктері жетіспейді. Ол тек файлдарды қашықтағы серверден оқи алады және жаза алады. Хаттама кейбір жергілікті желілерде кеңінен қолданылады, өйткені ол стандартты FTP хаттамасына қарағанда тезірек жұмыс істейді.

2.3.8 НТТР қызметі

HTTP қызметі (HyperText Transfer Protocol – гипермәтіндік файлдарды беруге арналған хаттама) Интернеттің жылдам өсетін және көп қолданылатын бөлігі болып табылатын World Wide Web-пен жұмыс істеуге арналған. WWW қызметтерінің негізгі мақсаты ақпаратқа қол жетімділікті қамтамасыз ету. Интерактивті гипермәтіндік ақпараттармен жұмыс істеу үшін қолданылатын веб-браузер тұтынушылық қосымшасы болып табылады, сондықтан ол серверден жұмыс істеуді талап етеді.

Веб-сайттарды шарлаудың икемділігі мен қарапайымдылығы гиперсілтемелер деп аталады. Гиперсілтеме дегеніміз – жаңа веб-параққа бағыттайтын веб-беттегі объект (сөз, фраза немесе сурет). Сілтемелері бар веб-парақ URL мекен-жайы (Uniform Resource Locator) деп аталатын ақпараттың мекен-жайын қамтиды.

Веб-клиент веб-сервердің IP-мекен-жайын алғаннан кейін клиент – браузер осы IP-мекен-жайы бойынша веб-қызметтерге сұранысты бастайды және оны 80-порт арқылы жібереді. Бұл сұрау гипермәтінді беру хаттамасының (HTTP) көмегімен серверге жіберіледі.

Сұрауды 80-порттан алғаннан кейін, сервер тұтынушының сұранысына жауап береді және тұтынушының сұратылған веб-парағын жібереді. Веб-парақтың мазмұны белгілеу тілдерінің көмегімен кодталған. HTML (гипермәтінді белгілеу тілі) ең танымал, бірақ бүгінде XML және XHTML сияқты тілдер барған сайын танымал бола бастайды.

HTTP хаттамасы қауіпсіз емес; ақпаратты желі арқылы беру кезінде оңай ұстауға болады. Деректердің қауіпсіздігін қамтамасыз ету үшін қауіпсіз тасымалдау хаттамасымен HTTP хаттамасын біріктіруге болады. Қауіпсіз HTTP хаттамасын пайдаланатын сұраулар 443 портына жіберіледі. Мұндай сұраныстар http: емес, https: префиксін қолдануы керек.

Нарықта көптеген түрлі веб-қызметтер мен веб-тұтынушылар бар. HTTP хаттамасы мен HTML сәйкестігі әртүрлі жеткізушілердің серверлері мен тұтынушыларының тиімді әрекеттесуін қамтамасыз етеді.

2.3.9 Telnet қызметі

Telnet қызметі – бұл алғашқы Интернет-хаттамаларының бірі (терминалды эмуляциялау бағдарламасы). Оны Интернет хосттың қашықтағы терминалы ретінде пайдалануға болады. Интернет-хост компьютерімен байланыс кезінде компьютер оның пернетақтасы мен дисплейі қашықтағы компьютерге тікелей қосылғандай жұмыс істейді. Пайдаланушы бағдарламаларды жер шарының қарама-қарсы жағында орналасқан компьютерде өзінің артында отырған сияқты оңай басқара алады. Telnet сеансы тұтынушының компьютерінің өңдеу қуатын пайдаланбайды. Оның орнына, Telnet бағдарламалық жасақтамасы перне түртулерін қашықтағы компьютерге жібереді және компьютер мониторында көрсетілетін нәтижелерді қабылдайды. Барлық деректерді өңдеу және сақтау қашықтағы компьютерде орындалады.

2.3.10 SMTP хаттама

Электрондық пошта – бұл Интернеттегі ең танымал тұтынушы-серверлік қосымшаларының бірі. Пошта серверлерінде жұмыс істейтін серверлік бағдарлама желідегі басқа пошта серверлерімен өзара әрекеттесуді қамтамасыз етеді.

Әрбір пошта сервері пошта серверінде жасалған жеке пошта жәшіктерінде пайдаланушы поштасын қабылдау және сақтау үшін жауап береді. Пошта серверіне өзінің пошта жәшігіне кіріп, хабарламаларды оқу үшін пайдаланушы пошта тұтынушысының бағдарламасын қолданады.

Пошта серверлері жергілікті пошта жәшіктеріне немесе басқа пошта серверлерінде орналасқан пошта жәшіктеріне жіберілген хаттарды жіберу үшін де қолданылады.

Пошта жәшігінің келесі форматы қабылданады: user@company.domain.

Поштаны өңдеу үшін SMTP, POP3, IMAP4 протоколдарын қоса, әр түрлі деңгейдегі хаттамалар қолданылады.

Электрондық поштаны бағыттаудың жеңілдетілген хаттамасы. Бұл хаттама (SMTP – Simple Mail Transfer Protocol) – бұл электрондық поштаны алмасуда қолданылатын тұтынушы / сервер негізіндегі TCP хаттамасы. SMTP хабарламаларды жергілікті пошта серверіне жіберу үшін пошта тұтынушысының бағдарламасы қолданады. Содан кейін жергілікті сервер хабарламаның кімге жіберілгенін анықтайды - жергілікті пошта жәшігі немесе басқа сервердегі пошта жәшігі. SMTP түрлі серверлермен өзара әрекеттесу кезінде қолданылады, мысалы, егер сіз басқа серверлерге хабарлама жібергіңіз келген жағдайда. SMTP сұраулары 25 портқа жіберіледі.

Сервер кіріс хабарларды пошта жәшіктеріне орналастырады, ал клиенттер оларды Post Office Protocol (POP) немесе Internet Message Access Protocol (IMAP) арқылы алады.

POP сервері пайдаланушылар үшін хабарламаларды қабылдайды және сақтайды. Тұтынушы мен пошта сервері арасында байланыс орнатылғаннан кейін хабарламалар тұтынушының компьютеріне жүктеледі. Әдетте, хабарламалар тұтынушы оқығаннан кейін серверде сақталмайды. Тұтынушылар POP3 серверлеріне 110 порт арқылы кіреді.

Сондай-ақ, IMAP сервері пайдаланушыларға жіберілген хабарламаларды қабылдайды және сақтайды. Алайда, хабарламаларды пайдаланушылардың пошта жәшіктерінде сақтауға болады, егер оларды қолданушылардың өздері тікелей жоймаса. IMAP хаттамасының соңғы нұсқасы – IMAP4 143 порт арқылы тұтынушылардың өтініштерін тыңдайды.

Желілік операциялық жүйелердің әртүрлі платформалары әртүрлі пошта серверлерін пайдаланады.

Пошта тұтынушысы мен пошта сервері арасында байланыс орнатқаннан кейін хабарламаларды жүктеу және қарау басталады. Электрондық пошта тұтынушыларының көпшілігі пошта жәшігінде тіркелген пошта серверінің түріне байланысты POP3 немесе IMAP4 үшін теңестірілген. Электрондық пошта тұтынушылары SMTP көмегімен серверге электрондық поштаны жіберуі керек.

Пошта серверлері кіріс және шығыс хаттарды өңдеуге қалпына келтіріледі.

Пошта тұтынушысының қалпына келтірулері:

- POP3 немесе IMAP4 серверінің атауы

- SMTP серверінің атауы

- Пайдаланушы аты

- Пароль (құпия сөз)

- Спамдар (қажет емес хабарлама) мен вирустарға арналған сүзгілер.

2.3.11 NAT хаттамасы

Қажет болса, ішкі желі түйіндерінің саны Интернет қызметінің шығарған нақты IP мекенжайларының санынан асып кетсе, Интернетке қосылыңыз. NAT тіркелмеген мекен-жайларды пайдаланатын жеке IP желілеріне Интернет ресурстарына қол жеткізуге мүмкіндік береді. NAT функциялары жеке (ішкі) және жалпы желіні (Интернет сияқты) бөлетін шеткі маршрутизаторда қалпына келтірілген. Әрі қарай, біз жалпыға ортақ желіні сыртқы желі, ал жеке желіні - ішкі желі деп атаймыз. Пакеттерді сыртқы желіге жіберместен бұрын NAT функциясы ішкі жергілікті мекен-жайларды бірегей сыртқы IP адрестерге аударады.

«Ішкі желі» термині ұйым ішіндегі және аударманы қажет ететін мекенжайларды пайдаланатын желілер үшін қолданылады. Мұндай желілік доменде тораптар бір адрестік кеңістікті пайдаланады, ал сыртында олар NAT функцияларының параметрлерімен анықталған басқа мекенжай кеңістігіндегі мекенжайларға қол жетімді. Бірінші мекенжай кеңістігі, әдетте, жергілікті деп аталады, ал екіншісі – ғаламдық мекенжайлық кеңістік деп аталады.

Сонымен, сыртқы желі термині ішкі желінің домендері қосылатын желілерді білдіреді. Бұл желілер ұйымдардың бақылауында емес.

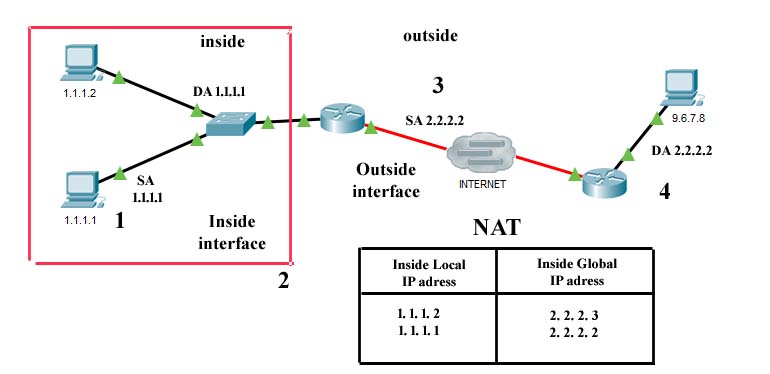
NAT функциясын қалпына келтіруді бастамас бұрын жергілікті және ғаламдық ішкі мекенжайлар туралы қол жетімді ақпаратты талдау керек.

Source ішкі адрестерді аудару. Бұл NAT функциясы ішкі IP мекенжайларын ғаламдық мекенжай кеңістігіне кіретін бірегей мекенжайларға, қажет болған жағдайда ішкі желінің сыртқы желімен өзара әрекеттесуін қамтамасыз етуге мүмкіндік береді. Статикалық немесе динамикалық аударымды қолдануға болады:

- Статикалық аударма «бірден бірге» түріндегі мекенжайлардың сәйкестігін, яғни бір ғаламдық ішкі мекенжай бір жергілікті ішкі мекен-жайға сәйкес келеді. Статикалық аударма белгілі бір ішкі түйінге белгіленген мекен-жайға сыртқы қол жеткізуге болатын жағдайларда қолданылады (мысалы, WWW сервері).

- Динамикалық аударма ішкі жергілікті мекен-жай мен ғаламдық мекенжайлар пулының арасындағы сәйкестікті орнатады.

2.12 суретте IP пакет тақырыптарының Source өрісіндегі түйіндердің мекен-жайларын ішкіден сыртқыға аударатын маршрутизатор көрсетілген.



2.12 сурет – Ішкі адрестерді аудару көзі

Source жергілікті мекен-жайларын аудару 2.12 суретке сәйкес төменде сипатталған.

1) 1.1.1.1 түйінінің пайдаланушысы В түйініне байланысты ашады.

2) Маршрутизатордың 1.1.1.1 түйінінен алған бірінші пакет маршрутизатордың NAT кестесін тексеруді бастауға алып келеді.

3) Егер аударма кестесінде статикалық жазба болса, онда маршрутизатор 5-қадамға көшеді.

4) Егер аудару кестесінде статикалық жазба болмаса, онда маршрутизатор пакет көзі- түйінінің мекенжайын (SA – Source Address) 1.1.1.1 динамикалық түрде тарату керектігін анықтайды. Әрі қарай, маршрутизатор мекенжай пулынан ақысыз ғаламдық мекенжайды таңдап, кестеде аударма жазбасын жасайды. Жазба түрі қарапайым жазба (Simple Entry) деп аталады.

5) В торабы ішкі глобальді адресті (DA, Destination Address) 2.2.2.2 пайдаланып 1.1.1.1 түйінінен пакет пен жауап алады.

6) Маршрутизатор ішкі ғаламдық мекен-жайы бар пакетті алған кезде, іздеу кестесі ретінде ішкі ғаламдық мекен-жайдың көмегімен NAT кестесін тексереді. Бұдан әрі ішкі ғаламдық мекен-жай 1.1.1.1 ішкі мекен-жайға аударылып, 1.1.1.1 торабына жіберіледі.

7) 1.1.1.1-тармақ осы пакетті алады және В торабымен өзара әрекеттесуді жалғастырады. Маршрутизатор әр пакетке қатысты 4-7 тармақтарда сипатталған әрекеттерді орындайды.

NAT-ті желілік ортада қолданудың көптеген себептері бар. NAT артықшылықтарының арасында келесілер бар:

- Жеке желінің Интернет сияқты сыртқы желіге кіру үшін тіркелмеген IP мекенжайларын пайдалану мүмкіндігі.

- Интернетте бұрыннан бар IP адрестерін қайта пайдалану мүмкіндігі.

- Жеке IP мекенжайлары жеткілікті тіркелмеген желілерде Интернетке қосылуды қамтамасыз ету.

- Екі біріктірілген компанияның желілері сияқты, өзара байланысты екі интражелілік адресті дұрыс аудару.

- Ескі Интернет-провайдерлер бөлген ішкі IP мекен-жайларды жергілікті желі интерфейстерін қолмен реттеместен, жаңа провайдердің жақында бөлінген мекен-жайларына аудару.

***NAT жұмыс істеу принципі***

NAT ішкі желі (жергілікті желі) және сыртқы желі (Интернет провайдері немесе Интернет сияқты жалпы желі) арасындағы тармақталу шекарасына жақын маршрутизаторда немесе маршрут процессорында қалпына келтірілген. Сыртқы желі басқа компанияның желісі болуы мүмкін, мысалы, екі желіні біріктіру кезінде. Маршрутизатор ішкі және сыртқы желілерді ажырататындығын ескеріңіз. NAT ішкі, жергілікті мекен-жайларды жаһандық бірегей IP адрестерге аударады. Осылайша, деректер сыртқы желіге түсе алады.

NAT хаттамасы бірнеше адамның белгілі бір уақытта сыртқы желіні қолданатынын ескереді. Процестер коммутациясы шығыс пакеттердің бастапқы мекен-жайын өзгерту үшін және оларды тиісті маршрутизаторға қайта жіберу үшін қолданылады. IP мекенжайлары желідегі түйіндерге қарағанда аз жұмсалады. Қорғаныс шлюздерін пайдалану.



NAT хаттамасын қолданудың кемшіліктері:

- NAT желінің жылдамдығын азайтады. Пакеттердің тақырыптардағы әр IP мекен-жайдың көп аударылуына байланысты коммутация маршруттарында кідірістер орын алады. Маршрутизатордың процессоры IP пакетін аудару және өзгерту керек екенін анықтау үшін әр пакетті өңдеуге қолданылады.

- NAT IP мекенжайларын нүктеден-нүктеге дейін жасырады. Осыған байланысты сіз кейбір қосымшаларды пайдалана алмайсыз. NAT IP шекаралық маршрутизатор арқылы IP адрестерді аударған кезде атаудың толық доменіне қарағанда физикалық мекен-жайларды қолдануды қажет ететін қосымшалар дерегі тағайындалған жерге жетпейді.

- Себебі, NAT IP-мекен-жайын өзгерткендіктен, бір нүктеден екінші нүктеге дейін IP іздеу мүмкіндігі жоғалады. Бірнеше пакеттің мекен-жайындағы өзгерістер IP қадағалау бағдарламаларын шатастырады. Сонымен бірге, бұл қауіпсіздік тұрғысынан жағынана қарағанда артықшылық болып саналады: бұзақыларға пакеттің бастақы көзін анықтау мүмкіндігі азайтады.



***NAT қалпына келтіру***

***Статикалық трансляцияны қалпына келтіру***

Статикалық трансляция режимін ішкі жергілікті мекенжай мен ішкі ғаламдық мекенжайдың арасында орнатыңыз.

Router(config)#ip **nat inside source static 1.1.1.1 2.2.2.**2

Ішкі интерфейсті көрсетіңіз

Router(config)**#interface F0/0**

Бұл интерфейсті ішкі желіге сәйкес деп белгілеңіз.

Router(config–if)#**ip nat inside**

Ішкі интерфейсті көрсетіңіз

Router(config**)#interface S0/0**

Бұл интерфейсті сыртқы желіге сәйкес деп белгілеңіз.

Router(config–if)#**ip nat outside**

**Динамикалық трансляцияны қалпына келтіру**

Ғаламдық мекен-жай пулын анықтаңыз

Router(config–if**)#ip nat pool net–208 171.69.233.208 171.69.233.233 netmask 255.255.255.240**

Алдыңғы қадамда анықталған қол жетімді тізімге негізделген динамикалық трансляцияны орнатыңыз

Router(config–if)**#ip nat inside source list 1 pool net –208**

Ішкі интерфейсті көрсетіңіз

Router(config–if**)#interface serial 0**

Router(config–if)#**ip address 171.69.232.182 255.255.255.240**

Бұл интерфейсті сыртқы желіге сәйкес деп белгілеңіз.

Router(config–if)#**ip nat outside**

Ішкі интерфейсті көрсетіңіз

Router(config–if)#**interface ethernet 0**

Бұл интерфейсті ішкі желіге сәйкес деп белгілеңіз.

Router(config–if**)#ip nat inside**

Трансляцияға тиесілі мекен-жайларды басқаратын стандартты енгізу тізімін анықтаңыз)

Router(config)**# accses–list 1 permit 192.168.1.0 0.0.0.255**

Жоғарыда келтірілген конфигурация 1-енгізу тізімімен анықталған барлық бастапқы түйін мекнжайларын (192.168.1.0/24 мекен-жайларына рұқсат етілген) net - 208 адрестік пулына ауыстырады. Бұл пул 171.69.233.208-ден 171.69.233.233 дейінгі мекен-жайларды қамтиды.

***Бір ішкі ғаламдық мекенжайды пайдалану***

Бір ішкі ғаламдық мекенжайды пайдалану режимін реттеу үшін сізге: net - 208 деп аталатын мекен-жай пулын жасау керек. Бұл пулде 171.69.233.208-ден 171.69.233.233 дейінгі мекен-жайлар бар.

1-тізім. 192.168.1.0-ден 192.168.1.255 дейін жіберуші мекен-жайы бар пакеттерге мүмкіндік береді. Егер қазір трансляция процедуралары орындалмаса, онда 1-тізімге сәйкес келетін пакеттердегі мекенжайлар көрсетілген пулдан мекен-жайға аударылады. Маршрутизатор бірнеше ішкі мекенжайларға (192.168.1.0 - 192.168.1.255) бірдей ғаламдық мекен-жайларды пайдалануға мүмкіндік береді. Қосылысды анықтау үшін маршрутизатор порт нөмірлерін пайдаланады.

Ғаламдық мекен-жай пулын анықтаңыз

Router(config–if)**#ip nat pool net–208 171.69.233.208 171.69.233.233 netmask 255.255.255.240**

Алдыңғы қадамда анықталған енгізу тізімінде рұқсат етілген мекен-жайларды динамикалық трансляция режиміне орнатыңыз

Router(config–if**)#ip nat inside source list 1 pool net –208 overload**

Сыртқы интерфейсті көрсетіңіз

Router(config–if)**#interface serial 0**

Router(config–if**)#ip address 171.69.232.182 255.255.255.240**

Бұл интерфейсті сыртқы желіге сәйкес деп белгілеңіз.

Router(config–if**)#ip nat outside**

Ішкі интерфейсті көрсетіңіз

Router(config–if)#**interface ethernet 0**

Бұл интерфейсті ішкі желіге сәйкес деп белгілеңіз.

Router(config–if)#**ip nat inside**

Трансляцияға тиесілі мекен-жайларды басқаратын стандартты енгізу тізімін анықтаңыз)

Router(config)# accses–**list 1 permit 192.168.1.0 0.0.0.255**

***NAT қалпына келтірулерін тексеру***

NAT қалпына келтірулерін тексеру тексеру кезінде сізге екі команда көмектеседі. Show ip nat translation командасы NAT кестесіндегі түрлендірулерді көрсетеді:

**R(config**)# show ip nat translation

Pro Inside global Inside local Outside local Outside global

- 200.1.1.25 - 10.1.1.25

- 200.1.1.26 - 10.1.1.26

Show ip nat translation verbose командасы NAT кестесіндегі жазбалардың уақытының ескіргендігі сияқты басқа да мәліметтерді көрсетеді:

**R(config)#** show ip nat translation verbose

Pro Inside global Inside local Outside local Outside global

— 200.1.1.25 10.1.1.25

create 00:05:01, use 00:00:00, left 23:12:4(J, flags: none

Show ip nat statistics командасы кейбір конфигурация мәліметтерін, трансяция статистикасын және NAT кестесіндегі деректерді көрсетеді:

R(config)# show ip nat statistics

Total active translations:2(0 static, 2 dynamic,0 extended)

Outside interfaces: Loopback 0, Seriall

Inside interface: Serial0

Hits: 243 Misses: 2

Expired translations: 0

Dynamic mappings:

--Inside Source

access-list 2 pool insidepool refcount 1

pool insidepool: netmask 255.255.255.0

start 200.1.1.1 end 200.1.1.4

type generic,total address 5,allocated 2 (50%),misses 0

**NAT ақауларын жою**

NAT ақауларын жою үшін debug ip nat командасын қолданыңыз. Төмендегі тізімде 10.1.2.5 бастапқы адресі 206.1.2.5 соңғы адресіне пакет жіберетініне назар аударыңыз. «->» белгісі бастапқы мекен-жайы пакетінің аударылғанын білдіреді. «\*» белгісі пакеттің **жылдам маршрут** арқылы өтетіндігін білдіреді. Басқа түйінмен диалогта пакет әрқашан ауыстырылған **баяу маршрутпен** өтеді. Егер кэште бастапқы және тағайындалған мекенжайлар туралы жазба болса, барлық басқа пакеттер жылдам бағыт бойынша жүреді.

**PAT хаттамасы**

PAT (Port Address Translation) – бұл NAT нұсқасы және Cisco маршрутизаторларындағы мекен-жайларды түрлендірудің жалғыз мүмкіндігі. PAT хаттамасы TCP порттарын қолданады. Осының арқасында бүкіл желі тек бір жаһандық басқарылатын IP мекенжайды пайдаланады.

PAT желі мекенжайларын үнемдейді. Сонымен қатар, ол бүкіл LAN-ге бір IP мекен-жайын тағайындайды. Барлық WAN трафигі бір мекен-жай бойынша көрсетіледі. Ішкі желі сыртқы желіге немесе Интернетке көрінбейді, өйткені сыртқы желі барлық трафик бағыттаудан келетін сияқты әсер қалдырады.

Егер пайдаланушыларға сыртқы желідегі белгілі бір қашықтағы серверге кіру қажет болса, сіз тұрақты мекенжайды қалпына келтіруіңіз керек. PAT белгілі порт нөмірі бар пакеттерге, мысалы, FTP немесе Telnet файлдарды жіберу хаттамалары арқылы өтуге мүмкіндік береді.



**PAT кемшіліктері**

PAT-ті қолданудың кемшіліктері бар, өйткені бұл хаттама тікелей және екі нүктелік трансляцияны жүзеге асыра алмайды. Осындай кемшіліктерді келесідей.

- сыртқы түйіннен жеке желі түйінен Ping бағдарламасын қолдана алмайсыз.

- Telnet портының өңдегіші қалпына келтірілмеген болса, сыртқы түйіннен ішкі түйінге қайта жіберілмейді.

- Ішкі желіде тек бір FTP сервері мен бір Telnet сервері қолданылады.

- Ішкі желінің мекен-жайы емес (DHCP, SNMP, Ping немесе TFTP) маршрутизаторға арналған пакеттер қабылданбайды немесе PAT көмегімен сүзілмейді.

- Егер бір уақытта 12-ден астам компьютер ішкі желіге қосылуға тырысса, олардың біреуі немесе бірнешеуі қате туралы хабарлама алуы мүмкін. Бұл серверге кірудің мүмкін еместігін көрсетеді.

- Ішкі компьютерлер PAT жазбаларын 400-ге дейін бөлісе алады. Егер TCP қосылымдары орнатылса және TCP күту уақыты жұмыс уақытына қолдау көрсететін болса, белгілі бір уақытта 400 машина сыртқы желіге кіре алмайды.

- Кейбір танымал порттар үшін порт өңдеушілер анықталмаған. Олардың құрамына келесі порттар кіреді. DHCP сервер жауаптарын алу үшін маршрутизатор пайдаланатын DHCP тұтынушы порттары. Windows ішкі желі тұтынушыларымен пайдаланылатын WINS NetBIOS порттары WINS хаттама мәліметтерін алу үшін қажет.



**PATқалпына келтіру**

PAT функциясы жеке IP мекенжайлары бар жергілікті түйіндерге сыртқы әлеммен байланыс орнатуға мүмкіндік береді. Маршрутизатор пакетті сыртқы желіге жібермес бұрын IP тақырыбының бастапқы мекен-жайын ғаламдық, ерекше IP мекен-жайға аударады. Сол сияқты, кері қайту жолында IP пакеттері арнайы жеке IP мекенжайларымен салыстырылады.

PAT қосылған кезде RIP пакетін беру автоматты түрде өшіріледі, бұл жеке IP адрестер туралы ақпараттың сыртқы желіге түсуіне жол бермейді.

PAT қосу үшін екі команда қолданылады. 1) **set ip pat on**. Бұл пәрмен NAT-ты қосады және орнатылған set ip pat port командасын қолдануға болатындай етіп орнатылады. 2) set Ip pat porthandler Порт өңдегіші жалпы TCP немесе UDP портын жеке IP мекен-жайына аударады. Пакет сыртқы желіден шыққан кезде, PAT порт нөмірін 15-тен аспайтын жазбаларды қамтитын порттың өңделушілерінің ішкі тізімімен салыстырады. Егер порт үшін арнайы өңдегіш анықталса, пакет тиісті порт өңдегішке (IP мекен-жайы) жіберіледі. Егер стандартты порт өңдегіші көрсетілген болса, пакет оған бағытталады. Келесі құпиялар болуы мүмкін:

- default барлық порттардың негізгі өңдеушілері үшін порт өңдегішін қосады. Ерекше жағдай - тек арнайы өңдегіш үшін.

- telnet Telnet хаттамасының 23 порты үшін порт өңдегішті қосады.

- ftp FTP файлдарды жіберу хаттамасы үшін порт өңдегішін қосады және 21-хаттама портын пайдаланады.

- smtp қарапайым SMTP пошта жіберу хаттамасы үшін порт өңдегішін қосады және 25 хаттамасын қолданады.

- wins 139 портындағы NetBIOS сеанс қызметі үшін порт өңдегішін қосады.

- http World Wide Web - HTTP 80 немесе 443 портын қорғайды. off порт өңдегішін ажыратады.



**Тексеру жұмысы № 4**

**№1 жаттығу Сөйлемді аяқтаңыз:**

А бағанынан сөйлемнің басын В бағанынан ең қолайлы соңымен салыстырыңыз. Нұсқаны таңдап, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір затты тек бір рет пайдалануға болады.

|  |  |
| --- | --- |
| **А баған** | **В баған** |
| * 1. broad packet \_\_\_\_\_   2. DHCP-клиент\_\_\_\_   3. NAT\_\_\_\_ \_\_   4. DNS \_\_   5. HOSTS \_\_\_\_ | А. Ethernet-те енгізілген виртуалды желі  Б. Әдетте TCP/IP тұтынушсынын бағдарламалық хаттама жиынтығының құрамдас бөлігі ретінде орындалатын бағдарламалық жасақтама құраушысы. Мекенжайлық сұраныстарды, ерекшелеуді ұзарту туралы сұраныстарды шығарады  B. белгілі домен атауларының тізімі және олардың сәйкес IP-адрестері бар арнайы мәтіндік файл, бұл домендік атауларды шешудің статикалық әдісі.  Г. Берілген желідегі барлық құрылғылар қабылдауға арналған желіні беру түрі.  Д. ішкі желідегі көптеген тұтынушылардың атынан желілік қосылыстарды басқаратын және барлық шығыс трафиктің бастапқы мекенжайларын сыртқы желінің интерфейсімен алмастыратын арнайы бағдарламалық қамтамасыздандыру.  E. TCP/IP статикалық иерархиялық түйін атауының қызметі |

**№2 жаттығу Дұрыс жауапты таңдаңыз**

1. Мекенжайы 202.121.74.37, маскасы 255.255.255.224 болатын түйінмен бірдей ішкі желіде қандай түйін бар?

а) 202.121.74.5

б) 202.121.74.10

в) 202.121.74.15

г) 202.121.74.25

д) 202.121.74.35

2. Қандай сөйлемде жалпы адресаттың мәселелерін сипаттайды? :

а) түйінде жарамсыз желі идентификаторы болады

б) DNS қолдану үшін түйін қалпына келтірілмеген

в) түйін сол желідегі басқа түйіндер сияқты бірдей желі идентификаторын қолданады.

г) түйін WINS қолдану үшін қалпына келтірілмеген

д) түйін HOSTS қолдану үшін қалпына келтірілмеген

3. Төмендегі ұсыныстардың қайсысы динамикалық бағыттауға қолданылмайды?

а) маршрутизаторлар мәліметтерді бөліседі

б) RIP қажет етеді

в) OSPF талап етеді

г) Бағыттау кестелеріне қолмен қолдау көрсетіледі

д) үлкен желілерде қолдану орынды

4. Сіздің желіңіз компьютер атауларын анықтау үшін таратылатын хабарларды пайдаланады. Microsoft технологиясы мұндай хабарламаларға деген қажеттілікті қалайша шектей алады?

а) DNS серверін орнатыңыз және күйге келтіріңіз

б) DHCP ретрансляция агентін орнатыңыз

в) DHCP серверін орнату және қалпына келтіру

г) сенімді WINS агентін орнатыңыз

д) WINS серверін орнату және қалпына келтіру

5. Маршрутизация кестесіне қай қызметтік бағдарламаның көмегімен жаңа жолдарды қосуға болады? .

а) ping

б) trasert

в) inconfig

г) route

д) arp

6. Сіздің TCP / IP желіңіз әрқайсысы 4 ішкі және 30 түйіннен тұрады. Ішкі желілердің біреуі үшін IP мекенжайларын автоматты түрде қалпына келтіру керек. Сіз қандай құралды орнатып, конфигурациялауыңыз керек?

а) DNS

б) DHCP

в) ЖЕҢІЛДЕР

г) HOSTS файлы

д) LMHOSTS файлы

7. Хост атауларын анықтау әдістерінің қайсысы тұрақты мәтіндік файлды қолданады?

а) DNS

б) ҚОНАҚТАР

в) LMHOSTS

г) домендік атаулар кеңістігі

д) WINS

8. Жергілікті желідегі адресті анықтаған кезде кэшті тексергеннен кейін компьютер не істейді?

а) маршрутизаторға сұраныс жібереді

б) HOSTS файлына қөмек сұрау

в) ARP серверіне сұранысты жібереді

г) хабар таратуға сұраныс жібереді

д) DNS серверіне сұранысты жібереді

9. Cisco маршрутизаторы үшін NAT-ті конфигурациялау кезінде қандай ішкі жергілікті мекенжай қолданылады?

а) сыртқы желіде саналатын ішкі түйіннің IP мекенжайы

б) ішкі торапта саналатын сыртқы түйіннің IP мекенжайы

в) ішкі желідегі болып саналатын ішкі түйіннің IP-мекен-жайы

г) сыртқы желідегі түйінге тағайындалған, қалпына келтірілген IP мекен-жайы

10. Төмендегі пәрмендер көмегімен маршрутизаторды конфигурациялау кезінде NAT-ты динамикалық аудару үшін қанша мекен-жайы қолжетімді болады?

Router(config)#ip nat pool TAME 209.165.201.23 209.165.201.30 netmask 255.255.255.224   
Router(config)#ip nat inside source list 9 pool TAME

а) 7

б) 8

в) 9

г) 10

**№3 жаттығу Мәлімдемені растаңыз немесе жоққа шығарыңыз**

Келесі сөйлемдерден Иә немесе Жоқ таңдаңыз.

1. NAT мекенжайы intranet желілерін жекешелендіруге байланысты тіркелген адрес схемасын сақтайды. Иә. Жоқ.

2. DHCP маршрутизаторларды, коммутаторларды және серверлерді қалпына келтіруге арналмаған, өйткені түйіндерде статикалық IP мекенжайлары болуы керек. Иә. Жоқ.

3. FTP - бұл компьютерлер арасында хабарламалар мен электрондық пошталарды жіберуге арналған ең көп таралған хаттама. Иә. Жоқ.

4. Windows сокеті TCP / IP тобының желілік интерфейсі деңгейінде болады. Иә. Жоқ.

5. Домен - бұл IP желісіндегі TCP / IP түйіндерінің логикалық тобы. Иә. Жоқ.

6. DNS атаулар кеңістігі сызықтық құрылымға ие. Иә. Жоқ.

7. HTTP хаттамасы - екі бағытты байттық байланысын қамтамасыз ететін хаттама. Иә. Жоқ.

**№ 4 Қолданбалы тапсырмалар**

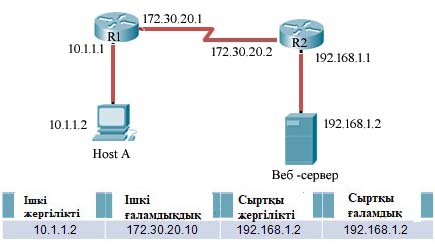
1. Сіз өзіңіздің DHCP серверіңізді ішкі желідегі тұтынушылық компьютердің IP мекенжайларын автоматты түрде бөлетіндей етіп к\қалпна келдірдіңіз. Тұтынушылық компьютерлер IP-мекен-жайын жалға алғаннан кейін дәл 10 күн өткен сайын оны жаңартуға тырысуы үшін не істеу керек?

2. Компьютер LNHOSTS файлын және WINS серверін атауларын рұқсат ету үшін пайдалануға келтірілген. Басқа компьютерге қалай қосылуға болады?

3. Сіз желідегі барлық компьютерлер үшін, тіпті WINS-ті қолдамайтын компьютерлер үшін атаулардың автоматты ажыратылымдығын қамтамасыз еткіңіз келеді. Бұл үшін желіні қалай орнатуға болады?

4. Сіз A, B, C ішкі желілерінің жобасын жасайсыз. Тек А ішкі желісінде орнатылған және келтірілген DHCP сервері бар. В және С ішкі желілерінің тұтынушылары IP-мекенжайларды А ішкі желісінде орналасқан DHCP серверінен ала алатындай етіп қалай конфигурациялау керек?

Суретке қараңыз R1 маршрутизатор 10.1.1.0/24 ішкі желі үшін NAT түрлендіруін орындайды. Веб-серверге HostA түйіні сұраныс жіберді. Веб-сервергмен қайтарылған пакет қандай белгіленген IP мекенжайға ие болады?



## 2.4. Корпоративтік желідегі коммутация және бағыттау

2.4.1 Коммутация және желіні сегментациялау

Ethernet деректерін беру – тұрақтылық пен сенімділіктің болмауы. Бұл жартылай дұрыс, CSMA/CD алгоритмі осы принцип бойынша жұмыс істейді. Осы кемшіліктерді жою үшін 1990 жылы Kalpana (кейіннен Cisco сатып алған) Ethernet сегментінің коммутация технологиясын ұсынды. Осылайша, бөлінген орта (соқтығысулардың домені) шектелмеген (көпірлер немесе маршрутизаторларды пайдалану), соңында мүлдем жоғалады. Бұл жұмыс қарапайым түрде құрылған, сол кезде қол жетпейтін технологиялық кезеңде әр түрлі порттарда кіріс жақтаулардың параллель өңделуіне негізделеді (көпірлер кадрды тізбектей, кадрдан кадрға дейін өңдейді). Бұл мүмкіндік Kalpana коммутаторларына әр жұп порттарының арасында кадрларды дербес беруге және ортақ ортадан бас тарту туралы тартымды идеяны жүзеге асыруға мүмкіндік берді. Трафикті бір қосылған құрылғыдан басқаларға тарататын концентратордан айырмашылығы, коммутатор деректерді тек алушыға тікелей жібереді. Бұл желінің өнімділігі мен қауіпсіздігін жақсартады, желінің басқа сегменттеріне олар үшін арналмаған мәліметтерді өңдеуге қажеттілікті (және мүмкіндікті) жояды.

Коммутаторлар (көпірлер сияқты) желі деңгейінің протоколдары үшін ашық, бағыттаушылар «оларды көрмейді». Бұл желінің негізгі жұмыс сұлбасын өзара ауыстырмауға мүмкіндік берді.

Коммутатор OSI моделімен каналдық деңгейде жұмыс істейді, сондықтан, жалпы жағдайда, ол тек сол желі түйіндерін өздерінің MAC адрестері бойынша біріктіре алады. Маршрутизаторлар желілік қабат негізінде бірнеше желілерді қосу үшін қолданылады.

Кадр көпір интерфейсіне келгенде, көпір раманы хаб сияқты барлық басқа интерфейстерге көшірмейді (жібермейді), бірақ кадрдың құрамындағы тағайындалған мекенжайды (MAC арқылы) тексереді және рамканы қабылдағышқа апаратын интерфейс арқылы жіберуге тырысады.



Көпірлерде өзіндік оқу мүмкіндігі бар:

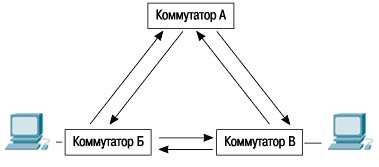
- Бастапқыда көпірдің кестесі бос;

- Кадр келгенде тағайындалған орын кестеде болмаса, көпір жақтаудың көшірмесін барлық порттарға жібереді (CSMA/CD);

- Әрбір алынған кадр үшін көпір өз кестесінде жіберушінің адресі мен порт нөмірін сақтайды, онда порт номері, кадр қайдан келді және келу уақыты (егер әр түйін кадр арқылы берілсе, онда кесте толы!) толық жазылады.



Кадр тағайындалған кестедегі порттардың біріне жеткенде, көпір жақтауды тиісті портқа жібереді. Егер белгілі бір уақыт ішінде (қартаю уақыты) көпір белгілі бір адрестен кадр алмаса, онда мұндай адрестер кестеден жойылады. Алушы мекен-жайы 01: 12: 23: 34: 45: 56 болатын кадр 2 порттан келді делік. Егер бұл мекен-жай кестеде болмаса, онда көпір өз кестесін қосады. Қартаю уақыты 60 минут деп есептейік. Содан кейін 62: 10: 22-ге дейін: FE: F7: 11: 89: A3 ешқандай кадрлар келмесе, ол кестеден жойылады. Егер желіде жаңа станция пайда болса, ол таратылатын кадрды жақын көпірге жібереді. Көпір жаңа мекен-жайды мәліметтер базасына жазады және кадрларды барлық порттарға жібереді. Кадр басқа көпірлерге кіреді және логикалық цикл арқылы оралады, мекенжайлар базасында жаңа өзгеріс тудырады. Яғни, логикалық ілмектер эфирдегі дауылдарға және көпірлерді дұрыс үйрете алмауына әкеледі. Логикалық цикл мысалы 2.13 суретте көрсетілген.



2.13 сурет – Логикалық цикл

2.4.2. STP хаттама

Spanning Tree Protocol (STP) арнайы «түбір коммутаторын таңдау» амалын қолданып логикалық ілмектерді жояды. Бұл амал конфигурация кезінде әкімшінің қосқыштарына тағайындалған идентификаторларға негізделген. Ең жоғары басымдылық сәйкестендіргіштің ең төменгі мәніне сәйкес келеді. Амалдың басында барлық коммутаторлар BDPU пакеттерін жібереді, онда олар өздерінің адрестері мен идентификаторын түбірлік қосқыштың адресі ретінде көрсетеді. Төменгі идентификаторы бар коммутатор түбір ретінде көрсетілген пакетті алғаннан кейін, коммутатор пакеттерді жібере бастайды, онда төменгі идентификаторы бар жаңа қосқыш түбір ретінде көрсетілген. Осылайша, барлық қосқыштар ағаштың түбірінде қайсысы орналасқандығын біледі.

Түбір қосқышы анықталғаннан кейін, ағаштың құрылымын анықтау кезеңі басталады. Енді тек түбірлік қосқыш BDPU пакеттерін жібереді. Ағаштың құрылымын анықтау үшін әр қосқыштан түбіоге дейінгі ең қысқа жол анықталады. BDPU пакеттік пішіні түбірге апаратын жолдың құнын қамтиды және пакетті алған әрбір қосқыш осы өріске өз құнын қосады және пакетті түбірден басқа барлық порттарға жібереді. Құнын беру әкімшімен орындалады немесе әдепкі бойынша анықтайды; бұл жағдайда ол 1000/S тең, мұндағы S – порттың жылдамдығы, Мбит/с-қа тең. Әр қосқыштың түбірлік портына BDPU пакетіне келетін түбір коммутаторынан ең төменгі құны бар порт тағайындалады.

BDPU пакеттерін құны неғұрлым жоғары немесе оған тең болатын түбір қосқышынан алатын порттар уақыт өте келе желілік топологиядағы ілмектерден шығатындықтан оқшауланған күйге келтіріледі.

Оқшауланған күйдегі порт BDPU пакеттерін әрі қарай жіберместен қабылдайды. Барлық басқа трафик қабылданбайды немесе берілмейді. Порт оқшауланған күйден шығуы мүмкін, егер ол белгілі бір уақыт ішінде BDPU пакетін алмаған болса, бұл кез келген себептен желі конфигурациясының өзгеруін білдіреді.

Оқшауланған күйден шығу тек тыңдау арқылы орындалуы мүмкін, бұл қайта конфигурация кезінде жаңа топологияны дұрыс анықтамау қаупін азайтуға арналған кідірісті білдіреді. Шын мәнінде, тыңдау кезінде порт конфигурацияны өзгертуі қажет екендігін растайды. Егер BDPU пакеттері тыңдау кезінде алынбаса, порт оқу күйіне өтеді, яғни оған қосылған станциялардың мәліметтер базасын құру қажет. Оқу кезеңін тыңдау мерзіміне тең болғаннан кейін порт беру режиміне өтеді, яғни ол толық жұмыс істейді.

2.4.3 Қосқыштар

Функционалды түрде, көп портты қосқыш көп портты көпір қызметін атқарады, яғни ол байланыс деңгейінде жұмыс істейді, жақтау тақырыптарын талдайды, мекен-жай кестесін автоматты түрде құрастырады және осы кестеге сүйене отырып, кадрды шығыс порттарының біріне бағыттайды немесе оны буферден шығарады. Инновация – бұл жақтаулардың параллель өңделуі, ал көпір жақтаулармен өңделеді. Қосқышта әдетте бірнеше ішкі кадрларды өңдейтін процессорлар болады, олардың әрқайсысы көпір алгоритмін орындай алады. Осылайша, қосқыш ішкі параллелизмге байланысты жоғары өнімділікке ие мультипроцессорлы көпір деп болжауға болады.

«Қосқыш» терминін түсіндіруде кейбір келіспеушіліктер бар. Классикалық анықтамаға сәйкес, қосқыштар екі деңгейлі OSI-де жұмыс істейді және көпір сияқты жұмыс істейді. Көпір мен қосқыштың айырмашылығының мәні мынада, көпір сақтау-тарату құралы ретінде жұмыс істейді, бірақ қосқыш істемейді. Қосқыш тағайындалған адресті декодтағаннан кейін бірден тиісті портқа кадр жібереді. Трансмиссия дереу басталады, тіпті кадр әлі толық қабылданбаған болса да.

Қосқыш – бұл желілік концентратор түрінде жасалған және көп порттты көпір рөлін атқаратын құрылғы, біріктірілген коммутация механизмі жергілікті желіні сегментациялауға, сонымен қатар желінің соңғы станцияларына өткізу қабілеттілігін бөлуге мүмкіндік береді.

Мұндай жүйенің артықшылығы - оның жоғары жылдамдығы. Кемшілігі - қосқыш барлық кадрды, сонымен қатар бүлінгендерін де жібереді. Қосқыштың көпірден айырмашылығы, бір уақытта бірнеше жіберушілерден бірнеше алушыларға (ішкі желілерге немесе жеке құрылғыларға) деректерді жіберуге қабілетті. Бұл LAN қосқыштары. (WAN қосқыштары бар).

Қосқыштың жұмысының техникалық негізі өте қарапайым: оның кірісіне (source port) кіретін кадр барлық белсенді порттарға емес (концентратор сияқты) тек MAC адрес құрылғысына қосылған кадрдің адресімен (destination port) сәйкес келетін құрылғыларға бағытталады. Сәйкесінше шешілуі керек бірінші мәселе – коммутациялық порттардың қосылған құрылғыларға (дәлірек айтқанда, олардың MAC мекенжайларына) сәйкестігі. Жұмыс үшін арнайы корреспонденттік кесте қолданылады (content-addressable memory, CAM), ол коммутатор «өзін-өзі оқыту» процесінде келесі принципке сәйкес туындайды: егер порт құрылғыдан физикалық Х адрестен жауап алса, CAM кестесінде сәйкес сәйкестік алмасу сызығы пайда болады.

Кестеде тағайындалған адресі (destination address, DA) бар кадрлар тиісті портқа жіберіледі. Бұл жағдайда барлық түйіндерге арналған немесе белгісіз тағайындалған адрес DA барлық белсенді порттарға жіберіледі.

Жұмыс кезінде қосылған жабдықтың нақты адресі өзгеруі мүмкін. Сонымен қатар кестеде жаңа жазба пайда болады. Егер бос орын болмаса, ең ескі жазба жойылады (толтыру қағидасы).

Алайда, мұндай жеңілдетілген алгоритм қиын (өзгеріссіз) тек басқарылмайтын қосқыштарда (Dumb) қолданылады. Бұл арзан, қарапайым құрылғылар, хабтарды қарапайым желілердің торынан сәтті шығарады. Әдетте, оларда порттардың саны аз, «кеңсе» өнімі және жоғары техникалық сипаттамалары жоқ. Әкімшіні басқару мүмкіндігі жоқ. Дамытудың келесі қадамы қосқыштарды қосу (Smart). Оларда әкімші көптеген маңызды конфигурация параметрлерін өзгерте алады, олар тек бір рет оқылады (жүктеу кезінде). Мысалы, осылайша сіз «өздігінен білім алу» тетігін оқшаулай аласыз (портативті хат алмасудың MAC адрестерімен статистикалық кестесін құра аласыз), сүзгілеуді, виртуалды желілерді орнатуды, жылдамдықты орнатуды және тағы басқаларды орындауға болады. Бірақ ең үлкен мүмкіншілік басқарылатын қосқыштарда (Intelligent) бар. Оларда толыққанды процессордың интерфейсі бар (дәлірек айтқанда, компьютер, өйткені оның да жадысы бар), ол сізге қайта жүктеместен басқару және құрылғы параметрлерін өзгертуге мүмкіндік береді. Сондай-ақ, пакеттерді нақты уақыт режимінде бақылауға, трафиктің өтуін және т.б. бақылауға болады.

Дегенмен, мүмкіндіктер деңгейінің (және шығындар) үлкен айырмашылығына қарамастан, жалпы қағида өзгеріссіз қалады. Барлық түйіндер «бөлек» арналарға толық өткізу қабілеттілігімен қосылады (егер бір уақытта бірнеше құрылғылардың біреуінде енгізу болмаса) және бір-біріне күдік келтірмей жұмыс істей алады.



«Қосқыш» термині мыналарға қолданылады:

1. конфигурацияны ауыстыру;

2. коммутациялық кадрлар;

3. коммутациялық ұяшықтар;

4. фреймдер мен ұяшықтар арасындағы түрлендірулер.

«Коммутация» жалпы термині мыналарға қолданылады:

1. Қарапайым жеке жұмыс тобының қосқыштары;

2. Екінші санаттағы жұмыс топтарының қосқыштары бір немесе бірнеше порттардың сервермен немесе негізгі желімен жоғары жылдамдықты байланысын қамтамасыз етеді;

3. Кәсіпорын бөлімінің желілік қосқыштары;

4. Желілік коммутаторлар.



2.4.4 WAN-қосқыштары

Интернетте WAN қосқыштарының мағынасы мүлдем басқаша. Олар, әдетте, деректер байланысы қабатында жұмыс істейді, бірақ кейбір модельдер желілік деңгей функцияларын ішінара қолдана алады. Сондықтан қазіргі заманғы қосқыштарды көпірмен емес, маршрутизатормен салыстырған дұрысырақ. Қорытынды: заманауи қосқыш жоғары жылдамдықтағы маршрутизаторға, ал классикалық қосқыш жоғары жылдамдықтағы көпірге ұқсайды. Қазіргі заманғы қосқыш коммутатор портына әртүрлі тәсілдермен орналастырылған желілік қабат адрестерін анықтау арқылы деректер пакеттерін шешеді (мысалы, ARP потоколдарымен). Бір жіберушіден сол алушыға кейінгі деректер пакеттері деректер байланысының деңгейінде ауысады, ал маршрутизаторлар мұны желілік деңгейде жасайды. Сонымен қатар, қосқыштар маршруттау хаттамаларына қатыспайды.

Көптеген қосқыштардың архитектурасы басқару және трафикті тасымалдау функцияларын бөлуді қарастырады. Уақыттың критикалы басқарушылық міндеттерін RISC процессорлары орындайды және коммутатордың әр түрлі желілік қызметтермен (қауіпсіздік, инвентаризация және т.б.) интеграциялануы амалдық жүйеге негізделген.Сондықтан бір өнімдегі желілік қосымшалар мен қызметтерге бағдарламалық қамтамасыз етуді қолдана отырып, трафиктің жоғары жылдамдығын өңдеуді үйлестіруге мүмкіндік береді, қызметі жоғары техникалық және экономикалық нәтижелерді алуға мүмкіндік береді. Бұл жағдайда амалдық жүйе арқылы келіп түскен сұраныстар мен нұсқаулар ASIC микросұлбаларының (Application Specific IC) коммутациясының сүзгі кестелеріне жазылады. Соңғысы 2, 3, 4 деңгейлі OSI ақпаратына негізделген жіктеуді орындау кезінде физикалық арналардың толық жылдамдығына жіберіледі.

Егер концентратор барлық қосылған құрылғыларға желілік трафикті тарататын болса, коммутатор екі құрылғы / қосалқы жүйелер арасында нүкте-нүкте байланысын қамтамасыз етеді. Ethernet-ке келетін болсақ, өткізу қабілеттілігі жұмыс станциялары арасында бөлінбейтін, бірақ толықтай пайдаланылған кезде коммутатор қосылған Ethernet-ті қамтамасыз ете алады. Осы тұрғыдан алғанда, Ethernet-ті ортақ тарату ортасы арқылы жүзеге асыратын құрылғы – хаб (Hub), ал таратылған тарату құралы – коммутатор (Switch). Коммутаторлар бірден бірнеше құрылғылар арасында жылдам ақпарат алмасуды қамтамасыз етеді. Бұл жерде бастысы - коммутаторлардың қажетті кадрларды дұрыс адреске жіберу мүмкіндігі емес, олардың бірден параллель ақпарат алмасу арналарын қолдау мүмкіндігі. Мұндай виртуалды желінің жалпы өткізу қабілеті секундына гигабитті құрады.

2.4.5 Қосқыштарды баптау

Телекоммуникациялық жабдыққа қосылу үшін терминалдық бағдарламалар қолданылады. Қазіргі уақытта көптеген бағдарламалар бар, мысалы, Secure CRT, Solar Winds және т.б. Бұл параметр Windows стандартты пакетіне кіретін Hyper Terminal бағдарламасын пайдаланады.

Маршрутизаторлар мен коммутаторлар Интернетке арналған арнайы операциялық жүйесіз жұмыс жасай алмайды (IOS). Әрбір Cisco маршрутизаторы / коммутаторы Cisco IOS жүйесінің бағдарламалық жасақтамасын анықтайтын және жүктейтін стандартты жүктеу жүйесімен алдын ала құрылған.

Маршрутизатор / коммутатор іске қосылғанда жүктеу процедурасы орындалады (өзіндік жүктеу бағдарламасы, bootstrap), содан кейін операциялық жүйе және конфигурация файлы жүктеледі. Егер жабдық конфигурация файлын таба алмаса, ол бастапқы конфигурация режиміне өтеді. Алғашқы конфигурация диалогын орындағаннан кейін жаңа конфигурация файлының резервтік көшірмесі энергияға тәуелсіз жадыға жазылады (Non Volatile Random-Access Memory – NVRAM жады).

Стандартты Cisco IOS бағдарламалық қамтамасыз етуді жүктеу жолының мақсаты - маршрутизаторды қосу/қосу және жұмыс істеу. Маршрутизатор / коммутатор көрсетілген конфигурацияға сәйкес қызмет етуі керек пайдаланушылық желілерге қосылымдардың сенімді жұмысын қамтамасыз етуі керек.

Қауіпсіздік мақсатында, маршрутизаторлар/қосқыштарда командалық қол жетімділіктің екі деңгейі бар:

- EXEC пайдаланушысы режимі. Бұл режимнің негізгі мақсаты – маршрутизатордың/коммутатордың күйін тексеру. Бұл режимде маршрутизатордың/коммутатордың конфигурациясын өзгертуге тыйым салынады.

- EXEC артықшылық режимі. Бұл режимнің негізгі мақсаты - маршрутизатордың конфигурациясын өзгерту.

Маршрутизатор жүйесіне кіргеннен кейін пайдаланушы EXEC режиміне кіргені туралы хабарлама пайда болады. Осы деңгейде енген командалар барлық артықшылықты режим командаларының жиынтығы болып табылады. Мұндай командалар маршрутизатордың параметрлерін оның конфигурациясын өзгертпестен көру үшін жеткілікті.

Командалардың толық жиынтығына ену үшін артықшылықты режимді енгізу керек.

Switch> **en**

Switch#

**Коммутаторға атау беру**

Коммутаторға атау беру үшін **hostname** командасы қолданылады.

Switch#

Switch#**configure t**

Switch(config)# **hostname 2950**

2950(config**)#exit**

2950#

**Интерфейс конфигурациясын қарау**

Барлық интерфейстердің статистикасын көрсету үшін show interfaces енгіземіз.

2950# **show interfaces**

**Жүйелік уақытты құру**

Жүйе уақытын орнату үшін clock set енгіземіз.

Switch#**clock ?**

Set Set the time and date

Switch#**clock set?**

Hh:mm:ss Current Time

Switch#**clock set 10:25:00?**

<1-31> Day of the month

MONTH Month of the year

Switch#**clock set 10:25:00: 25 ?**

MONTH Month of the year

Switch#**clock set 10:25:00: 25 may ?**

<1993-2035> Year

Switch#**clock set 10:25:00: 25 may 2006?**



**Коммутаторда парольдерді орнату**

Коммутаторда парольдерді орнату қажет, өйткені жабдыққа рұқсатсыз кіруге тыйым салынуы керек.

Пароль төрт таңбадан, сегізден аспауы керек. Коммутатор 2950 санын CLI интерфейстің IOS кіруге қолданады, пайдаланушы мен артықшылық режимдердің паролін орнату командалары маршрутизатордағы командалардан өзгеше.

Маршрутизаторларда қолданылатын құпия сөзді қосу командасын енгізіңіз.

Switch(config)# **enable password?**

**Level Set exec level password**

Switch(config)# **enable password level?**

**<1-15> Level number**

Пайдаланушы режимінің құпия сөзін енгізу үшін 1 деңгей қолданылады, ал рұқсат етілген режим үшін құпия сөзді енгізу үшін 15 деңгей қолданылады.

Switch(config)# **enable password level 1 student?**

Switch(config)# **enable password level 1 teacher?**

Switch(config)# **exit**



***Cisco Catalyst қосқыштарында құпия сөзді қалпына келтіру***

2950 коммутаторда парольді қалпына келтірген кезде, іске қосылудың алдын алу үшін алдыңғы панельдегі режим батырмасын 30 секунд бойы ұстап тұру керек.



* 1. Сурет – Catalyst 2950 коммутаторының алдыңғы панелі

Бұл жағдайда жүйені үктеуді аяқтау үшін флэш-файлды жіберместен бұрын тоқтатылды:

switch:**flash\_init**

switch:**load\_helper**

switch:**dir flash: (флэшті көру үшін)**

switch:

switch:

switch:**rename flash:config.text flash:config.old** (жүктеу файлының атын өзгерту)

switch:

switch:**boot**

Артықшылықты режимге ауысу.

switch:**en**

switch#

config.old flash: config.text командасымен конфигурация файлын бастапқы атауына өзгертеді.

switch:# **flash:config.old flash:config.text**

switch#

Конфигурация файлын жадыға көшіру.

switch:# **copy flash:config.text system:running-config**

switch#

Конфигурация файлы қайта іске қосылды. Құпия сөзді өзгерту.

switch:# **configure terminal**

switch(config):# **no enable secret**

switch(config):# **no enable password Cisco**

switch(config):# **^Z**

Ағымдағы конфигурацияны жазуды жадының командасымен сақтау.

switch:# **write memory**

switch#

## 2.5. Коммутатор базасы бойынша виртуалды желі

2.5.1 Виртуалды желі

Виртуалды жергілікті желі (ЖЖ) (Virtual Local Area Network, VLAN) – бұл 2 деңгейдегі коммутатордағы әкімшілік анықталған порттарға қосылған желілік пайдаланушылар мен ресурстарды логикалық топтау. Виртуалды жергілікті желілер әр түрлі қосалқы порттарды әр түрлі ішкі желілерге беру арқылы коммутатор ішінде кіші таратылым домендерін құруға мүмкіндік береді. Виртуалды жергілікті желі жеке ішкі желі немесе таратушы доменге айналады, ал тарату кадрлары сол виртуалды ЛВС порттары арасында ауысады.

Виртуалды жергілікті желілерді пайдалану құрылғылар мен пайдаланушылардың нақты орналасқан жеріне байланысты жұмыс топтарын құру қажеттілігін жояды. Виртуалды жергілікті желілерді құрылғылардың орналасқан жеріне, орындалатын функцияларға, ұйымдастыру бөліміне және ресурстардың немесе пайдаланушылардың қай жерде орналасқанына қарамастан, қолданылған қосымшаның немесе хаттаманың негізінде ұйымдастыруға болады.

**Виртуалды жергілікті желінің артықшылықтары**

2 деңгейде коммутаторлары домендерідің соқтығысуын сегментациялайды, бірақ тек маршрутизаторлар тарату домендерін сегментациялай алады. Виртуалды жергілікті желілері 2 деңгейлі коммутацияланған желілерінде тарату домендерін сегментациялай алады. Сонымен қатар, 2-ші деңгейдегі біріктірілген желіде әртүрлі виртуалды ЛЖ арасындағы байланыс үшін маршрутизаторлар қажет.

Біріктірілген желіде виртуалды ЖЖ құрудың көптеген артықшылықтары бар. 2-ші деңгейде коммутацияланған желіде желі тегіс болады. Әрбір тарату пакетін, құрылғы осы деректерге мұқтаж ба, жоқ па, қарамастан, барлық желілік құрылғылар қабылдайды. Тегіс желіде қауіпсіздік шаралары құпия сөзбен ғана шектеледі және кез-келген құрылғы кез-келген қолданушыға қол жетімді. Құрылғылардың таратылуына және пайдаланушылардың оған жауап беруге тырысуына жол бермеу мүмкін емес. Қауіпсіздік серверлердегі және басқа құрылғылардағы парольдермен қамтамасыз етіледі. Виртуалды ЖЖ құру 2-ші деңгейдің коммутациясының көптеген мәселелерін шешуге көмектеседі.

**Кең таратылымды басқару**

Тарату кез-келген хаттамада жүзеге асырылуы мүмкін, бірақ оның жиілігі хаттамаға, біріктірілген желіде жұмыс істейтін қосымшаларға және осы функциялардың қалай қолданылатынына байланысты. Виртуалды жергілікті желілер кішігірім тарату домендерін бөле алады, яғни қолданбаны оны пайдаланбайтын сайттарға таратуға тыйым салуға мүмкіндік береді.

Ескі қосымшалар өткізу қабілетін немесе өткізу жолағын азайтуға арналып есептлеген болса, ал жаңа қосымшасы өткізу қабілеттілігін барынша кең қолданады. Бұл мультимедиялық қосымшалар, олар эфирді және мультикастты көп пайдаланады. Сенімсіз жабдық, жеткіліксіз сегментация және нашар ұйымдастырылған брандмауэр ақпараттық бюллетеньді белсенді түрде қолданатын қосымшалармен байланысты ақауды ушықтыруы мүмкін.

Өткізгіштің кең өткізу қабілеттілігін қажет ететін бағдарламалар желінің дизайнына жаңа фактор қосады, себебі хабар тарату коммутацияланған желі арқылы таратыла алады. Әдетте, маршрутизаторлар тек бастапқы желіде таралады, ал 2-ші деңгей коммутаторлары барлық бөлімдерге хабар таратады. Мұндай желі тегіс деп аталады, өйткені ол бірыңғай тарату домені.

Желінің дұрыс орналасуын қамтамасыз ету әкімшінің міндеті болып табылады, сондықтан бір желінің орналасқан жеріндегі мәселелер бүкіл желіге таралмайды. Бұл үшін ең тиімді құрал – бұл коммутация және маршруттау. Коммутаторлар құны бойынша қол жетімді болғандықтан, көптеген компаниялар концентратордан, маршрутизатордан тұратын жалпақ желілерді таза қосылған желілерге және виртуалды ЖЖ-ге ауыстырады. Виртуалды жергілікті желілерімен берілген коммутаторлардың ең үлкен артықшылығы барлық виртуалды ЛЖ құрылғылары бірдей таратылатын доменде және барлық хабарларды қабылдайды. Әдетте, коммутаторда орналасқан және бірдей виртуалды ЖЖ жатпайтын барлық порттар сүзіледі.

Таратылым бүкіл желі бойынша таратылмауы үшін желі (виртуалды ЖЖ) арасындағы байланысты қамтамасыз ететін маршрутизатор, 3-ші деңгейлі коммутаторы немесе Route Switch Module (RSM) қажет.

***Виртуалды жергілікті желі шекараларын анықтау***

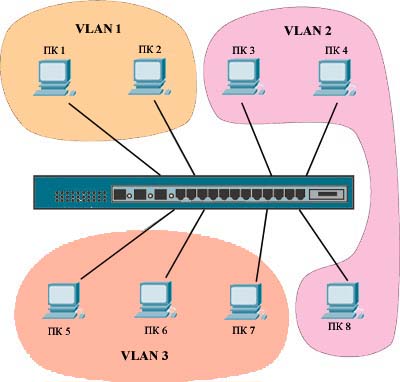
Коммутациялық блокты құру кезінде виртуалды ЖЖ-ның екі негізгі түрін білу керек:

- Аяқталатын виртуалды ЖЖ

- Жергілікті виртуалды желі

***Виртуалды жергілікті желілер*** барлық коммутациялық құрылғыларды өзара байланыстырады; жергілікті желідегі барлық қосқыштар барлық конфигурацияланған виртуалды желілер туралы ақпаратты алады. Бұл конфигурация функциялар, жобалар, бөлімдер және т.б. негізінде топтар құруға мүмкіндік береді.

Аяқталған жергілікті желілердің ең үлкен артықшылығы – пайдаланушылар физикалық орналасуларына қарамастан нақты виртуалды жергілікті желіге тағайындала алады. Әкімші пайдаланушының виртуалды ЖЖ мүшесі ретінде қосылған портты анықтайды. Егер пайдаланушы қозғалса, әкімші оған жаңа портты сол виртуалды желінің мүшесі ретінде анықтайды. 80/20 ережесіне сәйкес, виртуалды жергілікті желі құру кезінде әкімшінің міндеті - желілік трафиктің 80% жергілікті болып қалуын қамтамасыз ету, яғни виртуалды ЖЖ ішінде тек 20% немесе одан азы ғана виртуалды ЖЖ-ден тыс бола алады.



2.15 сурет – Бір коммутаторға құрылған виртуалды желілер.

***Жергілікті виртуалды желі*** физикалық орналасуларға сәйкес конфигурацияланған және функцияларға, жобаларға, бөлімдерге және т.б. негізделмеген, мысалы, виртуалды жергілікті желі. Жергілікті виртуалды ЛЖ желілері орталықтандырылған серверлік блоктары мен үлкен компьютерлері бар ұйымдарда қолданылады, өйткені бұл жағдайда виртуалды жергілікті желіге қызмет көрсету қиын болады. Басқаша айтқанда, 80/20 ережесін 20/80 ережесімен ауыстырған кезде, жергілікті виртуалды желілерге қарағанда виртуалды жергілікті желіге қызмет көрсету қиынырақ болады.

Аяқталған виртуалды жергілікті желілерден айырмашылығы, жергілікті желілер кеңістіктік орналасуына сәйкес конфигурацияланған; орналасу бірлігі ғимараттағы немесе ғимараттағы кеңсе болуы мүмкін, бұл қосқыштардың мөлшеріне байланысты. Кеңістіктегі виртуалды жергілікті желілер серверлік ферма сияқты орталықтандырылған ресурстарды қолданған кезде жобаланады. Пайдаланушылар уақытының көп бөлігін осы орталықтандырылған ресурстармен сұхбаттасуда өткізеді, ал уақыттың 20% (немесе одан аз) жергілікті желіде болады. Демек, трафиктің 80% -ы 3 деңгейлі құрылғыны кесіп өтеді, бір қарағанда, бұл тиімсіз болып көрінеді.

3-ші деңгейдегі құрылғылардың жылдамдығы артуына байланысты, жергілікті виртуалды желі 3-ші деңгейдегі ең жоғары жылдамдықты құрылғыларды қолдана алады, үлкен трафикті жеңе алады. Бұл құрылымның артықшылығы - пайдаланушыларға ресурстарды алдын-ала анықталған, дәйекті түрде алу әдісі ұсынылады. Бірақ қуаты 3-ші деңгейден аспайтын құрылғыда мұндай конфигурацияны құру мүмкін емес, сондықтан ол көп инвестицияны қажет етеді.

***Виртуалды жергілікті желі топтары***

Виртуалды ЖЖ құрғаннан кейін оларға коммутациялық порттарды тағайындау керек. Виртуалды ЖЖ портының конфигурациясының екі түрі бар: статикалық және динамикалық. Статикалық виртуалды ЖЖ жасау үшін аз жұмыс қажет, бірақ оны күту қиынырақ. Динамикалық виртуалды ЖЖ, керісінше, оны ұйымдастыруда көп жұмысты қажет етеді, бірақ оны күту оңайырақ.

***Статикалық виртуалды желілер***

Статикалық виртуалды ЖЖ-де әкімші оған ауысу порттарын тағайындайды, ал әкімші порт тағайындауды өзгерткенше бұл карта тұрақты болады. Бұл виртуалды ЖЖ құрудың әдеттегі және қауіпсіз әдісі. Бұл конфигурацияны ұйымдастыруға және басқаруға оңай, ал пайдаланушылардың қозғалысы іс жүзінде желілік орталықтардың есіктерін құлыптау арқылы басқарылады. Ыңғайлы болу үшін желіні басқарудың бағдарламалық жасақтамасын пайдалануға болады, бірақ бұл қажет емес.

***Динамикалық виртуалды желілер***

Егер әкімші басында аздап жұмыс істеуге және дерекқордағы барлық құрылғылардың аппараттық мекен-жайларын анықтауға келіссе, онда біріктірілген желіде виртуалды ЖЖ динамикалық тағайындалуын қамтамасыз етуге болады. Басқарудың бағдарламалық құралы динамикалық виртуалды ЖЖ құруға арналған аппараттық құралдарды (MAC), хаттамаларды немесе тіпті қосымшаларды шешуге мүмкіндік береді.

MAC мекенжайлары орталықтандырылған виртуалды ЖЖ басқару қосымшасына енгізілді делік. Егер осыдан кейін түйін тағайындалмаған коммутация портына қосылған болса, виртуалды желіні басқару дерекқоры аппараттық құралдың адресін тауып, сәйкес виртуалды ЖЖ үшін коммутаторды тағайындайды және құрады. Бұл әкімшіні басқаруды және конфигурациялауды жеңілдетеді. Егер пайдаланушы қозғалса, коммутатор оны қажетті виртуалды ЖЖ автоматты түрде анықтайды.

2.5.2 Магистральды хаттама

VLAN Trunk Protocol магистральдық хаттам (VTP) Cisco компаниясымен барлық виртуалды жергілікті желілерді коммутацияланған өзара байланысқан желіде басқару және бүкіл желі бойында біркелкілікті сақтау үшін құрылды. VTP хаттамасы әкімшіге виртуалды ЛЖ қосуға, жоюға және атын өзгертуге мүмкіндік береді, және бұл өзгертулер барлық қосқыштарға қолданылады.



VTP хаттамасы коммутацияланған желі үшін келесі артықшылықтарды ұсынады:

* Барлық желілік коммутаторлардағы виртуалды ЖЖ-ның біркелкі конфигурациясы
* Аралас желілерде, мысалы, Ethernet-тен АТМ-ге негізделген FDDI-ге дейінгі виртуалды жергілікті желілерін магистральдық желіге қосу мүмкіндігі.
* Виртуалды желілерді дәл қадағалау және бақылау.

- Виртуалды ЖЖ қосылуы туралы ақпаратты барлық қосқыштарға жедел хабарлау.

- Виртуалды ЖЖ-ні коммутацияланған желіге өздігінен кетіру.



VTP хаттамасына желінің виртуалды ЖЖ-ін басқаруға рұқсат беру үшін алдымен VTP серверін жасау керек. Виртуалды ЖЖ деректерін бөлісу қажет болатын барлық серверлерде бірдей домен атауы болуы керек. Коммутатор бір уақытта тек бір доменде бола алады; бұл тек бір VTP доменінде конфигурацияланған коммутаторлармен VTP доменінен деректерді айырбастай алатындығын білдіреді.

VTP доменін желіге қосылған бірнеше қосқышпен пайдалануға болады. Егер барлық желі коммутаторлары бірдей виртуалды ЖЖ-де болса, онда VTP қажет емес. VTP деректері магистральдық порттағы коммутаторлар арасында тасымалданады.

Коммутаторлар VTP басқару доменінің ақпаратын, сонымен қатар конфигурацияның қайта қарау нөмірін және белгілі параметрлері бар барлық белгілі виртуалды ЖЖ-ні таратады. Коммутаторларды VTP деректерін магистральдық порттар арқылы жіберетін, деректердің жаңартуларын қабылдамайтын немесе VTP дерекқорларын жаңартпайтын етіп қалыпқа келтіре алады. Бұл ашық VTP режимі.

Парольдер құру арқылы VTP доменінің қауіпсіздігін қамтамасыз етуге болады, содан кейін әр қосқыш бірдей құпия сөзге ие болуы керек және бұл күрделі болуы мүмкін. Егер қолданушыларды VTP доменіне санкцияланбаған қосулар мазаласа, онда пароль қою керек.

Виртуалды локальді желі (VTP) магистральдық арналарын қалыптастыруға арналған хаттама – виртуалды локальді желілерді басқару құралдарына ыңғайлы қосымша. Бұл желідегі бірнеше қосқыштарға виртуалдыЛЖ анықтамаларын автоматты түрде тағайындауға мүмкіндік береді.

VTP бағдарламалық қамтамасыз етуі коммутаторда үш режимнің біреуінде жұмыс істей алады: клиент, сервер және ашық.

VTP басқару домендері VTP параметрлерін басқару үшін қолданылады. Басқару доменінде VTP хаттамасын орындауға қатысатын барлық қосқыштардың білетін нақты атауы бар. Басқаша айтқанда, егер коммутатор VTP доменіне жатпаса, онда ол осы доменге жіберілетін виртуалды локальді желілер туралы ақпаратты алмайды. Коммутаторлар тек бір VTP доменіне ғана ие бола алады. Сонымен қатар, VTP доменінің дұрыс жұмыс істеуін қамтамасыз ету үшін бірқатар шарттар орындалуы керек.

Біріншіден, VTP домені үздіксіз болуы керек. VTP ақпаратының бір коммутатордан екіншісіне ауысуы үшін бұл қосқыштардың барлығы бір VTP доменінде болуы керек, ол бос емес.

Сонымен қатар, VTP туралы ақпарат магистральдық байланыстар жасалған порттар арқылы ғана таратылады. Сондықтан, егер магистральдық арналардың конфигурациясы дұрыс орындалмаса немесе магистральдық канал істен шықса, VTP ақпаратын беру тоқтатылады.

***VTP жұмыс режимдері***

VTP домені үш әрекет режимін қамтиды: сервер, клиент және ашық.

*VTP сервер режимі*

VTP серверінің режимі барлық қосқыштарда стандартты. Виртуалды ЛЖ деректерін домен бойынша тарату үшін VTP доменінде кемінде бір сервер қажет. Серверлік режимде келесі әрекеттерді орындау қажет:

* VTP доменінде виртуалды ЖЖ құруға, қосуға немесе жоюға болады

- VTP ақпаратын өзгерту; коммутатордың серверлік режимінің өзгерістері бүкіл VTP доменінде жарияланады

*VTP клиент режимі*

VTP клиенттері VTP серверлерінен мәліметтерді алады, жаңартуларды жібереді және алады, бірақ олар өзгеріс енгізе алмайды. Клиент қосқышындағы жаңа виртуалды ЖЖ проттары VTP серверінен бұрын ескертпестен қосу мүмкінн емес. Коммутатордың серверге айналуы үшін алдымен оны клиент ету керек, содан кейін ол виртуалды ЖЖ-де барлық қажетті ақпаратты алады; онда оны сервер ретінде анықтауға болады.

*VTP ашық режимі*

Ашық VTP қосқыштары VTP доменінің бөлігі емес, бірақ көрсетілген магистральдық арналардағы VTP хабарландыруларына жатады. Ашық қосқыштың конфигурацияланған магистральдық арналарға виртуалды ЖЖ хабарландыруларын жіберуі үшін VTP 2-ші нұсқасын пайдалану керек, әйтпесе ол ештеңе жібермейді. Ашық VTP коммутаторлары виртуалды желілерді қосып, жоя алады, өйткені олар өздерінің дерекқорларын қолдайды және оларды басқа қосқыштармен бөліспейді. Ашық қосқыштар жергілікті мағынаға ие.

***VTP бір қалыпқа келтіру***

VTP доменін орнатпас бұрын мыналарды орындау керек:

1. Пайдаланғыңыз келетін VTP хаттамасының қайта қарау нөміріне назар аудару.

2. Коммутатор қолданыстағы домен мүшесі болуы керек пе немесе жаңасын жасау қажет пе, жоқ па, соны анықтаңыз; бар доменге коммутаторды қосу үшін бар болса, домен аты мен құпия сөзді анықтау.

3. Өзара байланысқан желідегі әр коммутатор үшін VTP режимін таңдау.

***VTP нұсқасын*** ***бір қалыпқа келтіру***

Коммутаторларда VTP хаттамасының екі түрлі нұсқасын конфигурациялауға болады. 1 нұсқа - бұл барлық қосқыштардағы VTP стандартты нұсқасы, және көбінесе дәл солай қолданылады. 1-ші нұсқа үшін VTP нұсқасын конфигурациялау қажет емес. 1 және 2 тармақтар сәйкес келмейді, сондықтан қосқыштар үшін баптау бәрі немесе ештеңе емес дегенді білдіреді. Егер барлық коммутаторлар VTP 2 нұсқасымен үйлесімді болса, бір қосқышты ауыстыру барлық қосқыштарды өзгертеді. Барлық қосқыштардың 2-ші нұсқамен үйлесімді екендігіне сенімді болмасаңыз, абай болыңыз.

2-ші нұсқа келесі себептер бойынша қолданылады:

Token Ring виртуалды ЖЖ қолдауы Token Ring-ті қолдану үшін VTP 2-ші хаттама нұсқасы қажет, сондықтан барлық қосқыштар осы нұсқада жұмыс істеуге арналған болуы керек.

TLV қолдауы - белгісіз параметрлер типіне қолдау көрсету болып саналады, оған ұзындық - мән (тип - ұзындық - мән, TLV) жатады. Ұзындық мәні белгісіз параметрлері бар VTP хабарламасын алғаннан кейін, 2-ші нұсқа VTP қосқыштары өзінің магистральдық каналдары арқылы өзгерістерді таратады.

**Ашық режим.** Коммутаторлар ашық режимде жұмыс істей алады, ал олар тек хабарламалар мен ескертулерді дерекқорға қоспай жібереді. 1-ші нұсқада коммутатор доменнің атауын және нұсқасын жіберместен бұрын тексереді, ал 2-ші нұсқада VTP хабарламаларын нұсқаны тексерусіз жібереді.

Әдепкі бойынша қосқыш және қосқыштың басқа модельдері VTP сервер режиміне қосылады. VTP хаттамаларын қосу үшін алдымен домен атауын көрсету керек, одан кейін VTP параметр көмегімен конфигурация тексеріледі. Төменде көрсетілген мысалдың командасын қолданып қайтақосқыштарды серверлер режиміне қайта қосу қажет.

Switch (config)# **vtp?**

Switch (config)# **vtp server**

Switch (config)# **vtp domain Domen**

Switch (config)# **vtp password cisco**

Vtp show команда пайдаланып параметрлерді тексеріңіз:

Switch # **show vtp**

VTP доменіне жаңа қосқышты қоспас бұрын, дерекқорды жою керек. Коммутатордағы NVRAM-ны өшіру коммутатордағы VTP конфигурациясын жоймайды, өйткені VTP ақпаратында өзінің NVRAM жадысы бар. Коммутатордағы VTP ақпаратын жою үшін келесі команда қолданылады:

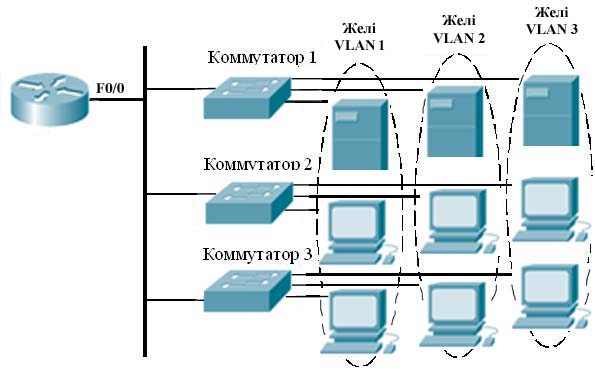
Switch #**delete?**

Switch #**delete vtp**

Команданы енгізгеннен кейін, VTP ақпаратын зауыттық әдепкі конфигурация мәндеріне орнатуға шақыру пайда болады.

2.5.3 Коммутаторда VLAN қосылымдарын құру

Виртуалды жергілікті желілерді конфигурациялаудағы бірінші қадам - әрбір VLAN желісіндегі пайдаланушылардың құрамын анықтау. VLAN желі санын және олардың мүшелерінің құрамын таңдап, VLAN желісін құруға болады. 2.16 суретіне сәйкес желіні құрастырыңыз.



2.16 сурет – VLAN-ды ұйымдастыру сызбасы.

Коммутатордағы VLAN-ді қосу үшін IOS орнату режиміне өтіу қажет. Қосу режиміне өту үшін **enable** енгізу керек, ал кеңейтілген конфигурация режиміне өту үшін **config t** енгізу керек.

Switch>**en**

Switch #**config t**

Стандартты IOS негізінде коммутаторда VLAN-ды құру үшін VLAN конфигурацияны құру режиміне өту қажет. Ол үшін **vlan** командасын енгізу қажет.

Switch (config)# **vlan 2**

Switch (config)# **name Sales**

Switch (config)# **vlan 3**

Switch (config)# **name Marketing**

Switch (config)# **vlan 4**

Switch (config)# **name Engineering**

Алайда, әдепкі бойынша, барлық ауысу порттарына сәйкес интерфейстің VLAN параметрлері тағайындалады және бұл интерфейс виртуалды желінің қай бөлігі болатынын көрсетеді.

VLAN желісін құрғаннан кейін олардың конфигурациясын **show vlan** командасымен тексереді.

**VLAN желінің коммутаторлық порттарын меншіктеу**

Анықталған VLAN желісінде порттарды құру switchport access vlan командасымен орындалады. VLAN желі порттарын қосу бір рет бір порттан ғана қосуға рұқсат береді. 2950 коммутаторында VLAN-ның бірнеше порттарды бір уақытта меншіктеу командасы болмайды. Порт үшін виртуалды жергілікті желінің мүшелігі статикалық немесе динамикалық болуы мүмкін.

3- VLAN 3 және 5 - VLAN 4 интерфейстерін меншіктеу командасын 2 - VLAN 4 интерфейс үшін келесі мысалды қолдана отырып енгізіңіз.

Switch #**config t**

Switch (config)#**interface Ethernet 0/2**

Switch (config-if)#**switchport mode access**

Switch (config-if)# **switchport access vlan 2**

Switch (config-if)#**exit**

**Магистральдық порттарды құру**

Қайта қосқыштар арасында барлық VLAN желілерге ақпаратты беру үшін коммутаторды құру керек. Бұл үшін алдымен коммутатордағы Switch 12 портты магистральдық байланысты автоматты түрде анықтау күйіне қосу қажет.

Switch (config)#**interface Ethernet 0/12**

Switch (config-if)#**switchport mode trunk**

Switch (config-if)# **switchport trunk allowed vlan add 2**

Switch (config-if)# **switchport trunk allowed vlan add 3**

Switch (config-if)# **switchport trunk allowed vlan add 4**

Switch (config-if)#**exit**

2.5.4 VLAN желілері арасындағы бағыттауды құру

Магистральдық каналдарды құру үшін магистральді каналдардың сипаттамаларын үйлестіру құралдары қалай жұмыс істейтіні туралы қысқаша қарастырайық. Динамикалық ISL хаттаманы (Dynamic ISL – DISL) немесе динамикалық магистральдық хаттаманы (DTP) қолдана отырып магистральдық каналдардың сипаттамаларын үйлестіру екі өзара байланысқан порттардың магистральдық портқа айналу керектігі туралы келісуге мүмкіндік береді. Мұндай үйлестіру әкімші магистральдық каналдардың екі жағында конфигурацияны құруды орындамас үшін және бір жағында құру жеткілікті болуы үшін пайдаланылады. Каналдың екінші шетінде орналасқан порт қажетті параметрлерді автоматты түрде реттей алады.

Автоматты үйлесімдік құралдары екі порт арасында үйлесімдік фреймдерін беру принципімен жұмыс істейді. Егер порттардың құру параметрлері үйлесімді болса, олардың екеуі де магистралды қолдау күйіне өтеді.

Егер ISL магистральды каналдардың параметрлерін конфигурацияға енгізу қажет болса, онда маршрутизатордың жылдам Fast Ethernet интерфейс конфигурациясына магистральдық канал параметрлерін енгізуге болады, онда қолдау көрсетілетін әр виртуалды ЖЖ үшін жеке интерфейстер құрылады.

2.16 суретке сәйкес желіні құрастырыңыз.

Коммутаторда VLAN-ді құру үшін IOS орнату режиміне өтіу қажет. Құру режиміне өту үшін **enable** енгіз, ал кеңейтілген конфигурация режиміне өту үшін **config t енгізу** қажет.

Switch >**en**

Switch #**config t**

Магистральді байланысты автоматты анықтау режимінде құрылғыны 11 портқа келтір.

Switch (config)# **interface Ethernet 0/11**

Switch (config-if)# **sitchport mode trunk**

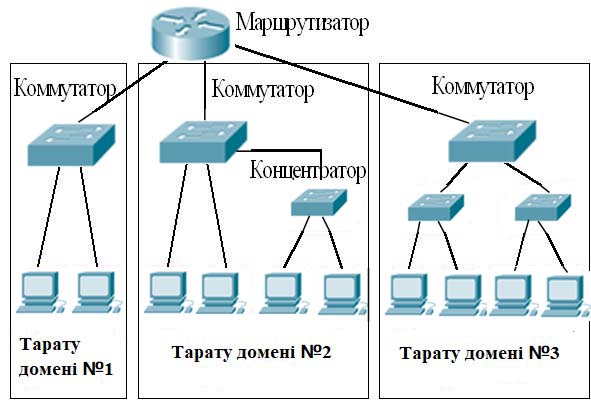
Switch (config-if)# **exit**

Маршрутизаторлардың каскадын VLAN желілер арасында бағыттауға келтіру үшін келесі тапсырмаларды шешу керек:

- маршрутизатор қосылған коммутатор портына ISL магистральдық режимін рұқсат бер.

- маршрутизатордың ішкі бетінде ISL инкапсуляцияға рұқсат бер.

- ішкі интерфейсте IP мекенжайын тағайындаңыз және қажет болған жағдайда басқа логикалық адресті орындаңыз.



2.16 сурет – VLAN арасындағы бағыт.

Ішкі интерфейсті құру үшін interface командасын кеңейтілген күйде немесе интерфейсті конфигурациялау режимінде төменде көрсетілгендей енгізу керек:

Router#**config t**

Router (config)#**interface fa 0/0.1**

Ішкі интерфейс құрғаннан кейін encapsulation командасын сәйкес келетін виртуалды жергілікті желіні ішкі интерфейске қосу үшін төменде көрсетілгендей енгізу керек:

Router (config-subif)#**encapsulation dotdiQ 1**

Келесі қадам стандартты ip address команданың көмегімен интерфейске IP мекенжайын тағайындау қажет.

Router (config-subif)# **ip address 172.16.10.1 255.255.255.0**

Router (config-subif)#exit

Router (config-subif)#int fa 0/0

Router (config-if)#**no shutdown**

Router (config-if)#exit

VLAN 1 желісінде инкапсуляция мен IP адресін құрылғаннан кейін осыған ұқсас әрекеттерді VLAN 2, 3 және 4 желілеріне орындау қажет.



Тексеру жұмысы № 5

**№1 жаттығу Сөйлемді аяқтаңыз:**

Сөйлемнің басын А бағанынан В соңғы бағанынына дейін салыстырыңыз. Параметрді таңдап, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір затты тек бір рет пайдалануға болады.

|  |  |
| --- | --- |
| **А баған** | **В баған** |
| 1. VTP\_\_\_\_\_\_ 2. STP\_\_\_\_\_\_\_\_ 3. VLAN \_\_\_\_\_\_\_\_\_ 4. trunk\_\_\_\_\_\_\_\_\_\_\_\_ 5. BPDU\_\_\_\_\_\_\_\_\_\_ | A. Магистралды желінің виртуалды желімен қосу хаттамасы  Б.Қосымша жүйеде ілмектердің алдын алуға арналған хаттама  B. Виртуалды желі қосылысының магистралды каналы  Г. Нақты жіберуші мен алушы арасындағы виртуалды жеке желі  Д. Хаттамалық деректер модулдерін ауыстыру  E. Ethernet адрестерінде енгізілген виртуалды желі |

**№2 жаттығу Дұрыс жауапты таңдаңыз**

1 VLAN адрестері не үшін қолданылады?

a) Тордың өлшемін қамтамасыз ету

б) Желінің қауіпсіздігін қамтамасыз ету

в) Деректер ағынын бақылау

г) Жоғарыда айтылғандардың барлығы

2. Басқару доменін құру үшін қандай команда қолданылады?

а) Switch (vlan))# domain Cisco

б) Switch (vtp))# domain Cisco

в) Switch (vlan))# vtp domain Cisco   
г) Switch (vtp))# vtp domain Cisco

3. Қандай VTP режимінде коммутатор VLAN желісін құра алады, VTP хабарламаларын елемейтін және VTP доменінің басқа мүшелеріне жергілікті VLAN ақпаратын жібере алмайтын?

а) клиент

б) сервер

в) қию

г) ашық

4. Төмендегілердің қайсысы VLAN үшін дұрыс?

a) Әрбір Cisco коммутацияланған желісінде сізде кемінде екі VLAN болуы керек

б) Барлық VLAN қол жеткізу деңгейінде келтіріледі және тарату деңгейіне дейін кеңейеді

в) VLAN-лар тарату қосқышынан өзекке ауысуы керек

г) VLAN-лар тарату қосқышынан өзекке ауыспауы керек

5. VLAN 1 желісі әдепкі параметрлерін қандай тұжырымдар сипаттайды?

a) VLAN 1 желісі , ол өзінің VLAN желісіне сәйкес келеді.

б) VLAN 1 басқа VLAN-ды конфигурациялау кезінде тек коммутаторда пайда болады.

в) VLAN 1 коммутаторда орналасқан барлық VLAN үшін әдепкі шлюз мекенжайын береді.

г) VLAN 1 пайдаланылмаған порттарға қол жеткізе алатын зиянкестердің қауіпсіздігін бұзу қаупін азайту үшін ажыратылады.

6. Коммутатордағы VTP параметрлерін тексеру үшін қандай команданы қолдану керек?

а) show vtp domain

б) show domain

в) show vtp info

г) set vtp domain output

7. Динамикалық VLAN қалай конфигурацияланған?

а) Статистикалық

б) Әкімшімен

в) DHCP серверінің көмегімен

г) VLAN басқару саясаты серверін (VMPS) пайдалану

8. VTP ашық режимге орнатқан кезде не болады?

a) Ашық режим ескертулер мен хабарламаларды өзінің дерекқорына қоспай жібереді

б) Ашық режим хабарламалар мен ескертулерді жібереді және оларды мәліметтер базасына қосады

в) Ашық режим хабарламалар мен ескертулерді жібермейді

г) Ашқ режим коммутатордың динамикалық қауіпсіздігін қамтамасыз етеді

9. Төмендегі тұжырымдардың қайсысы VTP үшін дұрыс?

a) Бір коммутатордағы VTP нұсқасын өзгерту барлық домендік қосылыстарды өзгертеді

б) Бір коммутатордағы VTP нұсқасын өзгерткен кезде оны барлық қосқыштарын өзгерту керек

в) VTP әдепкі қалпына қосылады және барлық Cisco коммутаторларында Cisco домендік атауы болады

г) Барлық қосқыштар – қалыпты жағдайда VTP клиенттері

10. Коммутатордағы түбірлік портты анықтау үшін не қолданылады?

a) Коммутация каналдарының құны

б) MAC мекен-жайы

в) IP мекенжайы

г) домендік атау

**№3 жаттығу. Мәлімдемені растаңыз немесе жоққа шығарыңыз**

Келесі сөйлемдерден Иә немесе Жоқ сөздерін таңдаңыз.

1. Пакетті бір VLAN желісінен екіншісіне беру үшін коммутатор қажет. Иә Жоқ

2. Көпірлер – VLAN желі байланыстарының негізгі компоненттерінің бірі. Иә Жоқ

3. VLAN жүктемені қайта бөлуге көмектеседі. Иә Жоқ

4. VTP хаттамасының екі нұсқасы, 1 және 2-нұсқа, бір басқарушылық доменде жұмыс істей алады, бұл екі нұсқа үйлесімді және бір доменде жұмыс істей алады. Иә Жоқ

5. Коммутаторларға негізделген желіде маршруттық процессорлар VLAN желі арасындағы байланыс үшін қолданылады. Иә Жоқ

6. Магистральдық канал әр канал үшін үлкен өткізу қабілетін қамтамасыз етеді. Иә Жоқ

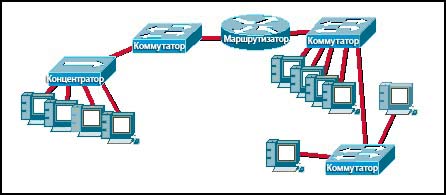
7. Барлық коммутациялық порттарда магистральдық каналдар қалыпты түрде қосылады. Иә Жоқ

8. VTP протоколы виртуалды ЖЖ-де бірнеше тарату домендерін ұсынады. Иә Жо**қ**

5. VTP протоколы VLAN желілерін автоматты түрде қосуды және конфигурациялауды қамтамасыз етеді. Иә Жоқ

6. Магистральдық арналарда VLAN қажетсіз қолмен алып тастау керек. Иә Жоқ

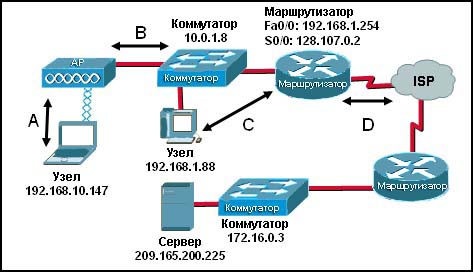
**№4 Қолданбалы тапсырмалар**



1. Суретке қараңыз. Егер барлық қосқыштардың әдепкі конфигурациясы болса, желі неше тарату домендерін қамтиды?

2.

Суретке қараңыз. Суреттің астындағы мәліметтерге сүйене отырып, деректер қайда жіберілетінін анықтаңыз.



IP қорек көзінің адресі: 192.168.1.88

IP тағайындау адресі: 209.165.200.225

MAC қорек көзінің адресі: 00-11-12-7a-41-10

MAC тағайындау адресі: 00-0d-cc-f4-ad-2c

Дерек көзі: 1464

Тағайындалу порты: 23

## 2.6. Ағаштарды байланыстыратын протокол және кіру тізімдері

Мұнда 2-ші деңгейлі коммутациясының үш негізгі функциясы талданады: адресті сүзу, мәліметтерді қайта жіберу немесе сүзу туралы шешім қабылдау және ілмектердің алдын алу; ілмектердің пайда болу мәселесі және 2-ші деңгейлі желіде олардың алдын-алу үшін ағашты байланыстыратын протоколдың әрекеті қарастырылады.

Ағашты байланыстыратын протокол туралы нақты түсінік алу өте маңызды. Бүгінгі таңда артық арналары бар желілер жиі құрылады. Бұл тіпті жеке арнаның істен шығуы жағдайында да желінің қол жетімді болуын қамтамасыз етеді, алайда ағаш ағымының протоколымен қамтамасыз ететін ілмектерді болдырмауға тура келеді. Сонымен қатар, артық арналар жүктемені теңестіреді.

2.6.1-ші деңгейді коммутациялаудың үш қабат функциялары

2 қабатты коммутация үш негізгі функцияларға ие:

* Адресті есте сақтау. 2-ші деңгейдің коммутаторлары мен көпірлері интерфейсте алынған әр кадрдың бастапқы аппараттық адресін сақтайды және оны MAC дерекқорына енгізеді.
* Жіберу және сүзу анықтамасы. Фрейм интерфейстен алынғанда коммутатор аппараттық құралдың соңғы адресін оқиды және MAC дерекқорынан тағайындалған интерфейсті табады.
* Ілмектердің алдын-алу. Егер қосқыштар арасында бірнеше қосылым көп болса, онда ілмектер пайда болуы мүмкін. Желі ілмектерін болдырмау үшін және сонымен қатар артықтықты қамтамасыз ету үшін ағашты байланыстыратын протокол қолданылады.

**Адресті есте сақтау**

2 деңгей қосқышы адресті сақтауға жауап береді. Егер тек коммутатор қосылса, MAC сүзу кестесі бос болады. Құрылғы беріліп, кадр интерфейске жеткенде, коммуникатор бастапқы адресті анықтайды және оны MAC сүзгі кестесіне орналастырады. Коммутатор таратқыш қай интерфейсте орналасқанын еске түсіреді. Соңғы құрылғының орналасқан жері оған белгісіз болғандықтан, ол кадрды желі арқылы таратуға мәжбүр болады.

Егер құрылғы фреймге жауап берсе және қайтарса, коммутатор фреймнен жаңа бастапқы адресті оқиды, алынған MAC адресін дерекқорға орналастырады және оны фрейм алған интерфейспен салыстырады. Коммутатордың сүзгі кестесінде екі MAC адресі болғандықтан, құрылғылар нүктеден бастап нүктеге дейін тікелей байланыс жасай алады және фреймдер олардың арасына тікелей жіберіледі. Сондықтан 2-ші деңгей коммутаторлары концентраторға қарағанда жақсы: концентратор желісінде барлық фреймдер әр уақытта барлық порттарға жіберіледі.

Егер екі құрылғы коммутатормен белгілі бір уақыт аралығында байланыс орнатпаса, коммутатор оны мүмкіндігінше ағымдағы күйінде сақтап, дерекқордағы жазбаларды жояды.

**Бағыттау және сүзгілеу анықтамасы**

2-ші деңгей қосқышы алынған фреймдерді қайта жіберу және сүзу үшін MAC адресіннің сүзу кестесін пайдаланады. Фрейм коммутатордың интерфейсіне келгенде, соңғы аппараттық адрес қайта жіберу деректерінің базасымен және МАС адрестерінің сүзгісімен салыстырылады. Егер аппараттық құралдың соңғы адресі белгілі болса және кестеде болса, фрейм тек қажетті интерфейске жіберіледі. Коммутатор фреймді тек тағайындалған интерфейске жібереді. Бұл желінің басқа бөліктерінде өткізу қабілеттілігін үнемдейді. Бұл процесс кадрларды сүзу деп аталады.

Егер MAC кестесінде аппараттық құралдың соңғы адресі болмаса, фрейм алынған белсендіден басқа барлық белсенді интерфейстерге жіберіледі. Құрылғы таратылымға жауап берген кезде MAC дерекқоры құрылғының (интерфейс) орналасқан жері туралы деректерін жаңартады.

**Ілгектің алдын-алу**

Сонымен, 2-ші деңгей қосқышы ілмектердің алдын алуға жауапты. Коммутаторлар арасындағы артық арналарды пайдалану өте пайдалы, өйткені олар желінің істен шығуына жол бермейді. Бірақ артық арналар өте пайдалы болғанымен, олар ақауды шешуден гөрі көбірек ақауларды тудырады. Келесі бөлімдерде олардың ең маңыздыларын қарастырамыз:

* Кеңінен таратылатын дауылдар
* Фреймдердің бірнеше көшірмелері
* Көптеген ілмектер

**Кеңінен таратылатын дауылдар**

Ілгектің алдын-алу құралдары болмаған жағдайда, қосқыштар бүкіл желі бойынша шексіз таратылады. Мұны кеңінен таратылатын дауылдар деп атайды.

**Фреймдердің бірнеше көшірмелері**

Тағы бір ақау - құрылғы фрейм арқылы бір уақытта желінің бірнеше аймақтарына келетін бірнеше көшірмелерін алады. Бұл жағдайда MAC адресінің сүзу кестесі құрылғының орналасқан жерін анықтай алмайды, өйткені коммутатор бірнеше арналардан фрейм алады. Коммутатор фреймді мүлдем жібере алмауы мүмкін, өйткені ол MAC адрестер сүзгі кестесіндегі бастапқы аппараттық құралдардың адресін үнемі жаңартып отырады.Оны MAC кестесінің бұзылуы деп атайды.

**Бірнеше ілмектер**

Ең қиын мәселелердің бірі – біріктірілген желіде пайда болатын көптеген ілмектер. Басқа ілмектер ішінде ілмектердің пайда болуы мүмкін. Егер осының оңында хабар тарату дауылы болса, желі фреймдерді ауыстыра алмайды.

Осы үш мәселені шешу үшін теректі байланыстыратын хаттама өңделіп (Spanning Tree Protocol STP) жасалған.

Ағаштың байланыс механизмі. Әдетте маршрутизатор болып табылатын 3-ші деңгей құрылғыларында маршруттау хаттамалары желіде маршруттау ілмектерінің жоқтығына жауап береді. Бұл үшін 2 деңгейдің коммутацияланған желілерінде не қолданылады? Мұнда бұл функция кеңейтілген ағаш протоколымен орындалады.

Ағашты байланыстыратын протоколының 2-ші деңгейіндегі (көпірлер немесе қосқыштар арасында) желілік ілмектердің алдын алу мүмкіндігі өте маңызды. Ол барлық арналарды анықтап, артық арналарын жауып, ілмектердің пайда болуын болдырмау үшін желіні үнемі қадағалап отырады.

Ағашы байланыстыру протоколы желідегі бақылау пунктін таңдайтын және оған артық жолдарды есептейтін ағаштың алгоритмін жүзеге асырады. Желідегі барлық арналар табылған кезде, тармақталған алгоритм фреймдерді жіберудің бір жолын таңдайды және желінің ілмектері пайда болмас үшін қалған артық арналарды жабады. Мұны істеу үшін желінің топологиясын анықтайтын тамырлы көпірді таңдалады.

Желіде тек бір тамырлы көпір бола алады. Түбірлік көпір порттары тағайындалған порттар деп аталады және экспедитор деп аталатын күйде жұмыс істейді. Бағытталған порттар трафикті жібереді және алады. Егер желіде басқа қосқыштар болса, оларды тамырлы емес көпірлер деп атайды. Түбірлік көпірге баратын жолдың ең аз құны бар порт түбірлік порт деп аталады және трафикті жіберуге, қабылдауға жауап береді. Құны арнаның өткізу қабілеттілігімен анықталады. Көпір жолындағы құны төменгі порттар тағайындалған порттар деп аталады. Басқа порт немесе басқа көпір порттары тағайындалмаған порт болып саналады және трафикті өткізбейді. Бұл режим блокталған деп аталады.

**Түбірлік көпірді таңдау**

Ағашты байланыстыратын протоколды жүзеге асыратын қосқыштар немесе көпірлер көпір протоколының деректер блогы (Bridge Protocol Data Units, BPDU) арқылы байланысады. BPDU құрылғылары конфигурациялық хабарламаларды мультикасттық кадрларға жіберу және әр құрылғының көпір кодын басқа құрылғыларға беру үшін қолданылады.

Көпір коды желінің түбірлік көпірін және түбірлік портты анықтау үшін қолданылады. Ол 8 байттан тұрады және басым ақпарат пен құрылғының MAC адресін қамтиды. Әдетте, ортаңғы бағдарламалық қамтамасыздандыру сілтемесінің IEEE нұсқасын қолданатын барлық құрылғылардағы басымдық 32768 болып табылады.

Түбірлік көпірді анықтау үшін көпірдің басымдығы мен MAC адресін біріктіру керек. Егер екі қосқыш бірдей басым мәнге ие болса, онда минималды мәнді анықтау үшін MAC адресі қолданылады.

Мысалы, егер A және B қосқыштары бірдей 32768 басымдыққа ие болса, онда MAC адресі түбірлік көпірді анықтау үшін қолданылады. Егер А қосқышының MAC адресі 0000.0c00.1111.1 111 болса, ал В қосқышының MAC адресі 0000.0c00.2222.2222 болып, А қосқышы түбірлік көпірге айналады.

BPDU модульдері фреймнің ұзындығы бойынша ақауға сәйкес таратудың кешігуіне, коммутациялық өңдеуге, өткізу қабілетіне және жүктеуге байланысты мәселелерге сезімтал болып келеді. Бұл желінің тұрақсыздығына әкелуі мүмкін, өйткені егер BPDU модульдері қашықтағы желі нүктесімен уақытында қабылданбаса, онда желіде уақытша ілмектер пайда болуы мүмкін. Таралу протоколы порттардан желілік топологияның дұрыс деректерін алу үшін таймерді қолданады.

**Белгіленген портты таңдау**

Түбірлік көпір таңдалғаннан кейін барлық қосқыштар онымен «достасуы» керек. Әр қосқыш барлық белсенді порттардағы BPDU модульдерді қабылдайды және бірнеше модуль алған кезде түбірлік көпірге артық канал бар екенін білдіреді. Коммутатор қай порттың тамырға айналатынын және қайсысын оқшауланған күйге қою керектігін анықтауы керек.

Түбірлік көпірмен байланыс орнатуға қызмет ететін портты анықтау үшін жолдың құны анықталады. Ағаштың байланыс құны – бұл каналдарды өткізу қабілеттілігіне негізделген жолдың жалпы құны.

Түбірлік көпірге дейінгі барлық каналдардың құны анықталған кезде, коммутатор портты ең төменгі құны бойынша орнатады. Бұл порт бағыттау режиміне өтеді, ал қалғаны блокталған режимге өтеді. Егер бірдей құны бар бірнеше жол болса, порт коды ең төмен мәні бағыттау режиміне ауыстырылады.

**Ағаш байланыс порттарының жағдайы**

Ағаш байланыс протоколын қолданатын көпір немесе коммутатор порттарының төрт күйі болады:

* Оқшауланған Порт фреймдерді жібермейді, тек BPDU хабарламаларын қабылдайды. Коммутатор қосылған кезде, барлық порттар әдепкі бойынша оқшауланған күйде болады.
* Порттың қабылдауы фрейм деректемелерін бергенге дейін BPDU модульіндегі хабарламаларды желідегі ілмектердің алдын алу үшін қабылдайды.
* Портың есте сақтауы MAC адресін есте сақтайды және фреймдерді жібермей сүзгі кестесін құрастырады.
* Көпірлі портты қайта бағыттау деректерді жібереді және қабылдай алады. Артық каналдар болмағанда немесе портта көпір түбіріне қолайлы жол болғандағы жағдайлардан басқасында Порт тасымалдау күйінде болмайды.

Әкімші портты өшіре алады; егер портта ақау болса, онда оны коммутатор өшіреді.

Әдетте коммутациялық порттар блотау немесе қайта жіберілген күйде болады. Қайта жіберу порты – бұл түбірлік көпірге ең аз шығын келтіретін порт. Егер желінің топологиясы каналдың істен шығуына немесе жаңа қосқыштың қосылуына байланысты өзгерсе, коммутатор порттары қабылдау немесе жады режиміне ауысады.

Оқшауанған порттар желілік ілмектерді болдырмау үшін қолданылады. Коммутатор түбірлік көпірге қолайлы жолды анықтаған кезде, қалған барлық порттар оқшауланған күйге өтеді. Оқшауланған порттар сонымен қатар BPDU модульдерін алады.

**Конвергенция**

Көпірлер мен қосқыштар бағыттау немесе оқшаулау күйіне өткен кезде конвергенция орын алады. Бұл жағдайда ақпарат жіберілмейді. Конвергенция құрылғылар бойынша дерекқордың сәйкестендірілуін қамтамасыз етеді.

Конвергенция мәселесі барлық құрылғыларды жаңартуға жұмсалған уақыт мәселесі болып табылады. Деректер жіберілмес бұрын барлық құрылғылар жаңартылуы керек. Әдетте оқшаулау күйінен қайта жіберу күйге ауысу 50 секундты алады. Стандартты ағаш байланысының таймерлерін өзгерту қажет емес, бірақ қажет болған жағдайда оларды қайта конфигурациялауға болады. Порттың қабылдау күйінен сақтау күйіне немесе жады күйінен қайта жіберу күйге өтуіне кететін уақыт қайта жіберудің кідірісі деп аталады.

2.6.2 Виртуалды логативті желілерде ағаш байланысын пайдалану

Шамадан тыс – бұл желі бұзылған кезде жедел қолдау мүмкіндігі, әйтпесе желіні немесе оның кез келген қызметтерін зақымдауы мүмкін. Шамадан тыс желіні құру - шамадан тыс энергиямен жабдықталатын желі, жабдық, каналдар және басқа интегралды компоненттермен орындалады, бұл жағдайда желілік ілмектер пайда болуы мүмкін. 2-ші деңгейдегі көпірлердің көмегімен қолднушылардың ашық ұйымымен байланысқан бұл ақаулардан құтылу үшін ағашты байланыстыратын хаттама жасалды.

Әрбір виртуалды ЛЖ арналған ағаш байланысы (Рег-VLAN Spanning Tree, PVST) – бұл ағашты байланыстыратын Cisco протоколының өзара құрылымы. Ол коммутациялық каналдар арасындағы бағыттауды қолданады және әрбір виртуалды ЛЖ үшін ағаш байланысының тармақталған бөлігін орындайды.

Әрбір виртуалды ЛЖ үшін ағаш байланысы Cisco коммутаторы үшін ағаш байланысының негізгі құрылуы. Әрбір виртуалды желіге жеке ағаш байланысының тармақталған данасы әсер етеді. Бұл қарапайым конвергенцияны қамтамасыз ететін кеңейтілген ағаш протоколының кішірек нұсқасы.

Ағаш байланысының протоколы үлкен коммутацияланған желілерде жақсы таралмайды. Үлкен коммутацияланған желілерде BPDU қабылдаудың кідірістері орын алуы мүмкін, бұл өз кезегінде кеңейтілген протоколдар базасының тұрақтылығын бұзуы мүмкін. Үлкен коммутацияланған желілердегі кідірістер конвергенция мәселелерін тудыруы мүмкін, яғни желі фреймдерді жібермейді.

BPDU модулінің кідірісін және конвергенция мәселелерін шешу үшін Cisco компаниясы әр виртуалды ЛЖ үшін жеке ағаш байланысын құрды. Бұл коммутаторлардың жұмысын жеңілдететін кеңейтілген протоколды жүзеге асыруды айтарлықтай азайтады. Сонымен қатар, осы іске асырудың арқасында әрбір виртуалды ЛЖ-сі түбірлік көпір, порт құны, жол құны және басымдылық үшін ерекше ағаш байланысының протоколының топологиясынан тұрады. Әрбір виртуалды ЛЖ үшін кеңейтілген ағаш байланысын пайдалану желілердің алдын алуды қамтамасыз етеді, бірақ тек әрбір виртуалды желіде.

Әр виртуалды ЛЖ + үшін кеңейтілген ағаш байланыс протоколының келесідей мүмкіндіктері бар:

* Порт-транкингтегі сәйкессіздіктер немесе коммутаторлар арасындағы виртуалды ЛЖ тепетеңдігі
* Белгісіз конфигурациялардың ақауын жоюға мүмкіндіктер береді
* 802.1q виртуалды ЛЖ ортасында әрбір виртуалды ЛЖ үшін BPDU моделінің ағаш байланыс протоколын көп адресті жіберім деректері ретінде өңдейді
* IEEE 802.1q комитеттің толық ағаш байланысының протоколдарының және әрбір виртуалды ЛЖ үшін Cisco компаниясының ағаш байланысының үйлесімділігін қамтамасыз етеді.
* 802.lq үйлесімді қосқыштармен және 802.lq таралымы арқылы толық ағаш байланыс протокол қолданысын өзара байланыстырады; толық ағаш байланыстың BPDU модулі IEEE стандартының көпір тобының MAC адресі бойынша беріледі немесе қабылданады
* Ілмектерді қайта жібеуді болдырмас үшін сәйкес келмейтін BPDU модулдері қабылдайтын порттарды бітеп тастайды
* Барлық ақаулар туралы ақпаратты пайдаланушыларға syslog хабарламалары арқылы хабарлайды

**Ағаш байланыс протоколын масштабтау**

Ағаш байланысының протоколы 2-ші деңгейлі коммутацияланған желілерінде ілмектердің алдын алады және орнатуды қажет етпейді. Неғұрлым сенімді желілік ортаны құру үшін кейде кейбір параметрлер мен стандартты таймерлерді өзгерту пайдалы.

Оңтайлы желілік топологияны ұйымдастыру үшін тамырлы көпірдің дұрыс орналасуы ерекше маңызды. Егер түбірлік көпір автоматты түрде таңдалса, фреймдердің берілу жолы ең нәтижелі болмауы мүмкін. Бұл жағдайда әкімші тиімдірек маршрут жасай отырып, тамырдың орнын өзгерте алады. Бірақ оның әрекеті керісінше нәтижеге әкелуі мүмкін, егер өзгерістер енгізбес бұрын желіні дұрыс жоспарлауға жеткілікті көңіл бөлінген болса.

Түбірдің орнын өзгертуге мына қызметтерді орындау қажет:

* Түбірлік құрылғыны анықтау
* Бұл құрылғыны қалпына келтіру
* -Порт басымдықтарын орнату
* -Виртуалды ЛЖ порттарына басымдық беру
* -Ағаш байланыс протоколының таймерін өзгерту

**Түбірлі құрылғыны анықтау**

Түбірлік құрылғыны анықтау желідегі кеңейтілген протоколды конфигурациялаудың маңызды бөлігі болып табылады. Егер түбірлік құрылғы дұрыс орналастырылмаған болса, онда желіні масштабтау қиын, сондықтан масштабты коммутацияланатын 2 деңгейлі біріктірілген желіні құру қажет.

Егер түбір қосқышын желінің ортасына жақын орналастырса, ең жақсы және детерминантты жолдарды анықтау оңайырақ болады. Сонымен қатар түбірлік көпірді және екінші және резервтік көпірлерді таңдай аласыз. Екінші көпірлер түбірлік көпір істен шыққан кезде желінің тұрақтылығы үшін үлкен маңызға ие.

Түбірлік көпір желінің ортасында болуы керек болғандықтан, олар әдетте қол жеткізу деңгейінің қосқышын емес, тарату деңгейінің қосқышын таңдайды.

Түбірлік көпір таңдалған және қалпқа келтірілген болса, барлық қосылған қосқыштар түбірлік көпірге оңтайлы жолды жолды анықтауы керек. Ағаш байланыс протоколы түбірлік көпірге баратын ең жақсы жолды анықтауда бірнеше шығын түрлерін қолданады:

* Порттың құны
* жол жүру құны
* Басымдық жолы

BPDU деректер модулі коммутациялық порттан жіберілген кезде портқа порттың құны тағайындалады. Содан кейін порттардың жалпы құны маршруттың құнын есептейді. Ағаш байланыс протоколы алдымен бағыттау және блоктау порттарын анықтау үшін жолдың құнын қарастырады. Егер түбірлік көпірде жолдарының құны бірдей екі немесе одан көп каналдар болса, түбір портын анықтау үшін порт коды қолданылады. Ең аз саны бар порт синалдарды тасымалдаушыға айналады. Коммутатордағы порт нөмірін порттың басымдылығын өзгерту арқылы өзгертуге болады, бірақ оны орындауға кеңес берілмейді.

Мысал. STP конфигурациясы. Rapid-PVST+ және Port Fast тепе теңдігін қолдау үшін R мәніне конфигурация жасау қажет.

R>**enable**

R#**config term**

R(config)#**spanning-tree mode rapid-pvst**

R(config)#**spanning-tree portfast default**

**Енгізуді басқару тізімдері**

Енгізуді басқару тізімі Access Control List немесе ACL – белгілі бір объектіге кім немесе не қол жеткізе алатындығын және осы объектіге қандай амалдарды жасауға рұқсат етілген немесе тыйым салынғанын анықтайтын енгізуді басқару тізімі.

ACL тізімі құрылғылары ғаламдық конфигурация режимінде құрады. Енгізуді басқару тізімдерінің түрлері өте көп: стандартты, жетілдірілген, IPX протоколдар тізімі, AppleTalk тізімдері және басқалары. Маршрутизаторда ACL құру кезінде әр тізімге ерекше нөмір берілуі керек. Мұндай сан тізімнің түрін анықтайды және белгілі бір тізімге бөлінетін сандар шеңберінен шықпауы керек. Енгізуді басқару тізімдерінің жиі қолданылатын протокол нөмірлері: стандартты IP тізімдері 1-99; кеңейтілген IP тізімдері 100-199; AppleTalk 600-699 протоколы стандартты IPX тізімдері 800-899; Кеңейтілген IPX 900-999 тізімдері IPX SAP (Сервистік жарнама хаттамасы - 1000-1099 хабарлама хаттамасы).

Әкімші команда жолының режимін қажетті жағдайға ауыстырғаннан кейін және тізім нөмірін таңдау керек болатын шешім қабылданғаннан кейін, ол кіру тізіміндегі access-list кілт сөзден дұрыс параметрлерге дейін ACL тізім директиваларын тізбектей енгізеді. Енгізуді басқару тізімін құру - бұл тек қызметтің жартысы ғана болып келеді. Процестің екінші және маңызды бөлігі - тізімнің интерфейспен байланыстырылуы.

ACL тізімі бір немесе бірнеше интерфейстермен байланысып, деректердің кіріс және шығыс ағынын сүзгіден өткізе алады. Тізімді интерфейске (файлдарға) байлау access-group командасымен жүзеге асырылады. Аccess-group командасы интерфейсті конфигурациялау режиміне енгізіледі. Енгізуді басқару тізімі кіріс немесе шығыс бағыттағы интерфейспен байланысты: кіріс немесе шығыс трафикке сәйкес. ACL тізімі қандай бағытта әрекет ету керектігін анықтау үшін «маршрутизатордың ішінен интерфейсті қарау керек», яғни сіз құрылғының ішінде екеніңізді елестетіп көріңіз. Бұл тәсіл көптеген жағдайларда трафик ағындарын түсінуге көмектеседі, бұл жағдайда қандай деректер ағынының қай бағытқа жіберілетінін түсіну қажет. «Маршрутизатор ішіндегі бақылаушының» көзқарасы бойынша сыртқы әлемнен құрылғыға интерфейс арқылы кіретін трафик қатынасты басқару тізімімен сүзуге болады; сәйкесінше, құрылғыдан интерфейс арқылы сыртқы желіге жіберілетін мәліметтер ағынын шығыс тізімімен сүзуге болады. Нөмірленген ACL тізімі құрылғаннан кейін оны қажетті интерфейске байлау керек. Нөмірленген енгізуді басқару тізіміндегі директивалардың ретін өзгерту үшін no access-list командасының көмегімен барлық тізімді жойып, оны қайта құру керек.

Әрбір хаттаманың өзіндік талаптары мен ережелері болғанына қарамастан, оларды орындау трафикті сүзгілеу үшін қажет, тұтастай алғанда енгізуді басқару тізімдерін жасау төменде келтірілген екі негізгі әрекетті ғана талап етеді.

1 қадам. ACL тізімін құру.

2 кезең. Белгілі бір интерфейске кіру тізімін қолданыңыз.

Мысал. Ethernet 0 интерфейсімен байланысатын 1 және 2 сандары бар енгізуді басқарудың стандартты тізімдерін құрыңыз.

R(config)# **access-list 1 permit 5.6.0.0 0.0.255.255**

R(config)# **access-list 1 deny 7.9.0.0 0.0.255.255**

R(config)# **access-list 2 permit 1.2.3.4**

R(config)# **access-list 2 deny 1.2.0.0 0.0.255.255**

R(config)# **interface ethernet 0**

R(config-if)# **ip address 1.1.1.1 255.0.0.0**

R(config-if)# **ip access-group 1 in**

R(config-if)# **ip access-group 2 out**

***host үлгісін қолдану***

Сіз *host* кілт сөзін пайдалана аласыз, ол Cisco IOS амалдық жүйеде тек бір толық адрестің тексерілуі керек екенін айтады. Төмендегі мысалда адрестің алдында 172.30.16.29 0.0.0.0 ұзын жолды енгізудің орнына *host* құпия сөзін жазуға болатындығы көрсетілген.

Мысалы, жолдың орнына

R(config)# **access-list 1 permit 172.30.16.29 0.0.0.0**

Мынаны жазса болады

R(config)# **access-list 1 permit host 172.30.16.29**

***Енгізуді басқару тізімдерін тексеріңіз***

Show ip interface интерфейстер туралы ақпаратты көрсетеді және оларға енгізудіі басқару тізімдері орнатылғанын немесе орнатылмағанын көрсетеді.

Show access-lists командасы барлық енгізуді басқару тізімдерінің мазмұнын көрсетеді. Егер енгізуі басқару тізімінің атауын немесе нөмірін параметр ретінде көрсетілген екі құпия сөзден кейін енгізсеңіз, нақты ACL мазмұны көрсетіледі.

***Стандартты ACL***

Енгізуді басқарудың стандартты тізімдері түйінге, желі адресіне негізделген барлық протоколдар жиынтығына тыйым салу немесе рұқсат ету қажет болған кезде қолданылады.

Мысалы, E0 немесе Fa0/0 интерфейсіне келетін пакеттер үшін жіберушінің адресі мен хаттамалары тексеріледі. Содан кейін олар енгізуді басқару тізімінің директиваларымен салыстырылады. Егер сәйкестік табылса, көрсетілген әрекет орындалады (рұқсат немесе тыйым әрекеті). Егер пакеттер рұқсат ережесіне (permit) сәйкес болса, олар маршрутизатор арқылы енгізуді басқару тізіміне логикалық түрде қосылған шығыс интерфейске бағытталады. Егер пакеттер жоққа шығару ережесіне (deny) сәйкес келсе, олар алынып тасталады.

ACL стандартты тізім директивасының толық синтаксисі:

R(config)# **access-list** **access-list-number{permit|deny|remark} source[source-wildcard] [log]**

Аталған құпия сөз тізімге түсініктеме қосу үшін пайдаланылады, ол кейінірек енгізуді басқару тізімін анықтауға көмектеседі. Мұндай түсініктеме сызығының ұзындығы жүз таңбадан аспауы керек.

Мысалы, бір қарағанда, мұндай жазба не үшін қажет деп айту қиын:

R(config)#**access-list 1 permit 171.69.2.88**

Егер енгізуді басқару тізімінде түсініктеме болса, онда нақты директиваға не жататынын анықтау оңайырақ болады.

R(config)#**access-list 1 remark Permit only Howard workstation though**

ACL 1 171.69.2.88

R(config)#**access-list 1 permit 171.69.2.88**

(Пікір: «ACL 1 тізімі арқылы Howard Workstation 171.69.2.88 тек Говард жұмыс станциясын енгізуге рұқсат беріңіз»).

Енгізуді басқарудың стандартты тізімін алып тастау үшін осы команданың құпия сөзімен үлгісі қолданылады:

Router(config)# **бойынша access-list number**

Ғаламдық конфигурация режиміндегі қатынау тізіміне кіру тізімі access-list командасының стандартты нұсқасы 1-ден 99-ға дейінгі аралықтағы енгізуді басқарудың стандартты тізімін орнатады. Келесі мысалда 4 директивасы бар стандартты кіру тізімі көрсетілген; барлық директивалар 2 нөмірмен кіру тізіміне енгізілген. Есте сақтау керек, егер пакеттер қол жеткізу тізімінің кез-келген ережелеріне сәйкес келмесе (яғни жазбалар немесе директивалар), олар ACL соңында барлық ережелер берілуіне тыйым салатын жасырын ережеге сәйкес келеді, бұл барлық пакеттердің (бұл ереже конфигурацияда көрсетілмейді) берілуіне тыйым салады.

Мысал. Қол жеткізуді басқарудың стандартты тізімінің директивалары

R(config)# **access-list 2 deny 172.16.1.1**

R(config)# **access-list 2 permit 192.168.1.0 0.0.0.255**

R(config)# **access-list 2 deny 172.16.0.0 0.0.255.255**

R(config)# **access-list 2 permit 10.0.0.0 0.255.255.255**

Енгізуді басқару тізімінің бірінші жолында инверттелген маска қолданылмағанын көрсетеді (ол жерде жоқ екенін ескеріңіз). Осындай жағдайда, маска көрсетілмеген кезде стандартты мәні 0.0.0.0 болатын инверттелген маска қолданылады. Бұл ACL тізім директивасы бір IP адресіне кіруге тыйым салады - 172.16.1.1.

Екінші жол 192.168.1.0, яғни, адрестерден желіге енуге мүмкіндік береді, адресі 192.168.1 комбинациясынан басталатын кез келген адреске сійкес келеді.

Үшінші жолдағы нұсқаулық 172.16.0.0 желісіге кіруге тыйым салады, ал төртіншісі жолдағы директива пакеттері 10-нан басталатын кез келген адреске жіберуге мүмкіндік береді, яғни желіден 10.0.0.0.

IP access-group қатынасу тобының командасы жасалған қатынасты басқару тізімін интерфейспен байланыстыру үшін қолданылады. Әр порт, хаттама және бағыт үшін тек бір тізімге рұқсат етілгенін ескеру қажет. Команда келесі форматта болады:

Router (config) # **ip access-group тізім номері {in | out}**

***ACLкеңейтілген тізімі***

Кеңейтілген тізімдер пакеттің бастапқы және тағайындалған адрес тізімінде көрсетілген адрестермен салыстыру арқылы трафикті басқарады. Бұл трафикті келесі критерийлер бойынша сүзгілеу қажет:

- хаттама;

- порт нөмірі;

- DSCP мәні;

- басымдылық;

- SYN битінің күйі;

Кеңейтілген ACL синтаксисі.

R(config)# access-list number [dynamic dynamic-name [timeout minutes]] {deny|permit} {protocol|protocol-keyword} {source source-wildcard|any} [source-port] {destination destination-wildcard|any} [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name] [fragments]

«Log» құпия сөзі осы өлшемге сәйкес келетін пакеттің консольге және жүйелік журнал файлына жазылуына себеп болады. Егер «tcp» немесе «udp» протокол ретінде көрсетілсе, онда бастапқы және тағайындалған-қойылмалы таңба сипаттамаларында «eq», «lt», «gt», «range» құпия сөздерімен осы протоколдардың порт нөмірлері болуы мүмкін. «tcp» протоколы үшін тек белгіленген tcp-сессиярын бөлектеу үшін белгіленген «established» сөзді қолдануға болады.

«Hostsource» құпия сөзі жазбаға балама болып табылады: «source 0.0.0.0» Мысал.

Бірінші шарт 1023-ден асатын порттарға кез келген TCP қосылыстарына мүмкіндік береді. Екінші шарт 128.88.1.2 аресі бойынша кіріс SMTP қосылыстарына мүмкіндік береді. Келесі өлшемдер ICMP хабарламаларын өткізуге мүмкіндік береді. Ethernet0-тен келетін барлық басқа пакеттер алынып тасталады.

R(config)#**access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 gt 1023**

R(config)#**access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25**

R(config)# **access-list 102 permit icmp 0.0.0.0 255.255.255.255 128.88.0.0 255.255.255.255**

R(config)# **interface ethernet 0**

R(config)# **ip access-group 102 in**

***Мысал.*** 192.168.1.2 түйініне FTP қатынасын рұқсат етіңіз және 192.168.1.3 түйінін қабылдамаңыз.

R(config)#**ip access-list extended 101**

R(config-ext-nacl)#**permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21**

R(config-ext-nacl)#**permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20**

R(config-ext-nacl)#**deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 21**

R(config-ext-nacl)#**deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20**

Бұл жерде біз 21 және 20 порттар үшін рұқсат етілген және тыйым салатын 2 ережені көреміз. Бұл FTP қызметі, командалар мен деректерді беру қызметі.

Енді біз тізімді 192.168.1.0/24 желі жағынан кіріске енгіземіз

R(config)#**int fa 0/1**

R(config-if)#**ip access-group 101 in**

***Мысал.*** Тек 80 және 443 порттарындағы WWW серверіне 10.0.0.0/24 желі трафигін және басқа желілерге толық қатынауға рұқсат етіңіз.

Бұл тапсырманы орындау үшін кеңейтілген енгізу тізімін құру қажет.

R(config)# **access-list 101 permit tcp 10.0.0.0 0.0.0.255 host 192.168.0.1 eq 80**

R(config)# **access-list 101 permit tcp 10.0.0.0 0.0.0.255 host 192.168.0.1 eq 443**

R(config)# **access-list 101 deny ip 10.0.0.0 0.0.0.255 host 192.168.0.1**

R(config)# **access-list 101 permit ip 10.0.0.0 0.0.0.255 any**

R(config)#**interface fastEthernet 0/0**

R(config-if)#**ip access-group 101 in**

***Аталған ACL***

Кіру тізімдерін нөмірлеуге ғана емес, сонымен қатар атауға да болады. Мүмкін бұл әдіс сізге ыңғайлы болып көрінуі мүмкін. Бұл командалар ғаламдық конфигурация контекстінде орындалады және синтаксисі келесі түрде болады:

R(config)#**ip access-list extended INT\_IN**

Router(config-ext-nacl)#**permit icmp 192.168.0.0 0.0.0.255 host 10.0.0.100 echo ( желіде 192.168.0.0/24 желі пингилерін кеңейту )**

R(config)#**int fa0/0**

R(config-if)#**ip access-group INT\_IN in**

R(config)#**ip access-list extended INT\_OUT**

R(config-ext-nacl)#**deny icmp host 10.0.0.100 192.168.0.0 0.0.0.255 echo**

R(config-ext-nacl)#**exit**

R(config)#**int fa0/1**

R(config-if)#**ip access-group INT\_OUT in**

Енгізу тізімі оны енгізгеннен кейін бірден жұмыс жасай бастайды. Оны қолданудың дұрыстығын тексеру үшін интерфейстің екінші жағында орналасқан хост байланыстың үзіліссіз тестілеуін жүргізу үшін ping командасын пайдалану қолайлы. Өзгерістерді «write memory» және «write network» командалардың көмегімен сақтауды ұсынамыз (егер TFTP серверінде конфигурация параметрлерін көшірсеңіз).

Арнайы интерфейстерге қандай қатынасу топтары тағайындалғанын көру үшін show config командасын пайдалануға болады. Соңында ол кіру тізіміндегі барлық жазбаларды көрсетеді. Бұл ақпаратты алудың неғұрлым ыңғайлы тәсілі «show access list» командасын қолдану. Егер кіру тізімінің нөмірін дәлел ретінде орнатсақ, тек сәйкес тізім көрсетіледі. (Мұны кез келген нөмірді жаңа тізімге тағайындаған сайын жасаған дұрыс, бұл нөмір әлі пайдаланылмағанына көз жеткізу керек.) Бұл қарастырып отырған команда енгізу тізіміндегі әр жазба үшін сәйкестіктер туралы статистика береді. Статистикалық есептегіштерді тазарту үшін «clear access-list counters» командасы қолданылады, тізім нөмірі дәлел ретінде де қолданылады.

Жоғарыда айтылғандай, жай кіріп, енгізу тізіміндегі жазбаны өзгерте болмайды, өйткені бұл жазбалар маршрутизаторға алғаш енгізілген ретпен өңделеді. Егер маршрутизаторға жаңа конфигурацияны жүктеу үшін TFTP протоколын қолдансақ, TFTP хостындағы конфигурация файлын өңдеп, содан кейін түзетілген нұсқасын жүктей аласыз. Бұл тәсілдің кемшілігі – жаңа конфигурация файлын жүктеу уақытын маршрутизатор қайта іске қосылған сәттен бастап үйлестіру қажетті.

Тізімдерге өзгертулер енгізудің тағы бір тәсілі – тізімді мәтіндік редакторға көшіру және сол жерде өңдеу. Маршрутизаторға тізімнің жаңа нұсқасын жазбас бұрын, алдымен ескі нұсқадан арылу керек, әйтпесе жаңасы ескісіне қосылады. Cisco фирмасының маршрутизаторындағы конфигурация параметрлері бар жазбаны жою үшін оған «no» сөзін көбірек енгізу арқылы қайтадан енгізу керек. Барлық енгізу тізімін жою үшін «no» сөзін және оның бір жазбасын енгізу жеткілікті. Бұл жағдайда маңызды кемшілік – біраз уақытқа дейін сіз жұмыс тізіміне енбей қалуыңыз мүмкін. Егер сіз қателік жасасаңыз немесе хостқа немесе қызметке кіруге кездейсоқ тыйым салсаңыз, қате не екенін білмейінше тізімді өшіруге тура келеді.

Қатынау тізіміне өзгертулер енгізудің ең жақсы әдісі – бұл мәтіндік редактордағы ескі тізімді редакциялау және оны маршрутизатор интерфейсіне қоспас бұрын оның атын өзгерту болып табылады. Сіздің әрекеттеріңіздің реті келесідей болады:

Пайдаланылған қатынау тізімін «show config» командасын пайдаланып көрсетіңіз және оны мәтіндік редакторға көшіріңіз.

Кіру тізімінің нөмірін өзгертіңіз және тізімді өңдеңіз.

«Конфигурация» режиміне кіріп, маршрутизаторға жаңа тізімді жазыңыз.

Сіз тізімді өзгерткіңіз келетін интерфейсті анықтаңыз, содан кейін «ip access-group xxx in/out» командаларын қолданып жаңа тізімді байланыстырыңыз (ескі тізімді өшірудің қажеті жоқ, себебі бұл жаңа іске қосылған кезде автоматты түрде пайда болады; әр интерфейсте тек бір енгізу тізімі болуы мүмкін).

Егер сіз жаңа тізімге қатысты мәселелерге тап болсаңыз, xxx ip access-group xxx in / out командаларын және оның нөмірін пайдаланып, ескі тізімге өтуіңізге болады.

Адамдар жиі бағыттармен шатасады. Мысалы, маршрутизаторға қосылған желі бар және міндеті – осы желіге трафикті енгізуге тыйым салу. Сонымен, бұл жағдайда кіріс трафикгі out тағы ACL қолдану арқылы сүзіледі, яғни шығу. Бұл қарапайым, сондықтан шатастырмау үшін сіз өзіңізді маршрутизатордың орнында елестетуіңіз керек. Егер трафик желіге кірсе, ол маршрутизатордан шығады және роутердің көзқарасы бойынша мұндай трафик шығатыны түсінікті.

Жалпы алғанда, бір интерфейске бірнеше ACL-ні енгізуге болады, бірақ олардың бағыты немесе протоколы өзгеше болып келеді (AppleTalk ACL IPX ACL бар).

ACL қайда қолданған дұрыс? Сұрақ, шын мәнінде, маңызды емес және тиісті тәжірибесі жоқ студенттер қате жауап береді. Мысалды қарастырыңыз: топологияны ескере отырып, компьютерге ноутбук желісіне кезекпен екі жолмен кіруге тыйым салу керек (алдымен стандартты, содан кейін кеңейтілген ACL қолдану).

Бұл туралы біраз ойланыңыз. Ақыл-ой мен cisco ұсынысы бізді келесі ережеге итермелейді: «Сіз стандартты ACL-ті трафик алушыға мүмкіндігінше жақын орналастыруыңыз керек». Шынында, стандартты ACL көмегімен біз жіберушінің мекен-жайын ғана көре аламыз және біз бұл трафиктің қайда кететінін білмейміз. Сондықтан, егер біз компьютердің IP-мекен-жайына кіруге тыйым салатын тізімді орналастырсақ, онда тек қана ноутбуктің желісіне ғана емес, барлық компьютерлерге, яғни барлық желілерге трафикті тыйым салуға немесе рұқсат етуге болады. Сондықтан мұндай ACL трафик алушыға мүмкіндігінше жақын қою керек.

Егер біз кеңейтілген ACL-ны қолданғымыз келсе, онда біз оны кез-келген жерге қоя аламыз, бірақ оны трафик жіберушіге мүмкіндігінше жақын қою орынды. Осылайша, біздің өмірімізді жеңілдететін кішкентай ереже бар: «стандартты ACL трафик қабылдағышқа мүмкіндігінше жақын, ал кеңейтілген ACL трафик көзіне жақын орналасады». Алдымен осы ереже бойынша орынды таңдаған дұрыс, содан кейін трафик қайдан келетінін және ACL орналастыруды қалай жақсартқаныңыз туралы ойлаңыз.

Есіңізде болсын, барлық ену тізімдерінің соңында deny any командасы болады, яғни егер сіз кіру тізімін параметрлерсіз жасап, оны интерфейске қолдансаңыз, онда барлық трафик оқшауланады. Енгізу тізіміндегі ережелер жоғарыдан төменге, бірінші сәйкестікке дейін тексеріледі, егер желіге арналған кеңейтілген директиваны жазса, онда кейін тізімді тексеру кезінде желідегі түйін рұқсат етілген директиваға өтеді, ал тыйым салушы тексерілмейді.



**Тексеру жұмысы № 6**

**№1 жаттығу. Дұрыс жауапты таңдаңыз**

1. Компания жұмыс станцияларына IPv4 адресін динамикалық түрде тағайындау үшін DHCP серверлерін пайдаланады. Жалдау адресінің ұзақтығы 5 күн болып белгіленген. Қызметкер бір апта болмағаннан кейін кеңсеге оралады. Қызметкер жұмыс станциясын жүктеген кезде, ол IP-адресін алу үшін хабарлама жібереді. Хабарламада қандай 2 деңгейдің және 3 деңгейдің адрестік хабарламасынан тұрады?

а) FF-FF-FF-FF-FF-FF и 255.255.255.255

b) DHCP серверінің MAC адресі және IPv4 адресі

c) DHCP серверінің MAC адресі және 255.255.255.255

d) FF-FF-FF-FF-FF-FF және DHCP серверінің IPv4 адресі

2. Қандай желі құрылғысы inter-VLAN бірнеше ішкі интерфейстердің конфигурациясын қажет етеді?

а) маршрутизатор

б) көп деңгейлі коммутатор

c) VLAN басқару үшін ауыстырғыш

d) VLAN-тегі бағыттауыш қосқыш

3. Көп деңгейлі коммутаторда VLAN бірнеше желісінде трафик қалай бағытталады?

а) Трафик физикалық интерфейстер арқылы жүзеге асырылады.

б) трафик ішкі VLAN интерфейсі арқылы жүзеге асырылады.

в) трафик барлық физикалық интерфейстерге таратылады.

г) трафик ішкі аралықта бағдарланған.

4. Екі коммутатор арасындағы трафиктің жоғары деңгейіне байланысты интерфейстің бітелуін шешудің ең тиімді әдісі қандай?

а) қозғалыс жылдамдығын арттыру

б) таратылатын домендерді азайту үшін жергілікті локальды желілерді көбірек қосу

c) порттарды EtherChannel көмегімен біріктіру

г) қосқыштардың арасына маршрутизатор салу

5. EtherChannel-дің орындалуы қандай мәлімдеме береді?

a) EtherChannel тек 2 деңгейінде жұмыс істейді.

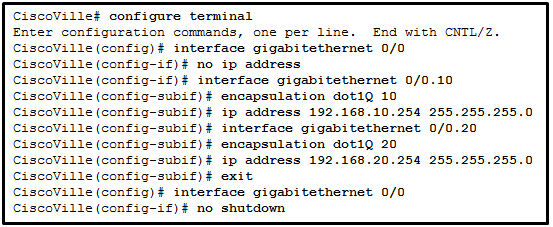
б) PAgP-ны EtherChannel-мен бірге қолдануға болмайды.

в) магистральдық порт EtherChannel қабатының бөлігі болуы мүмкін.

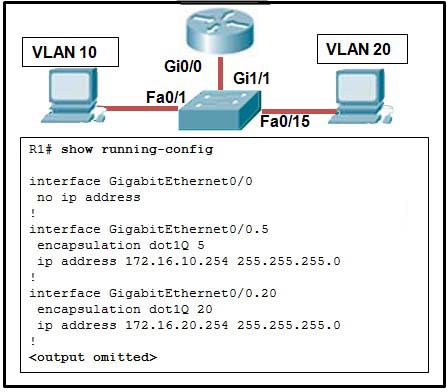
г) EtherChannel-ге ең көп дегенде сегіз бөлек сілтеме қосуға болады.

**№2 жаттығу. Қолданбалы тапсырмалар**

* 1. Суретке қараңыз. Желілік әкімші CiscoVille маршрутизаторын интерактивті VLAN маршрутизацисын қамтамасыз ету үшін қосты. Интерактивті inter-VLAN бағыттауды қосу үшін CiscoVille маршрутизаторындағы Gi0/0 интерфейсіне қосылған коммутаторға қандай команда қажет болады?\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* 1. Суретке қараңыз. Желілік әкімші inter-VLAN интерфейс бағыттауының конфигурациясын тексереді. PC2 пайдаланушылары PC1-мен байланықа шыға алмайтындықтарын хабарлайды. Мәселе неде?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**3 БӨЛІМ**

# Сымсыз желілер

Сымсыз желілер клиенттің икемділігін, оның кез келген уақытта, кез келген жерінен желіге қосылу қабілетін, сондай-ақ қосылысты жоғалтпай орнын ауыстыру мүмкіндігін қамтамасыз етеді. LAN (WLAN) сымсыз желісі әдетте үй, кеңсе және қоғамдық орталарда пайдаланылатын сымсыз желіге жатады. Сымсыз желі кабельдердің орнына радтожелілерді пайдаланады, әдетте ол коммутацияланатын желіде іске асады, ал кадр форматы Ethernet-те қолданылатын пішімге ұқсас.

Бүгінде қоғамдастық желілер тұрақты жол жүруде болатын пайдаланушыларды қолдауды қамтамасыз ете отырып, жылдам қарқынмен дамуда. Пайдаланушылар әртүрлі құрылғыларды пайдалана отырып, компьютерлерді, ноутбуктерді, планшеттік компьютерлер мен смартфондарды қоса алғанда, бәріне қосыла алады. Жеделдіктің осы тұжырымдамасы шеңберінде пайдаланушылар қозғалыста болып та желіге қосыла алады.

Мұндай жеделдікті әртүрлі инфроқұрылымдар қамтамасыз ете алады (сымды LAN , интернет-провайдерлер желісі), бірақ қоғамдастық ортаның маңызды құраушысы LAN (WLAN) сымсыз желісі болып табылады.

Еңбек өнімділігі мұнда тұрақты жұмыс орнымен немесе бюелгілі уақыт кезеңімен шектелмейді. Енді пайдаланушылар кез келген уақытта және кез келген жерден: кеңседен әуежайға немесе үйге дейін қосылу мүмкіндігіне сене алады. Қызметкерлер іскерлік жол жүрулерінде хабарламалар тексерістер немесе бірнеше хабарласуларды орындау үшін рейстер арасындағы телефон байланысын төлеуші еді. Енді қызметкерлер электронд және дыбыстық поштаны тексере алады, сондай-ақ өздерінің смартфондарынан өз жобаларының жағдайын байқай алады.

Қазіргі пайдаланушылар сымсыз желінің роумингін барлық жағдайда пайдалана алуға мүмкіндігі бар. Роуминг қосылысты жоғалтпай интернетке сымсыз құрылғылардың қатынауын қамтамасыз етеді.

Сымсыз желілер жеделдікті қалайша қамтамасыз ететінін мысал арқылы көру үшін суреттегі бейнені басыңыз.

**Сымсыз желінің артықшылықтары**

Сымсыз байланыс қоғамдастық, сондай-ақ үй желілері үшін көптеген артықшылықтарға ие болады. Мұндай артықшылықтарға өзгермелі талаптарға бейімделу және дамыту мүмкіндігінің шығындарын азайту өнімділік пен икемділікті арттыру жатады.

Көптеген компанияларда LAN қатынас желілері кеңсенің күнделікті жұмысы үшін пайдаланылады. Бірақ, қызметкерлер көбіне қашықтан жұмыс істейді және LAN қоғамдастық желі ресурстарына өз жұмыс үстелінен, сондай-ақ басқа адамдардан қатынай алады. Қызметкерлер өзінің сымсыз құрылғыларын жиналыстарға, әріптестер кабинетіне, конференц-залға, тіпті клиент нысандарына, кәсіпорын ресурстарына қатынай отырып, пайдалана алады. Бұл жағдайларда сымсыз желілер қажетті икемділікті қамтамасыз етеді. Қажет материалдарды жіберуге немесе желі ресурстарына қатынау үшін сымды қосылуды іздеуге уақыт өткізудің орнына, сымсыз байланыс арқылы LAN желісі ресурстарына әртүрлі сымсыз құрылғыларын оңай ұсына алады.

Сымсыз қатынау осы шамаларда өлшеу айтарлықтай қиын болса да, қызметкерлердің еңбек өнімділігін арттыруға және жұмыс бастылығының азаюына жағдай жасайды. Қызметкерлер сымсыз желілер арқасында кез келген уақытта және кез келген орында жұмыстың икемділік мүмкіндігін алады. Олар кеңседе немесе түскі үзіліте кафеде отырыпклиенттер сұранысына жауап бере алады. Олар басқаруды оңтайландыра отырып, клиенттер үшін нәтижелерге тез және сапалы қол жеткізіп, сондай-ақ кірісті ұлғайтып есептелген секундтарда электронды поштаға және басқа жұмыс ресурстарына қатыса алады.

Сондай-ақ сымсыз желілерді пайдалану шығындарды азайтуға мүмкіндік береді. Енді сымсыз инфроқұрылымды пайдаланатын компанияларда шығындардың үнемі, жабдықтың орнын ауыстыруы немесе кез келген өзгерістерінде іске асырылады – мысалы, қызметкердің ғимарат шегінде немесе жабдықты қайта ұйымдастыруда немесе зертханаларда, сондай-ақ осы немесе басқа жоба шеңберінде уақытша кеңселер мен нысандарда ауысуға мүмкіндік жасайды.

Сымсыз желілердің тағы бір маңызды артықшылығы – технологиялар мен қажеттіліктердің өзгеруіне бейімделу қабілеті болып табылады. Сымсыз желіге жаңа жабдықты қосу онша қиындық келтірмейді. Үй жағдайында сымсыз қосылудың мысалын қарастырайық. Пайдаланушылар ас үйде, қонақ үйде немесе бөлмеден тыс жерде отырып та веб-сайтқа қатынай алады. Үй желісін пайдаланушылар жаңа құрылғыларды қосады (мысалы, смартфондар, плашетті компьютерлер, ноутбуктар мен интеллектуалды функциялары бар теледидарлар).

## 3.1. Сымсыз байланыс тұжырымдамалары

3.1.1 Сымсыз технологиялар

Сымсыз байланыс әртүрлі кәсіптік салаларда пайдаланылады.

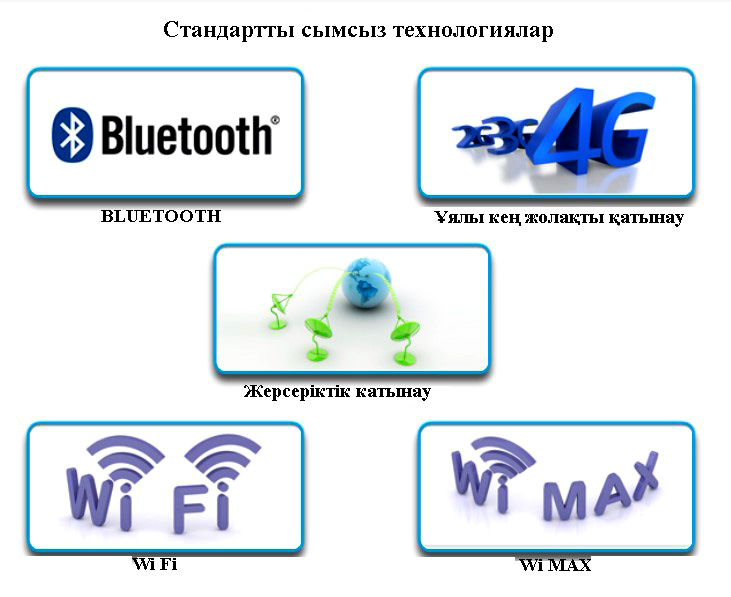
Сымсыз технологиялардың ауқымы тұрақты кеңеюімен бірге, осы жағдайда қарастырудың негізгі пәні жеделдікті пайдаланушылардың жеделдігін (ұтқырлық) қамтамасыз ететін сымсыз желілер болап табылады. тұтас алғанда, сымсыз желілерді келесі санаттарға бөлуге болады.

* **Дербес сымсыз желі (WPAN).** Бұл желінің әрекет радиусы бірнеше метрді құрайды. WPAN желілерінде Bluetooth немесе Wi-Fi Direct қолдауымен пайдаланылатын құрылғылар.
* **LAN (WLAN) сымсыз желілері.** Бұл типтегі желілер бірнеше жүз метр ауқымында (мысалы, бөлмеде, үйде, кеңседе және тіпті ғимараттар кешендері желілерінде) жұмыс істейді.
* **Ауқымды желілер (WWAN).** Бұл желілер бірнеше киллометр радиусында жұмыс істейді (мысалы, муниципаль желілерінде, ұяла байланыс желілерінде немесе тіпті СВЧ-реле арқылы халықаралық байланыс арналарында).

Жоғарыда аталған сымсыз желілер құрылғыларына қосылуды қолдайтын әртүрлі сымсыз технологиялар туралы қосымша мәліметтерді бейнелеу үшін суреттегі компонеттерді басыңыз:

* **Bluetooth**. Бастапқыда WPAN IEEE 802.15 стандарты болды, оны 100 метрге дейінгі қашықтықта (0,1 км) деректермен алмасу үшін құрылғыларды қосу үшін пайдаланады. Bluetooth кейінгі нұсқалары Bluetooth Special Interest Group (<https://www.bluetooth.org/>) сәйкес стандартталған.
* **Wi-Fi (wireless fidelity, сымсыз нақтылық).** Үй және қоғамдастық желілерді пайдаланушылар үшін 300 м дейінгі (0,18 мили) қашықтықта дауыс пен деректерді қоса алғанда, желіге қатынауды ұсыну мақсатында WLAN IEEE 802.11 қосылады.
* **WiMAX (кең жолақты радиобайланыс хаттамасы).** WWAN IEEE 802.16 желі стандарты 50 км (30 миль) дейінгі қашықтықта сымсыз кең жолақты қатынауды қамтамасыз етеді. WiMAX кабельді және кең жолақты DSL – қосылысының баламасы болып табылады. 2005 ж. WiMax стандартына жеделдік функциялары қосылды, осыған байланысты бұл стандартты байланыс операторлары ұялы кең жолақты қатынауды ұсыну үшін пайдалана алады.
* **Ұялы кең жолақты қатынау.** Ол желіге кең жолақты жедел қосу үшін ұсыну мақсатында байланыс операторының желіге ұялы қатынауды пайдаланатын бірнеше корпоративтік, мемлекеттік және халықаралық ұйымдардан тұрады. Екінші – буынды ұялы телефондар 1991 жылы (2G) алғаш пайдаланылды. 2001 және 2006 жж үшінші (3G) және төртінші (4G) буынды жеделдік байланыс технологиялары шеңберінде тіпті жоғары жылдамдыққа қол жеткізілді.
* **Жерсеріктік кең жолақтық қатынау.** Геостационарлық жерсерігі (GEO) бойынша реттелген жерсеріктік антеннасын пайдалану арқылы қашықталған нысандарға желілік қатынауды ұсынады. Әдетте, бұл технология өте қымбат және тікелей көрінуді қамтамасыз етуді талап етеді.

Сымсыз технологиялардың көптеген әртүрлі типтерін қолжетімді. Бірақ, бұл тарауда негізгі 802.11. стандартының WLAN желісіне назар аударылады.



Радио жиіліктер

Барлық сымсыз құрылғылар электрмагнитті спектрдің радио толқындары ауқымында жұмыс істейді. Радиожиіліктік (РЖ) реттеуді белгілеу үшін халықаралық электрбайланысу одағы, электрбайланысты стандарттау секторы (ITU-R) жауапты болады. әртүрлі мақсаттар үшін жиіліктік диапазондары қарастырылған, оларды жолақтар деп атайды. Кейбір жолақтар электрмагнитті спектрде қатаң тәртіптеледі және апатты құтқару қызметтерінің байланысу желілерінде, трафиктік бақылау салаларында пайдаланылады. Басқа құжаттар лицензиялауға жатпайды (мысалы, өнеркәсіптік, ғылыми және медициналық жиілікті диапазонында, сондай-ақ ұлттық ақпараттық инфроқұрылымның диапазондары).

WLAN желісі 2,4 ГГц жиіліктік жолақта өнеркәсіптік, ғылыми және медицина диапазонында, сондай-ақ 5 ГГц жиілігінде ұлттық ақпараттық инфроқұрылым жолағында жұмыс істейді.



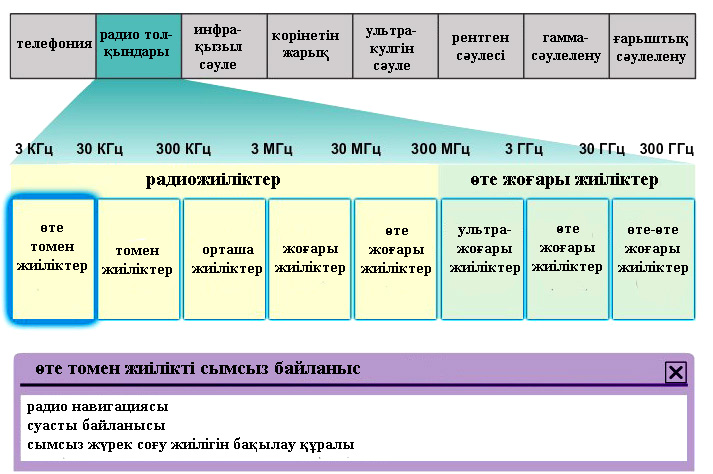
Суретте көрсетілгендей, сымсыз байланыс электрмагнитті спектрдің радиотолқындары диапазонына (яғни, 3-300 ГГц) іске асырылады. Радиотолқындар диапазоны СВЧ секторына және радио желілік секторына бөлінеді. WLAN, Bluetooth ұялы байланыс және жерсеріктік байланыс желілері УВЧ, СВЧ және КВЧ диапазондарында жұмыс істейді.

LAN сымсыз байланыс құрылғылары радиотолқын диапазонының нақты жиілігіне бағдарланған таратқыштармен және қабылдағыштармен жабдықталған. Жеке алғанда, 802.11 стандартының LAN сымсыз желісі үшін келесі жиіліктік жолақтар бөлінеді:

* **2,4 ГГц (УВЧ)**: 802.11b/g/n/ad
* **5 ГГц (СВЧ)**: 802.11a/n/ac/ad
* **60 ГГц** **(КВЧ)**: 802.11ad



**Электромагнитті сәуелелендіру спектрінің радиожиілікті диапазоны**



3.1.2 Сымсыз желі стандарттары

WLAN IEEE 802.11 желі стандарты сымсыз арналардың MAC дейгей асты және фихикалық деңгей үшін өнеркәсіптік, ғылыми және медициналық лицензияланатын жиіліктік жолақты диапазондарында радиожиіліктің қалай жұмыс істейтінін анықтайды.

Өткен жылдары үшін IEEE 802.11 стандартын іске асырудың бірқатары әзірленген. Төменде осы стандартты толығырақ қарастырамыз:

* **802.11.** 1997 жылы жасалған, бүгінгі күні ескірген болып есептеледі. Бұл 2,4 ГГц жиілікті жолақта жұмыс істейтін және 2 Мбит/с жылдамдығын қамтамасыз ететін WLAN желісінің бастапқы ерекшелігі. Осы стандартты жасау сәтінде LAN сымды желілері 10 Мбит/с жылдамдығын қамтамасыз етті, осы себепті жаңа сымсыз технологиялар бастапқы кезеңде кең танылмады. Сымсыз құрылғылар сымсыз сигналдарды тарату және қабылдау үшін бір антеннамен жабдықталған.
* **IEEE 802.11a.** Ол 1999 жылы әзірленген. Жүктелген 5 ГГц жиілікті жолақта жұмыс істейді және 54 Мбит/с жылдамдықты қамтамасыз етеді. Сонымен, бұл стандарт жоғары жиілікте жұмыс істейді, ол төсемнің аз аумағын алады және ғимарат ішінде тиімділігі аз. Сымсыз құрылғылар сымсыз сигналдарды тарату мен қабылдау үшін бір антеннамен жабдықталған. Осы стандартқа сәйкес жұмыс істейтін құрылғы 802.11b және 802.11g стандарттарымен сәйкеспейді.
* **IEEE 802.11b.** 1999 жылы әзірленген. 2,4 ГГц жиілікті жолақта жұмыс істейді және 11 Мбит/с дейінгі жылдамдықты қамтамасыз етеді. Осы стандартқа сәйкес келетін жұмыс істейтін құрылғы үлкен диапазонға ие және ғимарат ішінде пайдалану барысында 802.11а стандартының құрылғыларымен салыстырғанда жоғарырақ тиімділікті көрсетеді. Сымсыз құрылғылар сымсыз сигналдарды тарату мен қабылдау үшін бір антеннамен жабдықталған.
* **IEEE 802.11g.** 2003 жылы әзірленген. 2,4 ГГц жиілікті жолақта жұмыс істейді және 54 Мбит/с дейінгі жылдамдықты қамтамасыз етеді. Осы стандартқа сәйкес жұмыс істейтін құрылғы 802.11b стандартының құрылғысы жұмыс істейтін сол радиожиілікпен, сол диапазонмен жұмыс істейді, бірақ 802.11а стандартының өтпелі қабілетіне ие. Сымсыз құрылғылар сымсыз сигналдарды тарату мен қабылдау үшін бір антеннамен жабдықталған. Бұл стандарт 802.11b стандартымен сәйкеседі. Бірақ, 802.11b стандартының клиенттерімен жұмыс істеуде жалпы өтпелі қабілеті азаяды.
* **IEEE 802.11n.** 2009 жылы әзірленген. 2,4 ГГц және 5 ГГц жиілікті жолақта жұмыс істейді, екі жолақты құрылғы ретінде танымал. Деректерді таратудың стандартты жылдамдығы – 150-600 Мбит/с; әрекет ету диапазоны – 70 м дейін. Сонымен бірге, қатынау нүктелеріне және сымсыз клиенттерге жоғарырақ жылдамдықты қамтамасыз ету үшін көпарналы кіріс - көпарналы шығыс технологиясын (MIMO) пайдаланатын бірнеше антенна талап етіледі. MIMO технологиясы деректерді алмасу өнімділігін арттыруға мүмкіндік беретін таратқыш және қабылдағыш сапасындағы бірнеше антенналарды пайдаланады. Технология төртке дейінгі антеннаны қолдайды. 802.11n стандарты 802.11a/b/g құрылғыларымен кері сыйысымдылықты қолдайды. Бірақ, аралас ортаны қолдау деректерді тарату жылдамдығын шектейді.
* **IEEE 802.11ac.** 2013 жылы әзірленген 5 ГГц жиілікті жолақта жұмыс істейді, ол 450 Мбит/с-тен 1,3 Гбит/с (1300 Мбит/с)дейінгі диапазонда деректерді тарату жылдамдығын қамтамасыз етеді. Бұл стандарт деректерді алмасу өнімділігін арттыру үшін МІМО технологиясын пайдаланады. Бұл стандарт үшін сегізге дейінгі антенна қолданылады. 802.11ас стандарты 802.11a/n құрылғыларымен кері сыйымдылықты қолдайды, бірақ аралас ортаны қолдау деректерді таратудың болжалды жылдамдығын шектейді.
* **IEEE 802.11ad.** 2014 жылы шығару жоспарланған. Бұл стандартты WiGig деп атайды. Ол үшжолақты Wi-Fi шешім қолданады, онда 2,4 ГГц, 5 ГГц және 60 ГГц жиілікті жолақтар іске қосылады. Стандарт теориялық түрде 7 Гбит/с дейінгі деректерді тарату жылдамдығын қамтамасыз етеді. Сөйте тұра, 60 ГГц жолағы тікелей көрілімді талап ететін жұмыс үшін технология, демек сигнал қабырғадан өте алмайды. Құрылғылар роумингінде пайдаланушылар төмендеу жиілігі бар 2,4 ГГц және 5 ГГц жолақтарда байланысады. Стандарт Wi-Fi сәйкесті құрылғыларымен кері сыйымдылықты қолдайды. Бірақ, аралас ортаны қолдау деректерді тарату жылдамдығын шектейді.

Суретте 802.11 стандартының әрқайсысының қысқаша жазбасы ұсынылған .

**802.11 стандарттарын салыстыру**

|  |  |  |  |
| --- | --- | --- | --- |
| IEEE стандартты | максималды жылдамдық | жиілігі | кері үйлесімділік |
| 802.11 | 2 Мбит/с | 2,4 ГГц | - |
| 802.11а | 54 Мбит/с | 5 ГГц | - |
| 802.11b | 11 Мбит/с | 2,4 ГГц | - |
| 802.11g | 54 Мбит/с | 2,4 ГГц | 802.11b |
| 802.11n | 600 Мбит/с | 2,4 ГГц және 5 ГГц | 802.11a/b/g |
| 802.11ac | 1,3 Гбит/с (1300 Мбит/с) | 5 ГГц | 802.11a/n |
| 802.11 ad | 7 Гбит/с (7000 Мбит/с) | 2,4 ГГц 5 ГГц және 60 ГГц | 802.11 a/b/g/n/ac |

**Wi-Fi сертификациясы**

Бұл стандарттар әртүрлі өндірушілер дайындаған құрылғылардың үйлесімділігін қамтамасыз етеді. WLAN желісі стандарттарын анықтайтын үш халықаралық ұйым бар:

* **ITU-R радиобайланыс секторы** радиожиіліктері мен жерсеріктік орбиталардың спектрін бөһлуді реттейді.
* **IEEE** деректерді тарату үшін радиожиіліктерді қандай түрде модульдейтінін анықтайды. Бұл ұйым LAN/MAN IEEE 802 желі стандартты тобына жататын жергілікті және қалалық (MAN) желілер стандарттарына қызмет көрсетеді. 802.3 Ethernet және 802.11 WLAN стандарттары IEEE 802 стандарттары тобының негізгілері болып табылады. Мұнда IEEE радиожиілік модуляция құрылғылары үшін стандарттарды анықтайды, ал бұл ұйым өндіріс стандарттарын анықтамайды. Демек, әртүрлі жеткізушілерімен 802.11 стандарттарының интерпретациясы құрылғы сәйкестігімен кедергі жасауы мүмкі.
* **Wi-Fi Alliance**. Wi-Fi Alliance® ([http://www.wi-fi.org](http://www.wi-fi.org/)) өнеркәсіптік сауданың ауқымдық коммерциялық емес қауымдастығы болып табылады, оның міндеті WLAN желілерін дамытуға және енгізуге жағдай жасайды. Бұл қауымдастыққа салалық нормалар мен стандарттарға сәйкесті жеткізушілерді сертификаттау жолымен 802.11 стандарты өнімдерінің өзіндік құнын арттыруға бағдарланған жеткізушілер енді.

Wi-Fi Alliance Wi-Fi желісін және келесі үйлесімділік түрлерін сертификаттайды: IEEE 802.11a/b/g/n/ac/ad үйлесімділігі

* IEEE 802.11i шеңберінде (EAP) кеңйтілген хаттамасын аутентификациялау және WPA2™ қауіпсіз пайдалану.
* Құрылғылар қосылысын қарапайымдылайтын Wi-Fi Protected Setup (WPS) функциясы.
* Ортаны құрылғылармен бірлесіп пайдалану үшін Wi-Fi Direct
* Wi-Fi қатынау нүктесі желісіне қарапайым және қауіпсіз қосылуды қамтамасыз ету үшін Wi-Fi Passpoint
* құрылғылар арасында бейнекөрілімді еш қиындықсыз тарату және бейнелеу үшін Wi-Fi Miracast

**WLAN желілерін LAN желісімен салыстыру**

WLAN желілерінің пайда болуы жергілікті Ethernet желілеріне ұқсас. IEEE 802 LAN/MAN иерархиялық желілердің архитектура стандарттарының портфелін таңдады. Оның негізгі екі жұмыс тобы 802: 802.3 Ethernet және 802.11 WLAN болып табылады. Дегенмен, бұл екі топ арасында елеулі өзгешеліктер бар.

WLAN желісінің деректерін тарату арнасының деңгейі физикалық деңгейде және МАС-деңгейішілік деңгейінде кабельдердің орнына ражиожиілікті қолданады. Кабельдер мен радиожиіліктер арасында келесі ерекшеліктер байқалады:

* Радиожиіліктерде қоршаммен қорғалған кабельдерге қарағанда мұндай шектеулері жоқ. Сондықтан деректер кадрлары радиожиілікті сигналды қабылдай алатындардың бәріне оған қатынауды ұсыну мақсатында радиожиілікті арналар бойынша таратылуы мүмкін.
* Кабель экрандаушы қоршаммен қорғалған уақытта радиожиіліктер сыртқы сигналдардан қорғалмаған. Радиожиіліктер бір географиялық сала шегінде бір біріне тәуелсіз жұмыс істейді, бірақ бір және сол немесе соған ұқсас жиілікте жұмыс істеу барысында бөгеуілдер болуы мүмкін.
* Радиожиіліктерді тарату кез келген толқынды технологиялардың, мысалы радионың, өзіне тән сол проблемаларымен байланысты. Мысалы, радио сигналды көздерінен ажыратқанда радио стансалар бір біріне қондырылады, ол статистикалық кедергі деңгейін арттырады. Соңында сигнал толық жоғалады. LAN сымды желілерінде сәйкесті ұзын, сигналдың тиісті қуатын қамтамасыз ететін кабельдер пайдаланылады.
* Әр елде радиожиілікті жолақтар әртүрлі құрылады. WLAN желісін пайдаланғанда LAN сымды желілеріне қолданылмайтын қосымша ережелер мен стандарттар жинағы әрекет етеді.

Сондай-ақ LAN сымды желісінен WLAN желісінің ерекшеліктері :

* WLAN желілері сымсыз қатынау нүктесі немесе сымсыз маршрутизатор арқылы клиенттерге қосу үшін қызмет етеді, бірақ Ethernet коммутаторы арқылы қосылмайды.
* WLAN желілері разеткаға қосылған жеке желілердің құрылғыларынан ерекшелігі көбіне жедел құрылымдарға қосу үшін аккумулятормен жұмыс істейді. Сымсыз желі адаптерлерін пайдалану аккумулятордың жедел құрылғысының жұмы уақытын қысқартады.
* WLAN желілері РЖ-тасушыларына (жиілікті жолақтарда) қатынауда бәсекелес тораптарды қолдайды. 802.11 стандарты деректерді тарату ортасына қатынау үшін (CSMA/CD) қақтығыстарын табу технологияларының орнына (CSMA/CA) қақтығыстарды болдырмау технологияларын пайдалануды уәждейді. Бұл қақтығыстарды осы немесе басқа орта шектерінде тиімді болдырмауға мүмкіндік жасайды.
* Ethernet сымсыз дербес желілерінде және сымды дербес желілерінде кадрлардың әртүрлі форматтары пайдаланылады. Сымсыз дербес желілер үшін 2-деңгейдегі кадрдың басына қосымша ақпаратты қосу қажет.
* WLAN желілеріне қатынаста құпиялықпен байланысты үлкен проблемалар туындайды, себебі радиожиіліктер нысанның шегінен тыс шығуы мүмкін.

**WLAN желілерін LAN желілерімен салыстыру**

|  |  |  |
| --- | --- | --- |
| Тән | 802.11 стандартты LAN сымсыз желі | 802.3 стандартты Ethernet  LAN желі |
| Физикалық деңгей | Радиожиілік диапазоны | Кабельді жалу |
| Бұқаралық ақпарат құралдарына кіру | Соқтығысуды болдырмау | Соқтығысуды анықтау |
| Қол жетімділігі | Кіру нүктесінің диапазонында радио байланысын қолдайтын желілік адаптерлері бар барлық пайдаланушылар | Кабель қосылымы қажет |
| Кедергі әсері | Ия | Салдарсыз |
| Реттеу | Үкімет тарапынан қосымша реттеу | IEEE стандарт бойынша анықталады |

3.1.3 WLAN желілерінің құрауыштары

*Сымсыз желілік адаптерлер*

Қарапайым сымсыз желі жасау үшін кемі екі құрылғы талап етіледі. Бұл құрылғылардың әрқайсысы бір жиілікке бағдарланған радиотаратқыштан және радиоқабылдағыштан тұруы қажет.

Бірақ, сымсыздардың көпшілігі үшін жайнамалау талап етіледі:

* сымсыз желілік адаптерлермен жарақталған соңғылық құрылғылар;
* инфроқұрылым құрылғысы (мысалы, сымсыз маршрутизатор немесе сымсыз қатынау нүктесі).

Сымсыз деректермен алмасу үшін соңғылық құрылғыларға тіркелген радиотаратқыш және радиоқабылдағыш арқылы сымсыз желілік адаптер және адаптерлер жұмысы үшін драйвер талап етіледі. Барлық қазіргі ноутбуктар, плашетті компьютерлер және смартфондар интеграцияланған сымсыз желілік адаптерлермен жабдықталған. Бірақ, егер құрылғыда сымсыз желілік адаптер болмаса, онда сымсыз USB-адаптерді пайдалануға болады.

3.1 суретте екі сымсыз USB-адаптер көрсетілген.



3.1 сурет – Сымсыз USB адаптердар

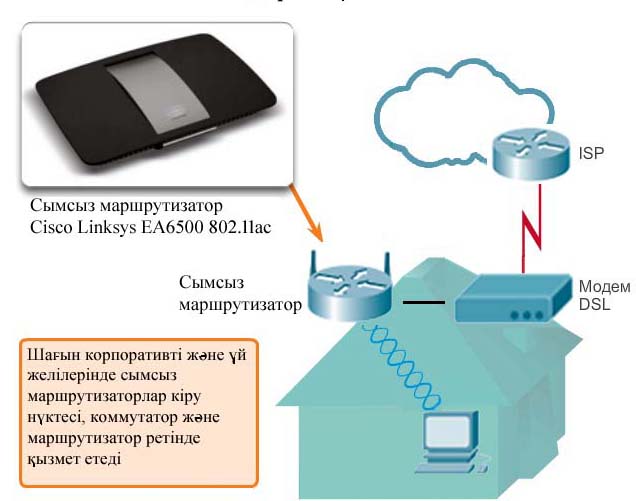
*Үйішілік сымсыз маршрутизаторы*

Инфроқұрылым құрылысының типінің соңғылық құрылғысында бірлестікті және аутентификацияны орындайды, WLAN желісінің мөлшері мен тармақтарына сай қолданылады.

Мысалы, пайдаланушы үй желісіне әдетте, кіріккен шағын маршрутизатор арқылы бір біріне сымсыз құрылғыларды қосады. Мұндай шағын маршрутизаторлар кіріккен сервистермен келесі қызметтерді атқарады:

* **Қатынау нүктесі –** 802.11a/b/g/n/ac сымсыз қатынауын ұсынады.
* **Коммутатор –** сымды құрылғыларды қосу үшін толық дуплексті режімде және төрт портты Ethernet 10/100/1000 камутатор түрінде ұсынады.
* **Маршрутизатор –** басқа желілік инфроқұрылымдармен байланыс үшін үндемеу бойынша шлюз түрінде ұсынады.

Мысалы, 3.2-суретте көрсетілген Cisco Linksys EA6500 маршрутизаторы үй желісі немесе шағын кәсіпорынның корпоративтік желісіне сымсыз қатынау құрылғысы сапасында іске асырылады. Сымсыз маршрутизатор DLS-модеміне қосылады және қызметтер жиынтығының жалпы идентификаторынан (SSID) тұратын сигналдарды тарату жолымен сымсыз маршрутизаторы қосылады және өз жұмысын жүргізеді. Ішкі құрылғылар SSID маршрутизаторының идентификаторын сымсыз табуды орындайды және Интернет желісіне қатынау үшін маршрутизаторға кірігу мен аудентификацияны орындауға тырысады.



3.2 сурет – Стандартты үй желісі

Бұл ортада Linksys EA6500 маршрутизаторына ұсынылатын жүктеме айтарлықтай төмен. Сөйтіп, маршрутизатор WLAN, 802.3 Ethernet желісіне және интернет-провайдер желісіне қосылумен қатынауды қамтамасыз етумен басқара алады. Сондай-ақ, маршрутизатор бірнеше қосымша функцияларды ұсынады, олардың ішінде шағын жинағыштарға немесе принтерлер қосу үшін Wi-Fi WPS, USB-порттары арқылы қарапайым орнату және баптаумен қызмет көрсету сапасының қызметі (QoS), IPv6 қолдауы, ағымдық бейнені таратуды қолдау үшін оңтайландыру, жоғары жылдамдықпен қатынау арасында бірқатар қосымша қызметтерді ұсынады.

Бұдан басқа, сымсыз желіде және сондай-ақ, сымды желіде желілік қызметтердің жиынын кеңейту талап етілетін үй желісін пайдаланушылар Powerline сымсыз адаптерін пайдалануына болады. Осы адаптерлер көмегімен құрылғы электр қоректендіру розеткалары арқылы желіге тікелей қосыла алады, бұлар ағымдық HD-бейнесін және онлайн-ойындарын тарату үшін өте ыңғайлы. Бұл құрылғыларды орнату қарапайым: электр қоректендіру розеткасына немесе желілік сүзгіге қосылыңыз және құырлығына бастырманы қарапайым басу арқылы қосыңыз.

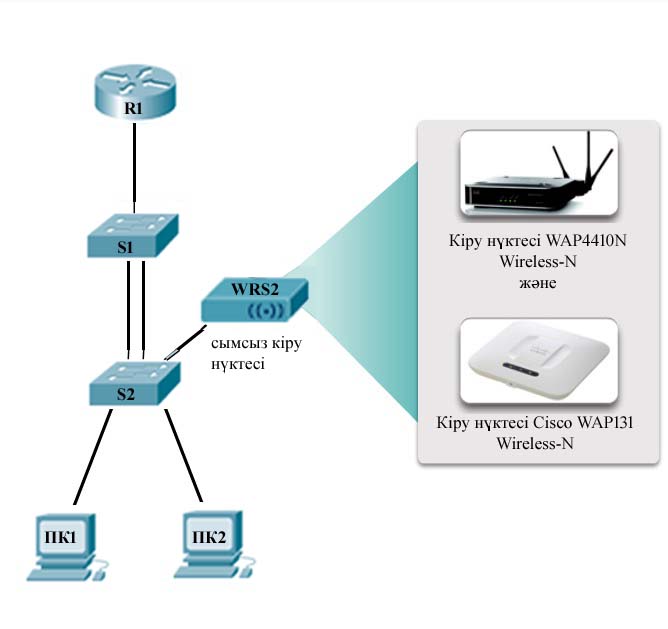
*Сымсыз бизнес-шешімдер*

Сымсыз желіге қосылуды ұсынатын ұйымдарға өз клиенттері үшін қосымша қосу мүмкіндігін қамтамасыз ететін WLAN инфроқұрылымы талап етіледі.

**Ескерту**. IEEE 802.11 стандарты шеңберіндегі сымсыз клиент (STA) стансасы деп аталады. Осы тарауда «сымсыз клиент» термині сымсыз желіге қосылуды қолдайтын кез келген құрылғыны білдіреді.



3.3-суретте көрсетілген шағын кәсіпорын желісі 802.3 Ethernet LAN стандартының LAN желісі болып табылады. Әр клиент (мысалы ПК1 және ПК2) желілік кабель арқылы коммутаторға қосылады. Коммутатор желіге қатынауды алатын клиенттің нүктесі болып табылады. назар аударыңыз, сондай-ақ сымсыз қатынау нүктесі коммутаторға қосылған. Бұл мысалда сымсыз желіге қосылу үшін Cisco WAP4410N немесе WAP131 қатынау нүктесі пайдаланылуы мүмкін.



3.3 сурет - Қатынау нүктесі сымды инфроқұрылымға қосылады

Өз SSID идентификаторын жариялаған сымсыз клиенттер жақын қатынау нүктесін табу үшін өзінің сымсыз желілік адаптерін пайдаланады. Бұдан кейін клиенттер 3.4-суретте көрсетілгендей қатынау нүктесінде бірігу мен аутентификацияны орындауға тырысады. Аутентификациядан өткеннен кейін сымсыз желіні пайдаланушылар желі ресурстарына қатынай алады.



**Ескерту**. Шағын компаниялар ірі компанияларға қарағанда сымсыз ресурстарға басқа талаптар қояды. Үлкен сымсыз желілер сымсыз желіні орнату мен басқаруды қарапайым ету мақсатында қосымша сымсыз жабдықты талап етеді.

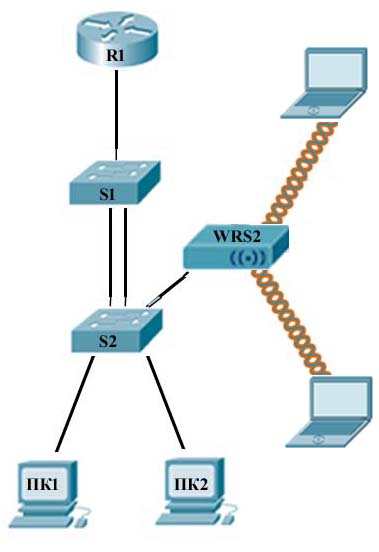


*Сымсыз қатынау нүктелері*

Қатынау нүктелері дербес және контроллермен басқарылатын болуы мүмкін.

**Қатынаудың дербес нүктелері**

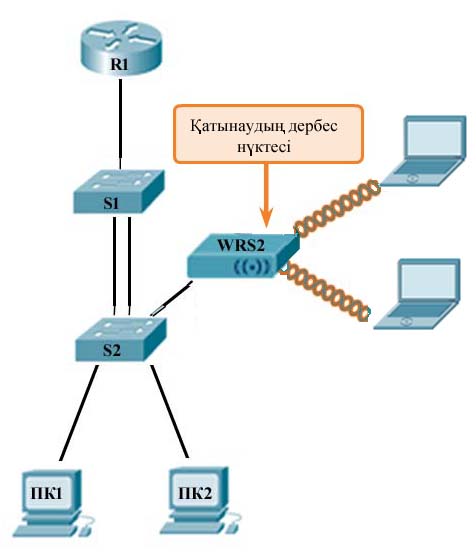
Кейде «ауыр» деп аталатын қатынаудың дербес нүктелері (CLI) Cisco командалық жол интерфейсі немесе пайдаланушының графикалық интерфейсі көмегімен бапталатын дербес құрылғылар түрінде болады. Қатынаудың дербес нүктелерін желіде кемі қатынаудың екі нүктесі болған жағдайда пайдалану ұсынылады. Қатынаудың бірнеше нүктелерін басқаратын нұсқасы ретінде CiscoWorks Wireless LAN Solution Engine (WLSE) және (WDS) сымсыз демоны арқылы іске асырылуы мүмкін.



* 1. сурет - Клиенттер қатынау нүктесіне қосылады

Қатынаудың дербес нүктесінің мысалы – үй маршрутизаторы, себебі қатынау нүктесінің барлық конфигурациясы құрылғыда сақталады.

3.5-суретте қатынаудың дербес нүктесі шағын желіде көрсетіледі. Сымсыз желі ресурстарына сұраныстың артуы мен қатынау нүктелерінің үлкен саны қажеттілігі тууы мүмкін. Қатынаудың әр нүктесі қатынаудың басқа нүктелеріне тәуелсіз жұмыс істейді. Оларды баптау және басқару қолмен орындалады.



3.5 сурет – Қатынаудың дербес нүктесі

3.1.4Контроллермен басқарылатын қатынау нүктелері

Контроллермен басқарылатын қатынау нүктелері құрылғылар серверіне тәуелсіз болып табылады, олар үшін бастапқы баптау талап етілмейді. Cisco контроллерді пайдалану арқылы екі сымсыз шешімді ұсынады. Контроллермен басқарылатын қатынау нүктелерін желіде қатынаудың көп нүктелері талап етілетін жағдайда пайдалану ұсынылады. Қосымша қатынау нүктелерін қосуда олардың әрқайсы автоматты түрде баптауы мен басқарудың WLAN контроллерімен орындалады.

3.6-суретте шағын желіде контроллермен басқарылатын қатынау нүктесі көрсетілген. Қатынау нүктелерін басқару үшін қажетті WLAN желісінің контроллеріне назар аударыңыз. Бұл контроллерді пайдалану артықшылығы оны қатынаудың бінеше нүктелерін басқару үшін пайдалануға болатындығында.



3.6 сурет - Контроллермен басқарылатын қатынау нүктесі

Қатынаудың кейбір нүктелері контроллермен басқарылатын қатынау нүктесі режімінде және сондай-ақ, дербес режімде жұмыс істей алады.

*Шағын сымсыз желілер үшін шешімдер*

Шағын сымсыз желілер үшін Cisco қатынаудың сымсыз дербес нүктелері ретінде келесі шешімдер ұсынады:

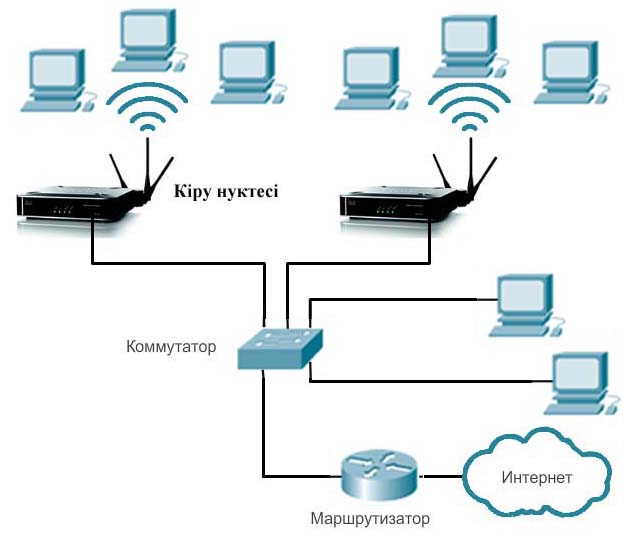
* **Cisco WAP4410N қатынау нүктесі**. Бұл қатынау нүктесі шағын компаниялар үшін өте ыңғайлы, себебі пайдаланушылардың шағын топтары үшін екі қатынау нүктесі және қолдауы талап етіледі.
* **Cisco WAP121 және WAP321 қатынау нүктелері**. Бұл қатынау нүктелері шағын компаниялар үшін өте ыңғайлы, ол үшін қатынаудың бірнеше нүктелерін пайдалану есебінен сымсыз желіні ықшамдау талап етіледі.
* **Cisco AP541N қатынау нүктелері**. Бұл қатынау нүктесі шағын және орташа компаниялар үшін өте ыңғайлы, мұнда басқаруда сенімді және қарапайым қатынау нүкте кластері талап етіледі.

Қатынау нүктелерінің көршілігін корпоративтік деңгейде РоЕ қолдайды.

3.7-суретте шағын корпоративтік желілер үшін топология мысалы ұсынылған, мұнда WAP4410N қатынау нүктесі пайдаланылаы.

Қатынаудың барлық нүктелерн қолдау және орындау жеке орын алады.Әрине қатынаудың бірнеше нүктесі талап етілсе, онда мәселелер туындауы мүмкін.

Міне осы себепті WAP121, WAP321 и AP541N қатынау нүктелері контреллерлерді пайдаланбай қатынау нүктелерінің кластерленуін қолдайды. Кластер әкімшілеудің бірегей нүктесі ретінде ұсынылады және әкімшіге жекелеген сымсыз құрылғылардың жиынтығы ретінде емес, нүктелерді бір сымсыз қатынау желісіне жаймалауды қарастыруға мүмкін береді. Кластерлеу өсімтал сымсыз желісін орнату, басптау және басқаруды оңай етуге мүмкіндік жасайды. Қатынаудың бернеше нүктелерін кластер шектерінде барлық құрылғыларды бір конфигурациямен жаймалауға және баптауға болады. бұл жағдайда сымсыз желіні басқару бір жүйе түрінде іске асырылады және мұнда нүктелер арасындағы өзара бөгеуілдерге мазалану немесе қатынаудың әр нүктесін жеке баптау қажет емес.



3.7 сурет – WAP4410 N қатынау нүктесін пайдаланатын WLAN қарапайым желісі

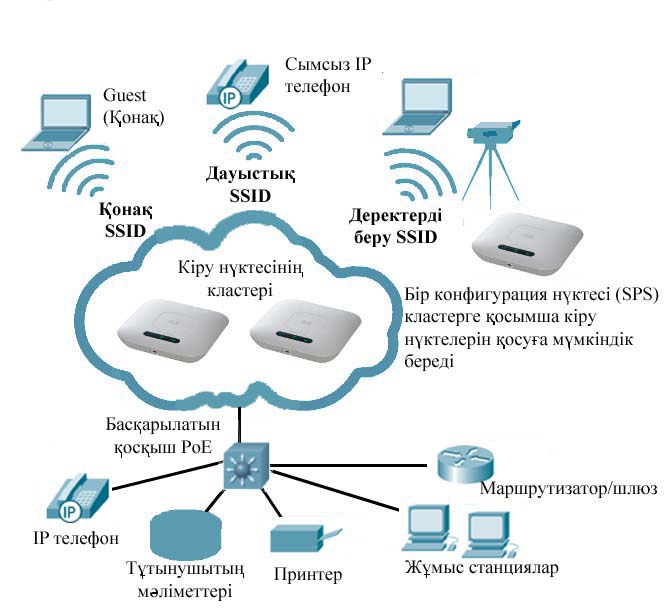
Жеке алғанда, WAP121 және WAP321 қатынау нүктелері баптаудың бірегей нүктесін қолдайды (Single Point Setup, SPS), бұл 3.8-суретте көрсетілгендей қатынау нүктесін жылдам және қарапайым жаймалауды қамтамасыз етеді. SPS - LAN желісі үшін WAP321қатынау нүктесінің сегіщ нүктесіне дейін, WAP121 төрт нүктесіне дейін масштабтау мүмкіндігін береді, бұл бизнес талаптарын өсуі немесе өзгеруі жағдайында қосымша пайдаланушыларды қамтуды және қолдауды қамтамасыз етеді. Cisco AP541N қатынау нүктесі кластерге қатынаудың 10-ға дейінгі нүктесін біріктіруге және бірнеше кластерлерді қолдауға қабілетті.

Кластерді қатынаудың екі нүктесін пайдалану арқылы құру мүмкіндігі бар. Ол үшін келесі шарттарды сақтау қажет:

* Қатынау нүктелерінде кластерлеу режімі қосылады.
* Кластерге енетін қатынау нүктелері кластердің бір атауына ие.
* Қатынау нүктелері желінің бір құрамына қосылған.
* Қатынау нүктелері радио байланыстың бір режімін пайдаланады (яғни, радиобайланыстың екі модулі 802.11n стандартына жатады).

*Үлкен сымсыз желілер үшін шешімдер*

Әлденеше қатынау нүктелерін кластерлеуді талап ететін компаниялар сенімді және ауқымды шешімдерді талап етеді. Қатынаудың үлкен нүктелерін пайдаланатын ірі компаниялар үшін Cisco контреллер негізінде Cisco Meraki басқаратын архитектурасын және Cisco Unified сымсыз желі архитектурасын қоса алғанда басқарылатын шешімдер ұсынады.



3.8 сурет - WAP321 қатынау нүктесін пайдаланатын WLAN қарапайым желісі

*Басқарылатын Cisco Meraki бұлтты архитектурасы*

Cisco Meraki бұлтты архитектурасы басқару үшін өзіндік шешім ұсынады, ол сымсыз желіні жаймалауды қарапайымдылайды. Осы архитектура арқасында 3.9-суретте көрсетілгендей бұлттағы контроллерден қатынау нүктелерін басқару бір орталықтан іске асырылады. Бұлттық желілер және басқару оверлейлік жүктемені әкімшілеу үшін қымбат және күрделі контреллермен бағдарламалық қамтуды пайдаланусыз бір орталықтан басқаруды, көрілімді және бақылауды қамтамасыз етеді.



3.9 сурет - Бұлтты басқару аясындағы сымсыз қатынау нүктесі

Бұл процесс шығындарды азайтуға және күрделілік деңгейін төмендетуге мүмкіндік береді. Контреллер Meraki қатынау нүктесіне басқару баптауын (мысалы, шағын бағдарламалық қамтуды жаңартуды), қауіпсіздік баптауын, сымсыз желілер баптауын және SSID идентификаторын береді.



**Ескерту**. Meraki бултты инфроқұрылымы арқылы тек қана басқарылатын деректер ағындары өтеді. Пайдаланушы трафигі Meraki деректерін өңдеу орталықтары арқылы өтпейді. Сөйтіп, егер Cisco Meraki бұлтқа қатынай алмаса, желі ақаусыз жұмыс істейді. Бұл пайдаланушылардың бұрынғыша аутентификациядан өтуін көрсетеді, желіаралық экран ережелері әрекет етеді, ал ал трафик ағындары толық жылдамдық сызығында беріледі. Тек басқару функциялары жұмыс істемейді (мысалы, есептер мен баптаулар құру құралддары).



Басқарылатын Cisco Meraki бұлтты архитектурасы үшін келесі құрауыштар талап етіледі:

* **Cisco бұлтты** басқарудың сымсыз қатынау нүктелері . Әртүрлі сымсыз желілер үшін түрлі үлгілер бар.
* **Meraki (MCC) бұлтты контроллері**. MCC контроллері Meraki сымсыз дербес желісі жүйесі үшін орталықтан басқару, оңтайландыру және мониторнинг функцияларын ұсынады.MCC — бұл сымсыз қатынау нүктелерін басқару үшін алуға және құруға қажет құрылғы емес. MCC, шындығында, желісі жұмысы туралы есеп мониторингін, оңтайландыруды және құруды тұрақты орындайтын бұлтты сервис.
* **Басқарудың Веб-панелі**. Meraki Dashboard басқарудың веб-панелі қашықталған баптау мен диагностиканы орындайды.

*Cisco Unified сымсыз желі архитектурасын бірыңғайлау*

Жекелеген МАС-адресін пайдаланатын Cisco Unified сымсыз желі архитектурасы үшін шешім WLAN (WLC) контроллерлер көмегі арқылы қатынау нүктелерін бақылауды және оснымен бірге Cisco Wireless Control Systems (WCS) сымсыз желісі бақылау жүйесі арқылы басқаруды іске асырады. Қатынаудың «Жеңіл» нүктелері WLAN контроллерімен деректерді алмасуды іске асырады, ол үшін Lightweight Access Control Point Protocol (LWAPP) хаттамасы қолданылады. Контроллер деректермен алмасу үшін қажетті барлық жоғарыкласты функцияларды қамтиды, ал қатынау нүктесі тек пакетті өңдейтін «саңылау» терминалы болып табылады.

Cisco Unified сымсыз желі архитектурасы келесі құрылғылардың болуын талап етеді:

* «Жеңіл» қатынау нүктелері. Cisco Aironet 1600, 2600 және 3600 моделдерінің сымсыз қатынау нүктелері тораптар үшін сенімді желілік қатынауды қамтамасыз етеді.
* Шағын және орта бизнес кәсіпорындары үшін контроллерлер.2500 сериялы Cisco сымсыз контроллерлері, Cisco сымсыз желі ауқымды контроллерлері немесе Cisco ISR G2 үшін Cisco сымсыз желі контроллерлері моделі деректерді сымсыз тарату мақсатында шағын немесе орта бизнес кәсіпорындары үшін базалық деңгейдің WLAN ұжымдық желісі жаймалау мүмкіндігін ұсынады.

Сондай**-**ақ, үлкен өнімділік мүмкіндіктері бар WLAN желісінің басқа контроллері де қол жетімді. Мысалы, Cisco 5760 сымсыз желі контроллерлері және 8500 сериялы Cisco контроллерлері сымсыз желілердің масштабталатын өнімділігін оңтайландыру, қауіпсіздігін қамтамасыз ету және басқаруды үнемдеу үшін әзірленген (мысалы, ғимараттар кешенінде ірі жаймалаумен байланыс оператор желілері).

*Деректерді сымсыз тарату антеннасы*

Ұжымдық класта қатынау нүктелерінің көпшілігінің толық жұмысы үшін сырт антенналарды пайдалану талап етіледі. Cisco корпорациясы 802.11 қатынау нүктелерімен пайдалану үшін анрайы антенналар әзірледі. Бұл антенналар физикалық орналасумен, қашықтық пен эстетикалық талғамдармен қоса, жаймалаудың өзіндік ерекшеліктеріне бейімделуге қабілетті.

Cisco Aironet қатынау нүктелерін келесілер пайдалана алады:

* Wi-Fi барлық бағытты антеннасы. Wi-Fi зауыттық модулі көбіне базалық дипольды базалық антенналарды пайдаланады, бұлар шағын рацияларда пайдаланатындарға ұқсас икемді қадалықты жылжымалы антенналар деп аталады. Барлық бағытты антенналар 360 градус аумақты қамтамасыз етеді және ашық алаңдарға, вестибюльдерге, конференц-залдарға және сыртқы алаңдарға өте ыңғайлы.
* Wi-Fi бағытталған антенналары. Бағытталған антенналар радио сигналды берілген бағытта фокустайды. Сөйтіп, қатынау нүктесінде сигнал жақсарады және антенна бағытталған бағытқа да жақсы жетеді, бұл бір бағытта үлкен және барлық басқа бағытта кіші сигнал қуатын қамтамасыз етеді.
* «Толқынды арна» (Yagi) типті антенналары – бұл алыс әрекетті Wi-Fi желісін құру үшін қолдануға болатын әрекетке бағытталған радиоантенналар. Әдетте, бұл антенналар қосымша құрылысқа қатынауды қамтамасыз ету үшін немесе ғимараттан тыс белгілі бағытта «ыстық нүктелер» диапазонын кеңейту үшін пайдаланылады.

Қатынаудың өту қабілетін арттыру үшін IEEE 802.11n/ac/ad МІМО технологиясын пайдаланады. Жеке алғанда MIMO технологиясын деректердің үлкен көлемін тарату үшін бірнеше антенналарда пайдаланады, бұл бір антеннаны пайдалану үшін жағдай ажсайды. Өту қабілетін ұлғайту үшін төрт антеннаға дейін пайдалануға болады.



**Ескерту**. Сымсыз маршрутизаторлардың барлығы бірдей емес. Мысалы, бастапқы деңгейдегі 802.11n маршрутизаторы бір модульді Wi-Fi желісін және құрылғыға жалғанған бір антеннаны қолдана отырып, 150 Мбит/с өту қабілетін қолдайды. 802.11n маршрутизаторына деректерді таратудың жоғары жылдамдығын қамтамасыз ету үшін көп радио модульдер және деректерді тарату арналарының үлкен санын паралельді басқару үшін көп антенналар талап етіледі. Мысалы, 802.11n маршрутизаторында екі радиомодуль мен екі антенна 300 Мбит/с дейінгі деректерді тарату жылдамдығын қолдайды, ал 450 және 600 Мбит/с жылдамдықты қамтамасыз ету үшін үш және төрт радиомодуль мен сәйкесті антенналар талап етіледі.



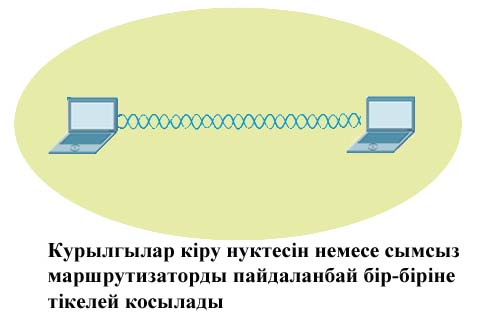
3.1.5 WLAN 802.11 желілерінің топологиясы

*802.11 сымсыз желісі топологиясының режімі*

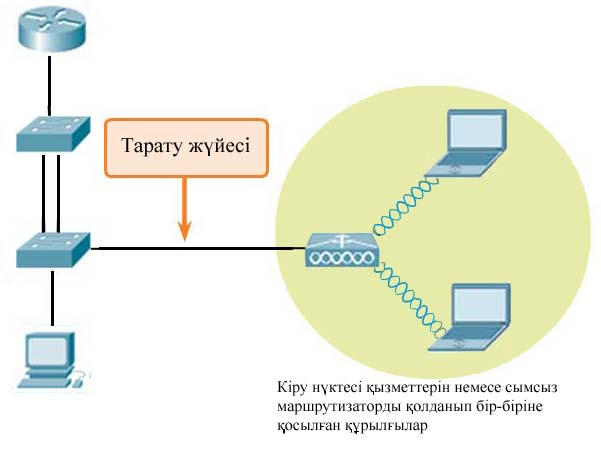
LAN сымсыз желісі желілердің түрлі топологиясын пайдалануы мүмкін. 802.11 стандарты сымсыз желі топологиясының негізгі екі режімін анықтайды:

* Тікелей қосылу режімі (ad hoc). Бұл режімде екі құрылғы сымсыз маршрутизатор немесе қатынау нүктесі түріндегі инфроқұрылым құрылғыларын пайдаланусыз сымсыз желілер бойынша қосылған. Бұл режімге мысал ретінде Bluetooth және Wi-Fi Direct айтуға болады.
* Инфрақұрылымды режім. Бұл режімде сымсыз клиенттер бір бірімен сымсыз маршрутизатор немесе қатынау нүктесі (мысалы, WLAN желісі) арқылы қосылған. Қатынау нүктесі желілік инфрақұрылымға кабельді тарату жүйелері арқылы қосылған, мысалы Ethernet.

3.10-суретте тікелей қосылу режімі көрсетілген, ал 3.11-суретте инфроқұрылымды режім мысалы ұсынылған.



3.10 сурет - Тікелей қосылу режімі



3.11 сурет – Инфроқұрылымдын режімы

*Тікелей қосылу режімі*

Тікелей қосылысты сымсыз желі сымсыз маршрутизаторды немесе қатынау нүктелерін пайдаланусыз бір рангты желілердегі екі сымсыз құрылғылар арасындағы деректермен алмасуды білдіреді. Мысалы, клиенттік жұмыс стансасын тікелей қосылу режіміндегі жұмысы үшін сымсыз байланыс қолдауымен баптауға болады, бұл оған басқа құрылғыларды қосу мүмкіндігін қамтамасыз етеді. Тікелей қосылу режімі мысалына Bluetooth және Wi-Fi Direct жатқызуға болады.

IEEE 802.11стандары шеңберінде тікелей қосылысты желілер сервистердің тәуелсіз базалық жиыны (IBSS) болып есептеледі.

Сымсыз дербес қатынау нүктесін жасау үшін ұялы байланыс арқылы деректерді таратуға смартфонмен немесе планшетті компьютермен қосылу шеңберінде бір рангты топология нұсқасы бар. Бұл функция модем режімі деп аталады. Әдетте, сымсыз қатынау нүктесі қысқа мерзімді шешім болып табылады, осы себепті смартфон сымсыз байланыс Wi-Fi-маршрутизаторының сервисін қамтамасыз ете алады. Ал басқа құрылғылар интернет желісіне қатынау үшін смартфонда немесе планшетті компьютерде аутентификациямен және біріугімен орындай алады. Apple iPhone-да бұл функция «Сымсыз қатынаудың дербес нүктесі» деп аталады, ал Android құрылғыларында – «Модем режімі» немесе «Қатынаудың шағын нүктесі» деп аталады.

*Инфрақұрылымдық режім*

IEEE 802.11 архитектурасы бірнеше құраушылардан тұрады, олар клиенттерді қолдауды қамтамасыз ететін WLAN желісін ұсыну үшін өзара жұмыс істейді. Бұл инфрақұрылымдық режім топологиясының екі құрылымдық элементін анықтайды: сервистердің базалық жиынтығы (BSS) және сервистердің кеңейтілген жиынтығы (ESS).

**Сервистердің базалық жиынтығы**

BSS қатынаудың бір нүктесінен тұрады, олар бәрімен байланысты сымсыз клиенттермен жұмыс істейді. Дөңгелектермен қамту зонасы белгіленген, оның шегінде BSS сымсыз клиенттері бір-бірімен байланыс жасай алады. Бұл зона негізгі қызмет көрсету (BSA) зонасы деп аталады. Егер сымсыз клиент қызмет көрсетудің негізгі зонасынан шықса, онда ол BSA зонасы шегінде басқа сымсыз құрылғылармен тікелей байланыса алмайды. BSS топологияның құрылымдық элементі, ал BSA — нақты қамту зонасы болып табылады (BSA және BSS терминдері көбіне өзара алмастырушы ретінде пайдаланылады).

2-деңгейдегі МАС-адресі BSS әр жиынтығының бірегей сәйкестендіруі үшін қолданылады, ол сервистердің базалық жиынтығының идентификаторы (BSSID) деп аталады. Сонымен, BSSID идентификаторы BSS формальды атауы болып табылады және әрқашан тек қана қатынаудың бір нүктесімен байланысады.

**Сервистердің кеңейтілген жиынтығы**

BSS-тің бір жиынтығы радиожиіліктік қамтуды жеткіліксіз қамтамасыз еткенде, онда жалпы тарату жүйесінің көмегімен BSS жиынтығының екі немесе одан көбімен байланыстыруға болады, бұл сервистердің (ESS) кеңейтілген жиынтығын түзейді. Мұнда енді сымсыз клиенттер BSA бір зонасында ESS бір жиынтығы шегінде BSA басқа зонасының сымсыз клиенттерімен деректерді алмастыра алады. Роумингтегі ауысатын ұтқыр сымсыз клиенттер BSA бір зонасынан екіншісіне ауыса алады (жиынтығы бұрынғыша ESS) және қосуда проблемасыз орындайды.

Тік бұрышты саламен қамту зонасы белгіленген, оның шектерінде ESS жиынтығының қатысушылары деректермен алмаса алады. Бұл сала кеңейтілген қызмет көрсету зонасы (ESA) деп аталады. Әдетте ESA өзара қиысатын жән/немесе жекелеген конфигурацияларда бірнеше BSS жиынтығынан тұрады.

Әрбір ESS SSID идентификаторымен, ал әр BSS ESS-те BSSID идентификаторымен анықталады. Қауіпсіздік жағдайларына байланысты қосымша SSID идентификаторлары желіге қатынау деңгейінен бөліну үшін ESS-те толтырылуы мүмкін.

802.11 стандарты шеңберінде тікелей қосылу режімі IBSS деп аталады.

3.1.6 Сымсыз жергілікті желінің жұмыс принциптері

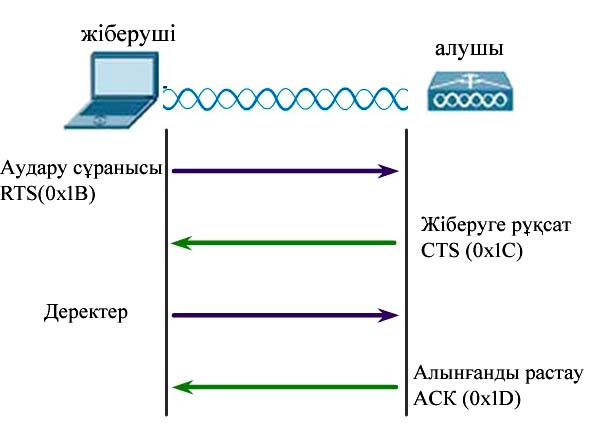
*Қақтығыстарды болдырмау және ағымдағыны бақылау мен көптік бақылау*

Ортада шиеленісті шешу әдісі егер желі бойынша трафикті жіберу талап етілсе, бұл жағдайда ортаға қатынасу уақыты мен әдістері құрылғыларын анықтау болып табылатынын еске сақтау керек. WLAN IEEE 802.11 желісі MAC CSMA/CA хаттамасын пайдаланады. Оның атауы Ethernet CSMA/CD ұқсас болса да әрекет ету приницпі тіпті өзгеше.

Wi-Fi жүйелері жартылай дуплексті режімде жұмыс істейді және ортаның жалпы конфигурациясын құрайды, демек сымсыз клиенттер бір радио арна бойынша деректерді қабылдайды және жібере алады. Осы себепті проблемалар туындайды, себебі сымсыз клиент тжөнелту процесінде деректерді алмайды. Сөйтіп, қақтығыстарды табу мүмкін болмайды. Бұл проблеманы шешу үшін электротехника және электроника бойынша инженерлер институты (ІЕЕЕ) қақтығыстарды болдырмаудың қосымша тетігін әзірледі. Ол бөлінген координация функциясы ретінде танымал (DCF). Сымсыз клиент DCF көмегімен деректерді тек қана өзінің бос арнасы арқылы таратады. Таратудың барлық операцияларының деректері бекітіледі. Демек, егер сымсыз клиент бекітуді алмаса, ол қақтығыстардың болғанын сезеді және ерікті күту интервалы бойынша әрекет жасайды.

Сымсыз клиенттер және қатынау нүктелері деректерді нақты таратуын қарапайымдылау үшін RTS және CTS бақылау кадрларын пайдаланады.

3.12-суретте көрсетілгендей деректерді жөнелтуде сымсыз клиент алдымен басқа құрылғылар мен деректерді тарату операцияларының белсенділігін анықтау үшін ортаны сканерлейді. Егер мұндай операциялар байқалмаса, сымсыз клиент қатынау нүктесіне RTS кадрын жібереді. Бұл кадр көрсетілген кезеңде радиожиіліктер тасымалы үшін бөлінген қатынаудың сұранысын жіберу үшін пайдаланылады. Қатынау нүктесі кадрды қабылдайды және мүмкіндігінше сымсыз клиентке СTS кадрын сондай ұзақықпен жіберу жолымен радиоиіліктер тасымалына қатынауды ұсынады. Қалған барлық сымсыз құрылғылар осы CTS кадрын көреді, таратқыш тораптан деректерді жіберу үшін ортаны босатады.



3.12 сурет - Деректерді тарату үшін бақылау кадрларын пайдалану

CTS бақылау кадры ұзақтық туралы деректерден тұрады, оларды тарату торабынан жіберуге рұқсат етілген. Қалған сымсыз клиенттер осы кезеңнен кем емес жағдайда таратуды бөгейді.

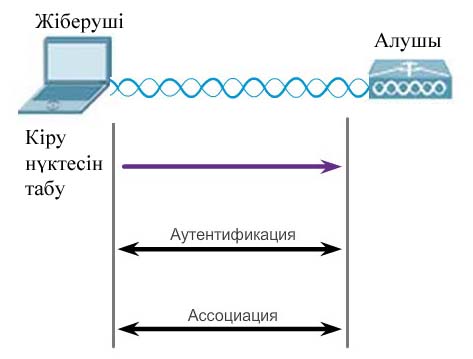
*Сымсыз клиенттердің қатынау нүктесінің Ассоциациясы*

Сымсыз құрылғылар желі бойынша деректермен алмасуды іске асыру үшін алдымен оларға қатынау нүктесінен немесе сымсыз маршрутизатормен ассоциацияны орындау қажет. 802.11 процесімен маңызды кезеңі WLAN желісін табу және оған одан әрі қосылу болып табылады.

Басқару кадрлары үш кезеңнен тұратын келесі процесті орындау үшін сымсыз құрылғыларды пайдаланады:

* Сымсыз қатынаудың жаңа нүктесін анықтау.
* Қатынау нүктесіндегі аутентификация.
* Қатынау нүктесіндегі ассоциация

Қатынау нүктесі және сымсыз клиент ассоциацияны орындай үшін ерекше параметрлерді келісуі қажет. осы процестердің келісімін шешу үшін осы параметрлерді қатынау нүктесіне одан кейін клиентке баптау қажет.



3.13 сурет – Үш кезеңді процесс

*Ассоциация параметрлері*

Сымсыз желінің жалпы бапталатан параметрлері:

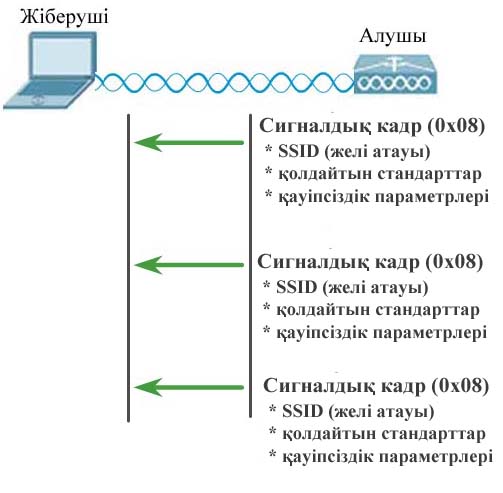
* SSID Идентификаторы – SSID идентификаторы сымсыз клиент сымсыз желілерді бір зонада ажырату үшін қолданатын ерекше идентификатор. SSID атауы клиентте қол жетімді сымсыз желілер тізімінде бейнеленеді. SSID идентификаторы желінің конфигурациясына байланысты желіге қатынаудың бірнеше нүктелерімен бірге пайдаланылуы мүмкін. Көбіне атау ұзындығы 2 – 32 символдарды құрайды.
* Пароль – қатынау нүктесінде аутентификациялау үшін сымсыз клиентке міндетті түрде ұсынылады. Кейде парольді қауіпсіздік кілті деп атайды. Пароль сымсыз желіге қажетсіз пайдаланушылар мен қаскүнемдердің қатынауын болдырмайды.
* Желілік режім (Network mode) – WLAN 802.11a/b/g/n/ac/ad желісінің стандартына жатады. Қатынау нүктесі және сымсыз маршрутизаторлар аралас режімде жұмыс істей алады, яғни олар бір уақытта бірнеше стандартты пайдалануы мүмкін.
* Қауіпсіздік режімі (Security mode) – бұл термин қауіпсіздік параметрлерін баптауына жатады (WEP, WPA немесе WPA2). Әрқашан қауіпсіздік қатынау деңгейлерінің ең жоғарғы белсенділігін қамту қажет.
* Арнаны баптау (Channel settings) – сымисыз деректерді тарату үшін пайдаланылатын жиілікті жолақтарға жатады. Сымсыз маршрутизаторлар және қатынау нүктесі арнаның баптауын таңдауы мүмкін. Сондай-ақ, басқа қатынау нүктесінің немесе сымсыз құрылғының тарапынан бөгеу болған жағдайда бұл баптауларды қолмен орындауға болады.

*Қатынау нүктелерін табу*

Сымсыз құрылғылар сымсыз маршрутизаторға немесе қатынау нүктесіне қосуды және табуды орындауы қажет. Сымсыз клиенттер қатынау нүктесіне сканерлеу процесін (іздеу) пайдалана отырып, қатынайды. Бұл процесс келесі режімдерде орындалуы мүмкін:

* Пассив режім (Passive mode) – қатынау нүктесі қауіпсіздік баптау және қолданылатын стандарттар туралы мәліметтерді SSID атауынан тұратын кең таратылымды жіберілімдер сигнал кадрларын тұрақты жөнелту жолымен өз қызметін ашық көрсетеді. Сигналдың негізгі міндеті – қатынау нүктесін және қажет желіні таңдау үшін осы зонада қатынаудың желілері мен нүктелері туралы деректерді сымсыз клиенттерге алуға рұқсат етеді.
* Актив режім (Active mode) – сымсыз клиенттер SSID атауын білуі қажет. Сымсыз клиент бірнеше ағзаларға ізденіс сұраныс кадрын кең хабармен жөнелту бойынша процесті жүргізеді. Ізденіс сұранысы SSID атынан және қолдайтын стандарттар туралы мәліметтерден тұрады. Активті режім сигнал кадрларын кең тарату жолымен тыйымға бапталған қатынау нүктесі немесе сымсыз маршрутизаторы үшін қажет болады.

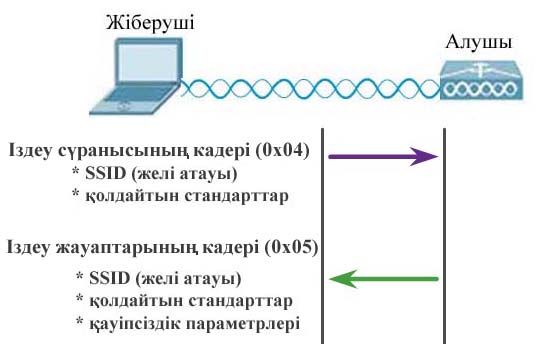
3.14-суретте пассивті желінің кезең кезеңімен кең хабар жіберу арқылы сигнал кадрына қатынау нүктесінің жұмысы көрсетілген.



3.14 сурет – Клиент құрылғылары қатынау нүктесін тыңдайды

3.15-суретте кең тарату жолымен нақты SSID ізденіс сұранысын беретін сымсыз клиентпен актив режімнің қалай жұмыс істейтінін көрсетілген. Ізденіс бойынша кадр жауабына SSID қатынау нүктесін жібереді.

Бұдан басқа, сымсыз клиент WLAN жақын желілерін табу үшін SSID атауынан, тұрмайтын ізденіс сұранысын жібере алады. Сигнал кадрларын кең тарату үшін бапталған қатынау нүктелері сымсыз клиентке SSID атауы көрсетілген және ізденіс бойынша жауаптан тұратын жауап жібереді. Кең тарату бойынша SSID тарату компоненті өшіріліп тұрса қатынау нүктесі жауап бермейді.



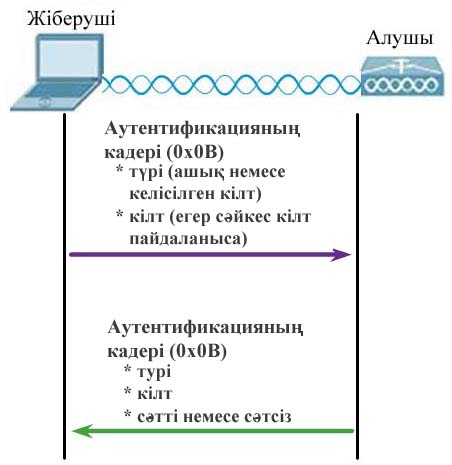
3.15 сурет – Қатынау нүктесі кезеңділікпен сигнал кадрларының кең таратылуын орындайды

*Аутентификация*

802.11 стандарты бастапқыда аутентификацияның екі механизмін ескере отырып, әзірленген:

* Ашық аутентификация – сымсыз клиент аутентификация сұранысын жіберетін және қатынау нүктесі растау жауабыныа жіберетін шеңберінде негізгі NULL аутентификациясы. Ашық аутентификация кез келген сымсыз құрылғы үшін сымсыз желіге қосылуды қамтамасыз етеді. Аутентификацияның бұл әдісін қауіпсіздік онша үлкен мәнде болмағанда пайдаланылады.
* Келісілген кілт аутентификациясы – бұл технология қатынау нүктесімен және клиентпен алдын ала келісілген кілтті пайдалануды айғақтайды.

3.16-суретте аутентификация амалының қысқаша жазбасы ұсынылған.



3.16 сурет – Клиент және қатынау нүктесінің аутентификациясы

Келісілген кілт пайдаланылатын жүйелердің көршілігінде деректермен алмасу келесі түрде орындалады:

1. Сымсыз клиент қатынау нүктесіне аутентификация кадрын жібереді;

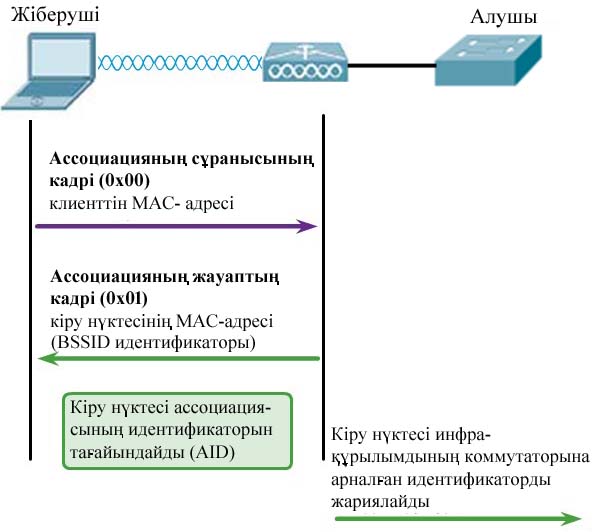
2. Қатынау нүктесі сұранысқа бақылау мәтінін жібереді.

3. Клиент келісілген кілтті пайдалана отырып, хабарламаны шифрлеуді орындайды және шифрленген мәтінді кері қатынау нүктесіне жібереді.

4. Осыдан кейін қатынау нүктесі өзінің келісілген кілтін пайдаланып, мәтіннің шифрін ашады.

5. Егер шифрленген мәтін бақылау мәтінімен сай келсе, онда қатынау нүктесі клиентті аутентификациялайды. Егер хабарламалар сәйкес келмесе, сымсыз клиент аутентификациядан өтпейді және сымсыз қатынауға ие болмайды.

Сымсыз клиент қатынау нүктесінің аутентификациясынан өткенннен кейін ассоциация кезеңінен ауысады. 3.17-суретте көрсетілгендей, ассоциация кезеңінде параметрлердің соңғы баптауы орындалады және қатынау нүктесі мен сымсыз клиент арасындағы деректерді тарату арнасы тағайындалады.



3.17 сурет – Қатынау нүктесінен клиентті ассоциациялау

Бұл кезеңде:

* Сымсыз клиент ассоциацияның сұраныс кадрын қайта жібереді, ол МАС-адерісінен тұрады.
* Қатынау нүктесі қатынау нүктесінің МАС-адресі болып табылатын, қатынау нүктесінің BSSID нүктесінен тұратын ассоциация бойынша сұранысқа жауап жібереді.
* Қатынау нүктесі сымсыз клиентпен ассоциация (AID) индентификаторы ретінде белгілі логикалық порттан тұрады. AID идентификаторы коммутатор портына тең мәнді және ол жөнелту үшін сымсыз клиентке жолданатын кадрлардың инфрақұрылымын коммутаторда байқауға мүмкіндік жасайды.

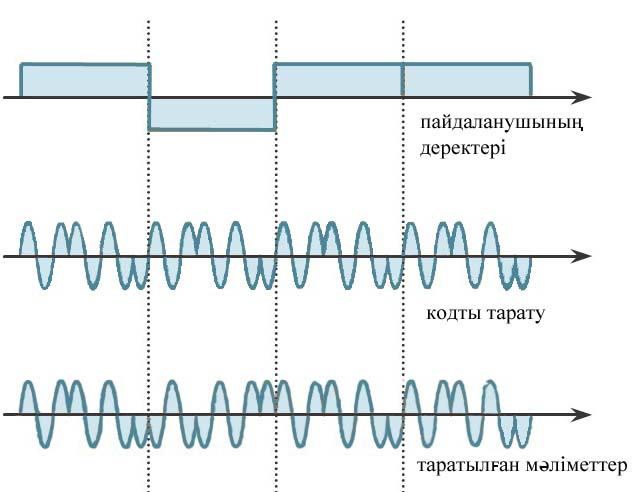
Сымсыз клиентті қатынау нүктесінен ассоциациялаудан кейін олардың арасында трафик берілуі мүмкін.

Арналарды басқару. Жиілікті арнаны қанықтыру

Алдында түсіндірілгендей LAN сымсыз желі құрылғылары деректермен алмасу үшін радиотолқындардың белгілі жиіліктеріне бапталған таратқыштар мен қабылдағыштардан тұрады. Әдетте диапазондар сапасы ретінде жиіліктер ерекшеленеді. Мұндай диапазондар содан кейін кіші диапазон-арналарына бөлінеді.

Егер нақты арнаға сұраныс өте үлкен болса, онда ол арна көбіне артық қаныққан болып есептеледі. Сымсыз желінің артық қаныққан ортасы деректермен алмасу сапасын төмендетеді. Соңғы жылдары деректермен алмасу сапасын жақсартататын және артық қанығуды азайтатын арнаулы қабылдағыштар әзірленді. Төменде санамаланған әдістер оларды тиімді пайдалану арқылы арналардың қанығуын азайтуға мүмкіндік жасайды.

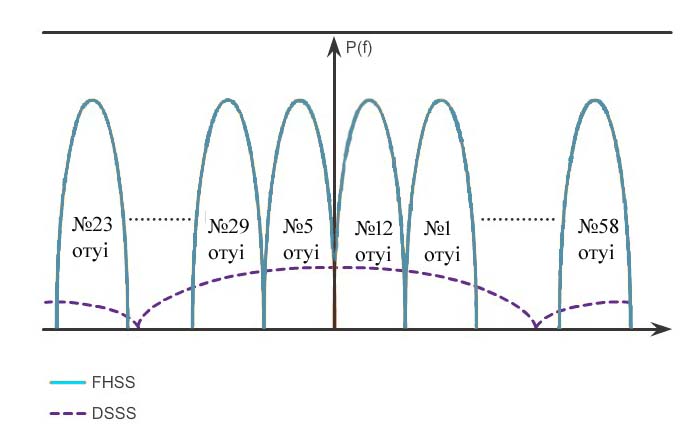
Тікелей тізбектелуде сигналды бөлу (Direct-sequence spread spectrum, DSSS) **–** DSSS сигналды бөлу модуляциясы технологиясын ұсынады. Спектрді бөлу технологиясы үлкен жиілік жолағы бойынша сигналды тарату мақсатында әзірленген, ол оның бөгеуілдерге тұрақтылығын арттырады. DSSS технологиясы көмегімен сигнал «жасанды жасалған шу» мәніне көбейеді, сондай-ақ ол спектрді кеңейту коды деп аталады. Алушыға спектрді кеңейту коды белгілі болғандықтан, ол математикалық түрде оның қосуларын шығара алады және қайтадан шығыс сигналын түзуге мүмкіндік береді. Нақтысында бұл сымсыз желі ортасының сапасының төмендеуін болдырмауды қамтамасыз етеді. DSSS технологиясы 802.11b стандартымен, сондай-ақ ол 900 МГц, 2,4 ГГц, 5,8 ГГц ұялы CDMA және GPS желілер жиілігінде жұмыс істейтін радиотелефондарда пайдаланылады (3.18-сурет).



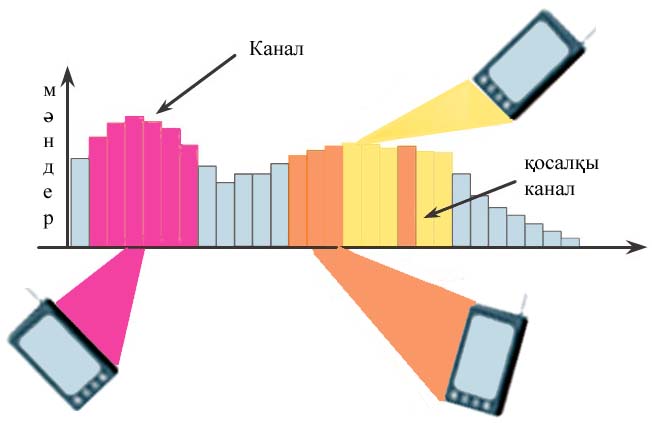
3.18 сурет – DSSS мысалы

Кеңейтілген спектрі бар жұмыс жиілігін секірмелі түрде ауыстыру (Frequency-hopping spread spectrum, FHSS**) –** деректермен алмасу үшін спектрді тарату әдісі қолданылады. Бұл технология DSSS-ке ұқсас, бірақ арналар жиіліктерінң көпшілігі бойыншажиілікті сигналдарды тез комутациялау арқылы радиосигналдарды жібереді. FHSS пайдалануда жіберуші және алушы синхрондалуы тиіс, бұл қай арнаға ауысуды білу үшін қажет. арналар арасындағы сигналдың өтуінің бұл процесі арналарды тиімдірек пайдалануды қамтамасыз етеді және олардың артық жүктемесін төмендетеді. 900 МГц жиілікте жұмыс істейтін шағын рациялар мен радиотелефондарда FHSS пайдаланады, ал сол уақытта Bluetooth сияқтылар бұл технологияны вариациялау нұсқаларының бірін ұстанады. Бұдан басқа, FHSS технологиясы 802.11. шығыс стандартын қолданады (3.19 сурет).

Жиіліктерді ортогоналдық бөлумен мультиплексирлеу (Orthogonal frequency-division multiplexing, OFDM) **–** жиіліктіреді бөлудің мультиплексирленген түрі, мұның деңгейінде жақын жиіліктерде бір арна бірнеше арнашаларды пайдаланады. OFDM жүйесіндегі арнашалар бір-біріне қатысты дәл ортогоналды, бұл арнашаларға өзара кедергісіз жұмыс істеуге мүмкіндік береді. Соның нәтижесінде OFDM жүйесі аралас арналарда кедергісіз спектр тиімділігін максималды үлкейтуге мүмкіндік береді. Негізінде бұл технология қабылдаушы стансаға сигналды «естуге» мүмкіндік жасайды. OFDM арнашаларды пайдаланатындықтан ол арнаны мейлінше тиімді етеді. ОFDM, 802.11a/g/n/ac стандартымен қоса, байланыстың бірнеше жүйелерін пайдаланады (3.20 -сурет).



3.19 сурет - FHSS мысалы



3.20 сурет – ОFDM мысалы

*WLAN жаймалауды жоспарлау*

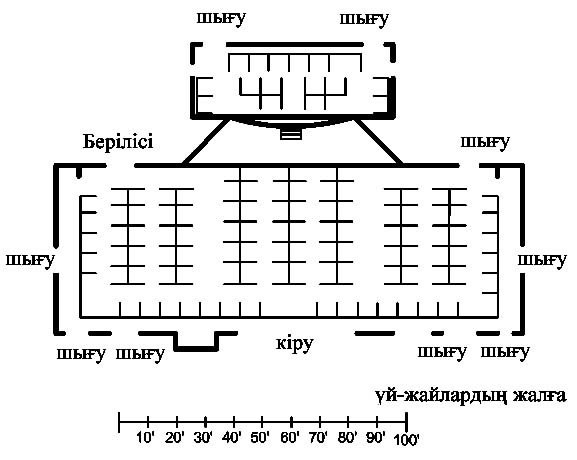
Жоғары сапалы қызмет көрсетуді қамтамасыз ететін және ресурстарды өте тиімді пайдаланатын WLAN желісін іске асыру тыңғылықты жоспарлауды талап етеді. WLAN желілерінің салыстырмалы қарапайымнан өте күрделіге дейінгі модельдері бар. Сымсыз желіні орындау алдында тыңғылықты жоспар жасаған дұрыс.

WLAN желісін қолдайтын пайдаланушылар саны айтарлықтай күрделі сұлба бойынша есептеледі. Пайдаланушылар саны нысандағы қатынау кеңістігіне, олар қуатты тарату баптауларымен ESS-ке қатынаудың бірнеше нүктелері мен үзілмейтін арналарды пайдалануда күтілетін деректерді тарату жылдамдығын орналастыратын құрылғылар санына тәуелді.

3.21-суреттегі қабаттық жоспарды қараңыз.

Қатынау нүктелерін орналастыруды жоспарлауда әкімшілікке қамту зонасын қарапайым шеңберлермен белгілеу және оларды жоспарда орналастыру жеткіліксіз болады. ұсынылған шеңберлік қамту зоналары өте маңызды, бірақ оған қосатын ұсыныстар қатары бар:

* Егер қатынау нүктелері қолданыстағы кабельдік жүйелерді пайдалану қажет болса немесе орналастырулары көрсетілсе, мұнда қатынау нүктесін орналастыруға болмайдыі яғни бұл орындарды картада белгілеу қажет;
* Қатынау нүктелерін физикалық бөгеуілдерден жоғары орналастырған дұрыс;
* Мүмкіндігінше қатынау нүктелерін әр зонаның орталығында төбемен қатар тік орнатады;
* Пайдаланушылар болатын орындарда AP орнатылады. Мысалы, әдетте қатынау нүктелерін орналастыру үшін дәлізге қарағанда конференц-зал қолайлы болады.

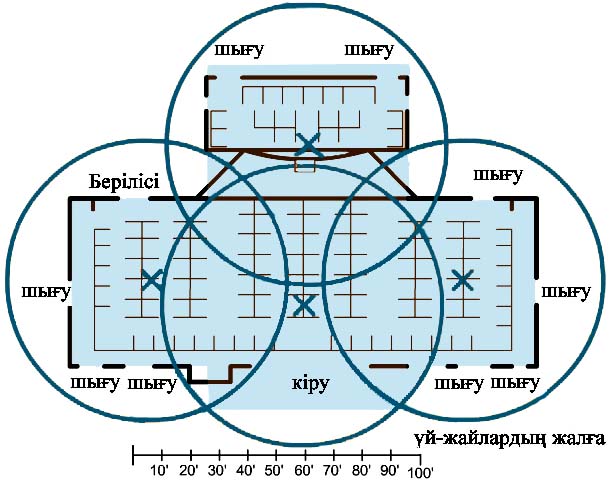


3.21 сурет – Қабаттық жоспар мысалы

Көрсетілген мәселелер шешілгеннен кейін қатынау нүктелерінің болжалдық қамту зонасын бағалау қажет. Бұл мән қатынау нүктесі үшін бапталған тарату қуаты, нысан сипаты, жаймалауға жататын WLAN желісі стандарттарын комбинациялау немесе стандарттау және көптеген басқа факторларда үлкен мәнге ие болады. Қамту зонасы жоспарын әзірлеуде пайдаланылатын қатынау нүктелерінің ерекшелігін тереңірек зерттеу қажет.

BSA қамту зонасы бір арнаны қамтамасыз ететін өздік қамту зонасын ұсынады. Кеңейтілген сервис жиынтығы (ESS) BSA қамту зоналары арасында ESS шектерінде 10–15% қамтуы қажет. BSA-ны SSID идентификаторымен және үзілмейтін арналармен (яғни, 1 арнада бір ұяшық, ал басқасы 6 арнада) 15% қамтуда роуминг мүмкіндігін жасауға болады.

3.22-суретте BSA қамту зонасы мүмкіндігінің мысалы көрсетілген.



3.22 сурет – BSA қамту зонасы

Басқа факторларға қатынау нүктесінің түрлі орналасу мүмкіндігін нақты айғақтайтын нысанды зерттеу жатады.

3.1.7 Сымсыз жергілікті желілер қауіпсіздігі

*WLAN желілерінің қауіптері*

Сымды желіні қорғауға қарағанда, сымсыз желінің қауіпсіздігін қамтамасыз ету тым күрделірек. Кімде кім әкімшілік желілерін пайдаланатын болса, барлығы үшін бірінші орында қорғаныс тұруы қажет.

WLAN желісінің қатынау нүктесінің әрекет ету аумағы қатынау нүктесінің ассоциациясын орындау арқылы сәйкесті есептік деректерге ие болатындардың барлығы үшін ашық. Қаскүнем сымсыз адаптер желісін және бұзу әдістерін біле отырып, WLAN желісі бар қатынау орнынан басқа жерде де оған қатынай алады.

Қауіпсіздік мәселелері күн өткен сайын үлкен мәнге ие болуда, себебі компанияның қызме әрекеті оның деректерінің қорғалуына тәуелді. Компаниялар үшін қауіпсіз жүйесінің бұзылуы апатты салдарға ұрындырады. Әсіресе өз клиенттерінің қаржы ақпаратының сақталуы алға тартылады. Сымсыз желілер көбіне кәсіпорындарда орналастырылады және көп жағдайларда тек тиімді нұсқа болып қоймай, өте маңызды сыни бөлігі де болып табылады. WLAN желілері үнемі шабуылға ұрынады, өйткені бұл желінің қолданылуы бірінші орында. Ал шабуылдар бөтен адамдармен немесе риза емес өз қызметкерлерімен, сондай-ақ қасақана жасалған кез келген қызметкермен ұйымдастырылуы мүмкін. Сымсыз желілер көбіне келесі қатерлерге ұшырайды:

* Сымсыз қаскүнемдер;
* Зиян шектіретін қосымшалар;
* Деректерді қолға түсіру;
* DoS шабуылы.

Бұл тарауда қатынау нүктесінің немесе сымсыз клиенттің МАС-адресі спуфингі ретіндегі қатерлер құрылымға шабуылдар және бұзулар қарастырылмайды.

*«Қызмет көрсетуден бас тарту» типіндегі шабуыл*

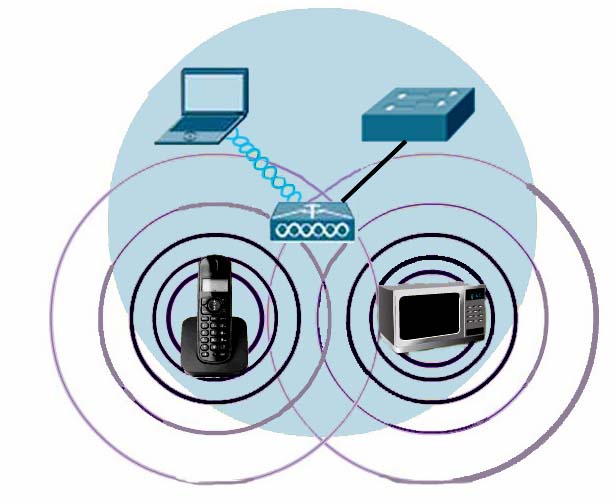
Төменде сымсыз желіде туындайтын DoS-шабуылдарының себептері келтірілген:

* Құрылғыларды теріс баптау – WLAN желісінің тоқтау себебі конфигурация қателігінен болуы мүмкін. Мысалы, әкімші кездейсоқ конфигурацияны өзгертеді және желіні өшіреді, немесе әкімші құқы бар қаскүнем әдейі WLAN желісін өшіруі мүмкін.
* Сымсыз желі бойынша деректер алмасуға әдейі кедергі келтіретін қаскүнем – мұндай қаскүнемдер желіні толық немесе белгілі бір дәрежеде ажыратуға ұмтылады, бұл жағдайда құрылғылар ортаға қатынай алмайды.
* Кездейсоқ бөгеуілдер – WLANжелісі лицензияланбаған, жиілік жолақтарда жұмыс істейді, чғни барлық сымсыз желілер қауіпсіздік функциясына тәуелсіз басқа сымсыз құрылғылардың тарапынан бөгеуілдер әсеріне ұшырауы мүмкін. Кездейсоқ бөгеуілдер мынандай құрылғылар жұмысында микротолқынды пештер, радиотелефонда, радио-нянялар т.б. болуы мүмкін. 2,4 ГГц жолағы 5 ГГц-ке қарағанда бөгеуіл әсеріне көбірек ұшырайды.

Зиянды шабуылдармен құрылғыларды тез баптау салдарынан DoS-шабуылдарының қатерін азайтуға болады, ол үшін барлық құрылғылар қорғанысын сақтауды, парольдерді сенімді орындарға қоюды, резервтік көшірмелер жасауды және конфигурацияны жұмыстан кейінгі сағаттарда өзгертуді қамтамасыз ету қажет.

Кездейсоқ бөгеуілдер тек қана басқа сымсыз құрылғылардың жұмыс жағдайында туындайды. Мұндай проблемаларды шешу және бөгеуілдерді болдырмау WLAN желісінің мониторингісінің оңтайлы шешімі болып табылады. себебі, 2,4 ГГц жолағы көп дәрежеде бөгеуіл әсеріне ұшырайды, ал нашар зоналарда 5 ГГц жолағын пайдалануға болады. WLAN желілері үшін кейбір шешімдер қатынау нүктелері арналарын автоматты реттеумен жасалады және бөгеуілдерді болдырмау үшін 5 ГГц жолақты пайдалануға мүмкіндік жасайды. Мысалы, 802.11n/ac/ad стандартының кейбір шешімі бөгеуілдерге қарсылық жасау мақсатында автоматты түрде реттеледі.

Төмендегі 3.23 суретте WLAN желісінің алмасу деректері үшін бөгеуілдер жасауы мүмкін радиотелефон мен микротолқынды пеш көрсетілген.



3.23 сурет – Кездейсоқ бөгеуілдер

Cisco CleanAir технологиясы 802.11 стандартына жатпайтын бөгеуілдер көздерін табуға және анықтауға мүмкіндік береді. Бұл технология өзгерген ортаға автоматты бейімделетін желі жасайды.

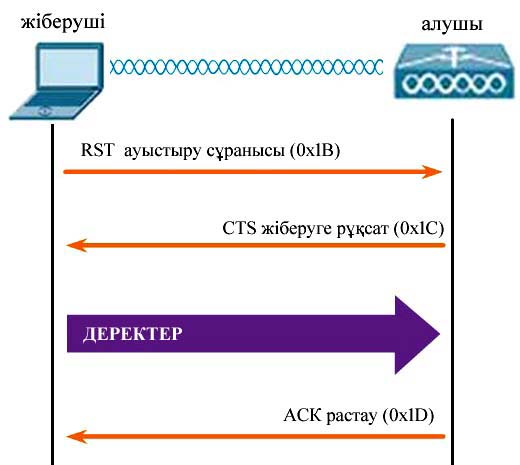
*Басқару кадрлары пайдаланылатын DoS- шабуылдары*

Бұл онша сенімді болмаса да қаскүнемдер кездейсоқ бөгеуіл жасайтын радиоэлектронды қарсы әрекет құрылғысын пайдалана отырып, әдейі DoS-шабуылын жасауы мүмкін. Қаскүнемдер басқару кадрларын пайдалануға тырысады, сөйтіп қатынау нүктелері, арналар пайдалану трафигін станциялайтын қызмет ете алмау үшін бүлдірулер жасайды.

Басқару кадрларын DoS-шабуылының әртүрлі типтерін ұйымдастыру үшін .пайдалануы мүмкін. Басқару кадрларын пайдалану жолымен шабуыл жасаудың екі түрі таралған.

* Жалған өшіру жолымен шабуыл – мұндай шабуыл жасау үшін қаскүнем «ассоциацияларды ауыстыру» командасының жиынтығын BSS шегінде барлық құрылғыларға жібереді. Бұл командалар барлық клиенттердің ажыратылуын жасайды. Бұл ажыратуда барлық сымсыз клиенттер бірден қайталама ассоциация орындауға тырысады, бұл өз ретінде трафиктің көлемін күрт ұлғайтады. Қаскүнем ассоциацияны ажырату кадрларын жібере береді және айналым қайталанады.
* CTS жөнелту шешімдерін жаппай шабуылдау – шабуылдың бұл типі барлық сымсыз клиенттер үшін қатынауды болдырмау және өту жолақтарының иемденуі үшін CSMA/CA ортасында шиеленістер шешу әдісін қолданғанда туындайды. Ол үшін қаскүнем тұрақты түрде жалған STA-ға CTS рұқсат жөнелтпесін жаппай жөнелтуді BSS-те орындайды. Радиожиіліктерді бірге пайдаланатын барлық қалған сымсыз клиенттер CTS-ті қабылдайды және қаскүнем CTS кадрларын тоқтатқанға дейін деректерді жіберуді тоқтатады.

3.24–суретте ортаға қатынау үшін CSMA/CA әдісін сымсыз клиенттің қалай пайдалануы көрсетілген.

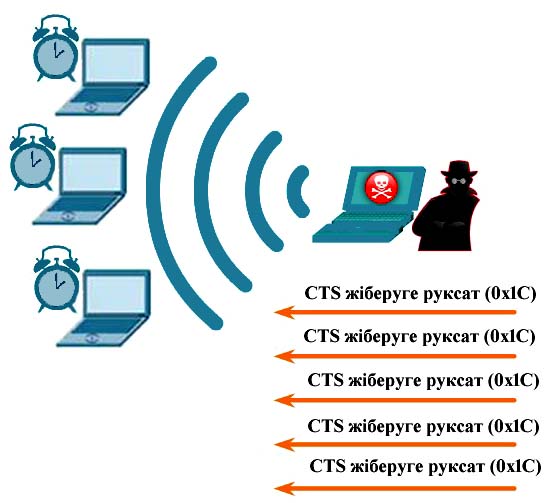


3.24 сурет – CSMA/CA пайдалан отырып, қалыпты режімде жұмыс істеу

3.25-суретте жалған сымсыз клиентте қаскүнемнің CTS кадрлардың жаппай жіберілуін қалай құратыны көрсетілген. Енді қалған барлық клиенттер CTS кадрында берілген кезеңнің аяқталуын күтуге мәжбүрленеді. Бірақ, қаскүнем CTS кадрларын жіберуді жалғастыра береді. Демек, қалған клиенттердің үнемі күтуіне тура келеді. Сөйтіп, қаскүнем ортаны бақылап отырады.

Бұл басқару кадрын қолдана отырып шабуылдаудың тек бірыңғай мысалы. Оның бірнеше басқа түрлері де бар.

Осындай шабуылдардың туу қатерін азайту үшін Cisco корпорациясы Cisco Management Frame Protection (MFP) функциясын қоса отырып, бірқатар шешімдер әзірледі, онда кадрлар мен құрылғыларды спуфингтен алдын ала толық қорғау қамтамасыз етіледі. Cisco Adaptive Wireless басып енуді болдырмау жүйесі бұл шешімде сигнатур шабуылдарын салыстыру жолымен бастапқы мерзімде бұзып енуді табудың функцияларымен толықтырады.



3.25 сурет – CTS жіберуді шешуде жаппай DoS-шабуылын құрушы қаскүнем

Сондай-ақ, IEEE 802.11 стандарты комитеті сымсыз желі қауіпсіздігінің екі стандартын жасады. Cisco MFP пайдаланатын 802.11і стандарты сымсыз желілер үшін қауіпсіздік тектері анықтайды, ал 802.11w басқару кадрларын ққорғау стандарты басқару кадрларын айламен байланысқан проблемаларды шешуге бағытталады.

*Қатынаудың зиянтасымды нүктелері*

Қатынаудың зиянтасымды нүктесі сымсыз маршрутизатор түрінде болады, оны келесі түрде сипаттаймыз:

* мұндай маршрутизатор ұжымдық саясатты бұзып және нақты авторлаусыз ұжымдық желіге қосылады. Нысандарға қатынауы бар кез келген пайдаланушы қымбат емес сымсыз маршрутизаторды қоя алады (әдейі немесе онсыз), бұл теориялық түрде қорғалған желі ресурстарына қатынауды қамтамасыз етеді.
* қаскүнем мұндай маршрутизаторды клиенттердің деректерін алу үшін қосады немесе қосылады немесе өзінің арам ойын жасырады, яки басып алу шабуылы мақсатын пайдаланады.

Дербес сымсыз қатынау нүктесін жасау өте оңай екенін ескеру керек. Мысалы, желіге қатынау қорғауы бар пайдаланушы Wi-Fi желісіне қатынау нүктесі сияқты Windows өзінің авторланған торабын баптайды. Бұл жағдайда станцияланбаған құрылғылар қауіпсіздік шараларын айналып өтеді және жалпы бір құрылғы ретінде желі ресурстарына қатынауға қол жеткізеді.

Қатынаудың зиянды нүктелерін тағайындауды болдырмау үшін ұйымдар қатынаудың станцияланбаған нүктелерінің болуына радиосигналдар спектрінің белсенді мониторингі үшін бағдарламалық қамтуды пайдалану қажет. Мысалы, Cisco Prime инфрақұрылымы желілерін басқару үшін бағдарламалық қамту экранындағы суретте анықталған жалған МАС-адресі қаскүнемнің орналасқан орнын анықтайтын радиожиіліктерінің картасы көрсетілген.

Cisco Prime желілерді басқару үшін бағдарламалық қамтамасыз ету болып табылады, ол желі туралы барлық деректерді жалпы ұсыну мен орталықтандыруды қамтамасыз ететін, басқа бағдарламалармен әрекетке түседі. Әдетте, бұл ПО өте ірі ұйымдарда қолданылады.

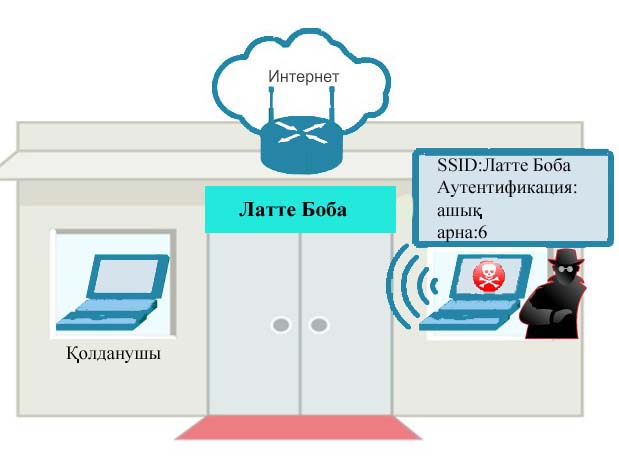
*Басып алу шабуылы*

Қаскүнемнің қолданатын шабуылдарының ішіндегі ең күрделісі - басып алу шабуылы. Басып алу шабуылын жасау үшін тәсілдер де көп.

Осындай тәсілдердің ең көп таралғандарының бірі – «қас егіз», мұнда қаскүнем қатынауға зиянды нүкте енгізеді және оны SSID атынан пайдалану арқылы баптайды. Мқндай типті шабуыл үшін ең лайықты нысандар әуежайлар, кафелер, мейрамханалар, бұлардың Wi-Fi желісіне қатынау тегін және оларда ашық аутентификация пайдаланылады.

Сымсыз клиенттерге қосылуда қатынаудың екі нүктесі бейнеленеді, бұлар сымсыз қатынаулар ұсынады. Қатынаудың зиянды нүктесімен қатар тұрғандар қуатты сигнал табады, бұл сигналды көбіне «қас егіз» жасайды. Енді пайдалангу трафигі қатынаудың барлық нүктесіне барады, ол өз кезегінде деректерді ұстап алады және қатынаудың сенімді нүктесіне жібереді. Қатынаудың станцияланған нүктесінің кері трафигі қатынаудың зиянды нүктесіне жөнелтіледі, содан кейін ештеңе сезбеген стансаға (STA) қайта жіберіледі. Сөйтіп, қаскүнем пайдаланушы паролін, жеке ақпаратын ұрлайды. Желіге қатынай алады және жүйені бұзады.

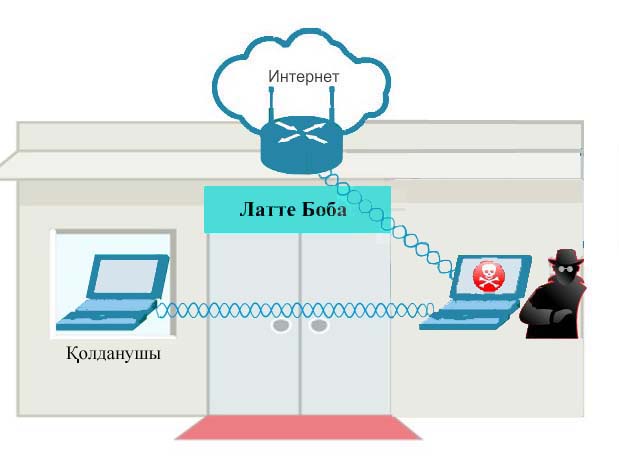
Мысалы, 3.26-суретте «Латте Боба» кафесінде тұр және ештеңе сезбейтін сымсыз клиенттерден трафикті ұрлауға тырысады. Қаскүнем бағдарламалық қамтуды қосады, оның ноутбугының қатынау нүктесіне «қас егізі» бар SSID атауымен арнаны және сымсыз маршрутизаторды басып алады.



3.26 сурет – Қаскүнем «қас егіз» шабуылын бастайды

3.27-суретте пайдаланушы сымсыз қосылудың екі қатынауын көреді, бірақ «қас егіз» қатынау нүктесінің ассоциациясы үшін таңдайды. Қаскүнем пайдалану деректерін басып алады және оны қатынаудың санкция нүктелеріне жібереді, ал олар өз кезеңдерінде «қас егіздің» қатынау нүктесіне жауап трафигін кері жібереді. «Қас егіздің» қатынау нүктесі жауап трафигін басып алады және оның деректерін ештеңе сезбеген пайдаланушыға жібереді.

Шабуылды қолға түсіру арқылы болдырмау WLAN желісінің инфрақұрылымының күрделігіне және желі мониторингінің мұқияттылығына тәуелді. Процесс WLAN желісінің станцияланған құрылғыларын анықтаудан басталады. Ол үшін пайдаланушылар дәлдестіруден өтуі қажет. Сөйтіп, барлық станцияланған құрылғылар аяқталған соң, желінің күмәнді құрылғылары мен трафиктерінің болуына мониторинг жүргізеді.



3.27 сурет - «Қас егіз» шабуылы ойдағыдай өтті

Қазіргі WLAN құрылғыларын пайдаланатын WLAN ұжымдық желілері әкімшілікке құрылғылар ұсынады, олар бөтен енуді (IPS) болдырмаудың сымсыз жүесі ретінде кешенде жұмыс істейді. Бұл құралдарға сканерлер жатады. Олардың көмегі арқылы қатынаудың зиянды нүктелері және бір рангты желілері, сондай-ақ қатынау нүктесінің жүктемесі мен белсенділігіне радиожиіліктік жолақтың мониторингін орындайтын радиоресурстары басқару құралдары жатады. Қатынау нүктесіне үлкен жүктеме әкімшіге станцияланбаған трафиктің болуы мүмкіндігі туралы сигнал береді.

*Сымсыз желі қауіпсіздігіне шолу*

Wi-Fi желісінің қауіпсіздігі әрқашан ерекше тынымсыздық тұдырады, себебі желі шегаралары кеңейтілген. Сымсыз байланыс сигналдары қатты кедергілер – төбелер, едендер, қабырғалар, үй немесе кеңсе шегінен тыс орындар арқылы таратылуы мүмкін. Қауіпсіздіктің қатаң шараларынсыз WLAN желісін орнату - Ethernet-порттарын барлық орындарда, тіпті көшеде орнатумен тең.

Сымсыз желіге енуге тырысатын қаскүнемдер тарапынан қауіпті болдырмау және деректерді қорғау үшін қауіпсіздікті қамтамасыз етудің екі функциясы пайдаланылады:

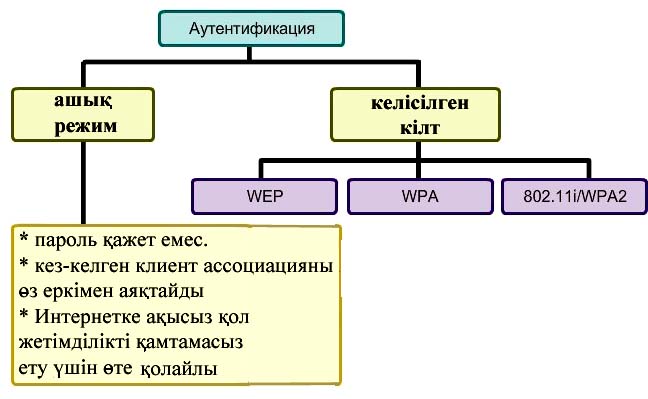
* SSID идентификаторын жасыру. Қатынау нүктелері және кейбір сымсыз маршрутизаторлар SSID идентификаторының сигнал кадрын сөндіруге береді. Сымсыз клиенттер желіге қосылу үшін SSID атауын қолмен белгілеуі қажет.
* MAC-адрестерді сүзгілеу. Әкімші клиенттерге МАС-адрестің физикалық жабдығына байланысты сымсыз қатынауға қолмен рұқсат етуі немесе тыйым салуы мүмкін.

Осы екі функция пайдаланушылардың көпшілігін сиретсе де, нақтысында SSID идентификаторын жасыру да, МАС-адрестерін сүзгілеу де майталман қаскүнемге бөгет жасай алмайды. SSID атауларын тіпті егер қатынау нүктелері олардың кеңтарату жолдарын орындамаған жағдайда да табу оңай, ал МАС-адрестерін қолдан жасауға болады. Сымсыз желіні қорғаудың ең оңтайлы тәсілі аутентификация және шифрлау жүйелерін пайдалану болып табылады.

Бастапқы 802.11 стандартында аутентификациясын екі типі ұсынылған:

* Ашық жүйені аутентификациялау. БАрлық сымсыз клиенттер қосылуды оңай орындай алуы мүмкін, және мұндай жүйе қауіпсіздік ерекше мәнге ие болмаған жағдайда да пайдаланылуы мүмкін (мысалы Интернетке тегін қатынауды ұсынатын орындарда – кафеде, қашықталған орындарда) .
* Келісілген кілтті аутентификациялау. Сымсыз клиенттер мен қатынау нүктесі арасында берілетін деректерді аутентификациялау және шифрлау үшін WEP, WPA немесе WPA2 сияқты мехнизмдер ұсынылады. Бірақ, парольді қосу үшін алдын ала тараптар арасындағы келісу қажет.

3.28-сурет сұлбасында аутентификацияның түрлі типтері туралы қысқа мәліметтер ұсынылған.



3.28 сурет – Аутентификациялау әдісі

*Келісілген кілтті аутентификациялау әдістері*

Келісілген кілтті аутентификациялаудың үш нұсқасы бар:

* Сымсыз байланысты шиярлау хаттамасы (WEP). Сымды қосылумен салыстырмалы деңгейде құпиялықты қамтамасыз ету үшін әзірленген 802.11. шығыс ерекшелемесі. Деректерді қорғау статикалық кілтті пайдаланумен RC4 шифрлау әдісі арқылы қамтамасыз етіледі. Бірақ кілт пакеттерді таратуда ешқашан өзгермейді, сол себепті оны бұзу оңай.
* Wi-Fi қорғалған қатынауы (WPA). WEP-ті пайдаланатын, бірақ уақытша кілтті қолданумен тиімдірек алгоритмді шифрлау есебінен деректерді (TKIP) қамтамасыз ететін Wi-Fi Alliance стандарты. TKIP әр пакет үшін кілтті өзгертеді, сол себепті оны бұзу қиынырақ.
* IEEE 802.11i/WPA2. IEEE 802.11i стандарты сымсыз желілердің қауіпсіз салалық стандарты болып табылады. Wi-Fi Alliance нұсқасы WPA2 деп аталады. 802.11i және WPA2 жетілдірілген шифрлау стандартын пайдаланады (AES). Қазіргі кезде AES шифрлаудың ең сенімді хаттамасы болып есептеледі.

WEP-ті пайдалану ұсынылмайды. WEP-тің жалпы кілттері өзінің жарамсыздығын көкрсетті, демек оларды пайдаланбаған дұрыс. WEP жалпы кілттерінің әлсіз жақтарын теңгеру үшін компаниялармен алдымен SSID идентификаторын жасыруға және МАС-адрестерін сүзгілеуге тырысты. Сөйтсе де, бұл әдістер өте сенімсіз болды.

WEP негізінде қауіпсіздік жүйесінің сенімсіздігіне байланысты бірқатар уақыт барысында аралық қауіпсіздік шаралары пайдаланылды. Cisco сияқты жеткізушілер қауіпсіздіктің жоғары талаптарын қанағаттандыруға ұмтылып, бір уақытта 802.11i стандартын жетілдіруге тырысып, өз жүйелерін әзірледі. 802.11i стандартын дамыту процесінде TKIP шифрлау алгоритмі жасалды, ол Wi-Fi Alliance WPA қауіпсіздігін қамтамасыз ету әдісімен байланысты болды.

Қазіргі сымсыз желілер әрдайым 802.11i/WPA2 стандарттарын қолдануы қажет. WPA2 802.11i стандартының Wi-Fi нұсқасы болып табылады, демек, WPA2 және 802.11i терминдері өзара алмастырғыштар болып табылады.

2006 жылдан WPA2 пайдалану үшін Wi-Fi Certified логотипі енгізілген барлық құрылғылар сертификатталды.

Өнімділігті оңтайландыру мақсатында Wireless-N желісі WPA2-Personal қауіпсіздік желісін пайдалану қажет.

Кесте келісілген кілттерді аутентификациялаудың үш типтік әдістері көрсетілген.

Кесте Келісілген кілтті аутентификациялау әдістері

|  |  |  |  |
| --- | --- | --- | --- |
|  | **WEP** | **WPA** | **802.11i/WPA2** |
| Аутентификациялау әдісі | Фазалық ығысуды кодтау (PSK) | PSK және 802.1х | PSK және 802.1х |
| Шифрлау | RC4 | TKIP | AES |
| Хабарламаның тұтастығы | CRC-32 | MIC | CCMP |
| Қауіпсіздік | әлсіз | сенімді | неғұрлым сенімді |

*Шифрлау әдістері*

Шифрлау деректерді қорғау үшін қолданылады. Егер қаскүнем шифрланған деректерді қолға түсірсе, онда ол қысқа мерзімде оларды шеше алмайды.

IEEE 802.11i, Wi-Fi Alliance WPA және WPA2 стандарттарын шифрлаудың келесі хаттамаларында пайдаланады:

* Уақытша кілттерді пайдаланып шифрлау (TKIP). TKIP WPA стандартында қолданылатын шифрлау әдісі болып табылады. Ол 802.11 WEP шифрлау әдісі үшін сипатты шығыс дәлсіздіктерін болдырмау есебінен WLAN желілері жабдығының алдыңғы нұсқасын қолдауды қамтамасыз етеді. Ол WEP-ті пайдаланады, бірақ, TKIPті қолдана отырып, 2-деңгейлі тиімді жүктемені шифрлауды және хабарлама санкцияланбай орындалатынына көз жеткізу үшін шифрланған пакетте хабарлама тұтастығын тексеруді орындайды.
* Шифрлаудың жетілдірілген стандарты (AES). AES WPA2 стандартында қолданылатын шифрлау әдісі болып табылады. бұл әдіс басымдырақ болып табылады, себебі IEEE салалық стандартына сәйкес келеді. AES TKIP сияқты функцияларды орындайды, бірақ мұның шифрлауы елеулі сенімділікті қамтамасыз етеді. Ол CCMP хаттамасын пайдаланады, бұл хаттама тораптарға санкциялаусыз пайдаланылатын шифрланған және шифрланбаған биттерді тануға мүмкіндік береді.

Әрқашан мүмкіндігінше AES-пен WPA2-ны таңдаған дұрыс.

WLAN желілері жұмысындағы ақауларды іздеу және болдырмау.

*Ақауларды іздеу және болдырмау тәсілдері*

Желідегі кез келген ақауларды ідеу және болдырмау үшін жүйелік келісті пайдалану қажет. Мысалы, OSI және TCP/IP логикалық желілік модельдер желі функцияларын модульдік деңгейлерге бөледі.

Ақауларды іздеу және болдырмауда желімен туындаған проблемаларды оқшаулау үшін физикалық желіге көпдеңгейлі модельдерді қолдануға болады. Мысалы, егер барлық белгілер нақты қосылудағы проблеманы көрсетсе, онда желілік маман физикалық деңгейде жұмыс істейтін арнадағы ақауды болдырмауға жұмыла алады. Егер бұл арна лайықты қызмет істесе, онда техникалық маман проблема тудыруы мүмкін басқа салалар деңгейлерін тексереді.

Ақауларды іздеу және болдырмау үш негізгі келісі бар, олар желі проблемаларын шешу үшін қолданылады:

* Төменнен жоғарыға: 1-деңгейден бастап жоғары бағытқа жылжу.
* Жоғарыдан төменге: жоғары деңгейден бастап төменгі бағытқа жылжу.
* «Бөліп ал да билік жүргіз»: тағайын адресіне жаңғрық-сұранысын жіберу. Егер жаңғырық-сұраныс өтпесе, онда төменгі деңгейлерді тексеру керек. Егер жаңғырық-сұраныс өтсе, онда жоғары деңгейлерді тексеру керек.

*Сымсыз клиентті қосу мүмкін емес*

WLAN желісінде ақауларды іздеу және болдырмауда кандидаттарды шығару процесін пайдалану ұсынылады.

3.29 суретте сымсыз клиент WLAN желісіне қосыла алмайды. Қосылу болмаған жағдайда келесіні тексеру қажет:

* Ipconfig командасы арқылы компьютерде желі конфигурациясын тексеріңіз. DHCP бойынша ДК ІР-адрес алғанына немесе статикалық ІР–адрес көмегімен бапталғанына көз жеткізіңіз.
* ПСымды желіге құрылғының қосылу мүкіндігін тексеріңіз. Құрылғыны LAN сымды желісіне қосыңыз және ІР-адресі ping командасын орындаңыз.
* Қажет жағдайда клиентке сәйкесті драйверді қайта жүктемелеу қажет. Басқа сымсыз желілік адаптерді қолдану талап етілуі мүмкін.
* Егер сымсыз желі адаптері түзу болса, онда клиенттегі шифрлау баптауын және қауіпсіздік режімін тексеру қажет. Егер қауіпсіздік баптау сәйкеспесе, онда клиент WLAN желісіне қатынай алмайды.

Егер компьютер жарамды болса, бірақ сымсыз желіге қосылу тиімді жұмыс істесе, онда келесіні тексеріңіз:

* Компьютердің қатынау нүктесінен қанша қашықтықта тұр? Компьютер жоспарланған қамту зонасы шегінен қаншалықта тыс тұр (BSA)?
* Сымсыз клиенттегі арна баптауын тексеріңіз. Егер SSID атауы ұрыс болса, онда клиентті БҚ сәйкесті арнаны табуды орындау қажет.
* Басқа құрылғылар зонасында 2,4 ГГц жолағында бөгеуілдер жасайтын жағдайларды тексеріңіз. Мұндай құрылғыларға радиотелефондар, радио-нянялар, микротолқынды пештер, қауіпсіздіктің сымсыз жүйелері және қатынаудың әлеуетті зиянды нүктелері жатуы мүмкін. Бұл құрылғылардан келіп түсетін деректер WLAN желісінің жұмысына бөгеуілдер жасауын және қатынау нүктесі мен сымсыз клиент арасындағы қосылыстардың үзілуін тудыруы мүмкін.

Одан әрі барлық құрылғылардың өз орнында тұрғанын тексеру керек. Физикалық қауіпсіздік проблемасының туу мүмкіндігін ұмытпаңыздар. Қоректендіру барлық құрылғыларға беріле ме? Барлық құрылғылар қосылған ба?

Түзетілмеген жалғағыштардың жоқ немесе зақымдалған кабелдеріне құрылғылар кабельдері көмегімен қосылғандардың қосылысын тексеріңіз. Егер барлық қажетті құраушылар орнында болса, онда қатынау нүктесін қоса отырып, құрылғылардың жаңғырық-тестілеуі көмегімен LAN сымсыз желісін тексеруіңіз. Егер бұл кезеңде қосылу әзірге болмаса, онда оның конфигурациясы немесе қатынау нүктесінде проблема туындауы мүмкін.

Егер компьютер проблемалар көзі болып табылмаса және құрылғының физикалық жағдайы тексерілсе, онда қатынау нүктесінің жұмысы меңгерілуі тиіс. Қатынау нүктесінің қоректену жағдайын тексеріңіз.

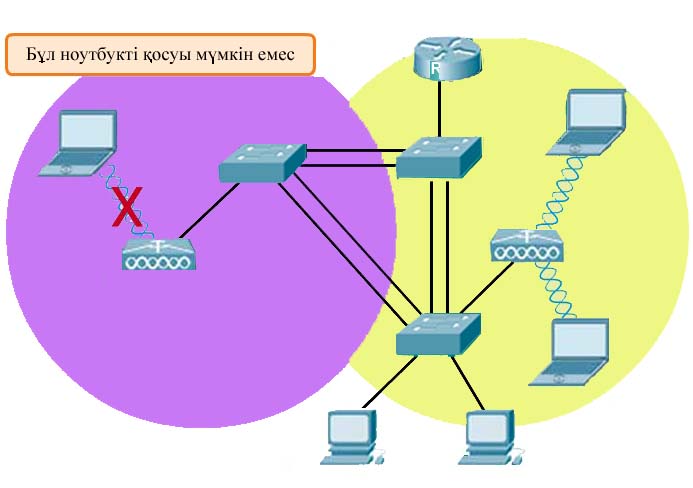
*Желінің баяу жұмыс істеуі жағдайында ақауларды іздеу және болдырмау*

Қос диапазонды 802.11n/ac маршрутизаторының өткізу қабілетін оңтайландыру және ұлғайту үшін келесілер орындалады:

* Сымсыз клиенттерді жаңалау. 802.11b және тіпті 802.11g құрылғысының ескірген моделі WLAN желісінің барлқ жұмысын бөгеуі мүмкін. Оңтайланған өнімділікке қол жеткізу үшін барлық сымсыз құрылғылар максимал рұқсатталған стандарттарды қолдауы қажет.
* Трафикті бөлу. Сымсыз желінің өнімділігін оңтайландырудың ең қарапайым тәсілі - 802.11n 2,4 ГГц және 5 ГГц жолағын бөлу болып табылады. Демек, IEEE 802.11n (немесе жоғары) стандартын трафикпен басқаруын жеңілдету мақсатында жекеленген екі сымсыз желі түрінде екі жолақты пайдалануға болады.

Трафикті бөлуді пайдалану үшін бірқатар алғышарттар бар:

* 2,4 ГГц жолағы кідірістерді сезбейтін базалық интернет-трафигі үшін жарамды.
* Өткізу жолағын WLAN жақын басқа желілерімен бірге пайдалануға болады.
* ГГц жолағы 2,4 ГГц жолағына қарағанда азырақ жүктелген және медиадеректерді ағындық тарату үшін өте қолайлы.
* ГГц жолағы көбірек арналардан тұрады, демек таңдалған арна бөгеуілдер әсеріне аз ұрынады.



3.29 сурет – Қосылу проблемалары

2,4 ГГц және 5ГГц жолақтарында қосдиапазонды маршрутизатордың үндемеуі бойынша желінің бірдей атауы қолданылады. Трафикті сегменттеудің ең қарапайым тәсілі сымсыз желілердің біреуін қайта атау болып табылады. жекелегн жазба атаулар болған жағдайда, қажетті желіге қосылу айтарлықтай қарапайым.

Сымсыз желінің әрекет ету ауқымын кеңейту үшін сымсыз маршрутизатордың нақты орналасу зонасында қандай да бір кедергілердің (жиһаз, арматура және биік заттар) болмауын қамтамасыз ету қажет. Аталған кедергілер сигналды блоктайды. Соның әсерінен WLAN желісінің әрекет аумағы азаяды. Егер проблема бұрынғыша шешілмесе, онда Powerline сымсыз технологиясын немесе Wi-Fi Range Extender қамтуын арттыру технологиясын пайдалануға болады.

WLAN желісі көбіне үй, кеңсе және ұжымдық орталарда іске асырылады. 802.11 стандартының WLAN желісі үшін 2,4 ГГц, 5 ГГц және 60 ГГц жиіліктері пайдаланылады. ITU-R радиобайланыс спектрі радиожиіліктерді бөлу спектрін реттейді, ал IEEE комитеті сымсыз желілердің физикалық деңгей және МАС деңгейі үшін осы жиіліктерді қолдануды анықтауға мүмкіндік беретін 802.11 стандарттарын ұсынады. Wi-Fi Alliance жеткізуші өнімінің салалық нормативтер мен стандарттарға сәйкестігін сертификаттайды.

Сымсыз клиент инфрақұрылым құрылғысына (сымсыз маршрутизатор немесе сымсыз қатынау нүктесі) қосылу үшін сымсыз желілік адаптерді пайдаланады. Сымсыз клиенттер SSID пайдалана отырып, қосылады. Қатынау нүктесі контроллер негізінде үлкен мөлшерлі желі құрамында немесе шағын кластерлер құрамында дербес құрылғылар ретінде іске асырылуы мүмкін.

Cisco Aironet қатынау нүктесі барлық бағытты антенналарға, бағытталған антенналарға немесе «толқынды арна» (Yagi) типті антеннаға сигналды бағыттау үшін қолданылуы мүмкін. IEEE 802.11n/ac/ad стандарты өткізу қабілетін арттыру және бір уақытта төрт антеннаға дейін қолдау үшін МІМО технологиясын пайдаланады.

Тікелей қосылу немесе сервистердің тәуелсіз базалық жиынтығы (IBSS) режімінде екі сымсыз құрылғы бір-бірімен бір рангты желі арқылы қосылады.

Инфрақұрылымдық режімідегі қатынау нүктесі сымды тарату жүйесін қолдана отырып , желілік инфрақұрылымға қосылады. Қатынаудың әр нүктесі BSS жиынтығын анықтайды және бірегей BSSID идентификаторын алады. Бірнеше BSS жиынтығын сервистердің кеңейтілген бір жиынтығына (ESS) біріктіруге болады. ESS-те SSID жеке атауын қолдануда ESS құрамындағы BSS жиынтығы бойынша еш проблемасыз алмастыру үшін мүмкіндіктер қамтамасыз етіледі. SSID атауымен нақты пайдаланылған желі қатынау деңгейін бөлу үшін қосымша SSID атауын пайдалануға болады.

Сымсыз клиент алдымен қатынау нүктесіндегі аутентификациялауды, ал содан кейін осы қатынау нүктесінің ассоциациясын орындайды. Мұнда 802.11i/WPA2 атунетификация стандартын пайдалануға болады. AES - WPA2 қатарында қолдануға қажетті шифрлау әдісін ұсынады.

Сымсыз желіні жоспарлауда нақты зонаны қамту үшін бірнеше қатынау нүктелерін жаймалауда жабылмайтын арналарды пайдалану қажет. ESS құрамындағы BSA зоналары 10-15% жабылуы қажет. Cisco қатынау нүктесі қондырғыны қарапайым ететін PoE қолдайды.

Сымсыз желілер көбіне DoS-шабуылдарға, деректерді басып алуға, қатынаудың зиянды нүктелері және қаскүнемдердің сымсыз шабуылдары сияқты қатерлерге ұрынады. Cisco корпорациясы осы типті қатерлерді азайтуға бағытталған шешімдер қатарын әзірледі.



Тексеру жұмыстары № 7

№1 жаттығу Сөйлемді аяқтаңыз:

А бағанынан сөйлемнің басын В бағанынан ең қолайлы соңымен салыстырыңыз. Параметрді таңдап, сөйлемді аяқтаңыз. Есіңізде болсын, В бағанындағы элементтердің біреуі артық, және әрбір затты тек бір рет пайдалануға болады.

|  |  |
| --- | --- |
| А бағаны | **В бағаны** |
| 1. ЕАР\_\_\_\_\_ | A. WLAN аймағы бірнеше сымсыз ұяшықтарды тарату жүйесін қолдана отырып, бір блокқа қосу арқылы пайда болады |
| 1. сеть ad-hoc\_\_ | Б. Сымсыз клиент |
| 1. STA\_\_\_\_\_ | B. Клиенттермен тең құқылы сымсыз қосылу желісі |
| 1. SSID\_\_\_\_ | Г сымсыз желі қандай сымсыз желіге жататындығын білдіретін қызмет |
| 1. ESS\_\_\_\_ | Д. Шифрлау үшін қолданылатын сымсыз желілерде қолданылады |
|  | E. Сымсыз желілерде пайдаланушылардың түпнұсқалығын растау үшін қолданылады |

**№2 жаттығу Дұрыс жауапты таңдаңыз**

1. Шағын шина компаниясына тауарлық-материалдық құндылықтарды басқару және нақты уақыт режимінде сату үшін бас кеңсеге WAN-дің арзан қосылымы қажет. Компания үшін WAN байланысының қай түрі жақсы?

а) SONET

б) T3

в) T1

г) DSL

д) жалға алынған желі

2. Қандай WAN байланысы анықталған енгізу жолағынан тұратын белгіленген арнаны қамтамасыз етеді?

а) нүкте-нүкте

б) электр тізбегінің коммутациясымен

в) пакеттік коммутациямен

г) кабель

3. Ethernet, WLAN, Wi-Fi, ATM және PPP сияқты жиі қолданылатын протоколдар мен технологиялар жұмыс істейтін OSI моделінің деңгейін көрсетіңіз.

а) 1 деңгей

б) 2 деңгей

в) 3 деңгей

г) 7 деңгей

4. DSL модемді қашан қолдану керек?

а) қызмет ұялы телефон арқылы көрсетілген кезде

б) кабельді теледидар арқылы жоғары жылдамдықты байланыс қамтамасыз етілген кезде

в) стандартты телефон желісі арқылы жоғары жылдамдықты сандық байланыс қажет болған кезде

г) спутниктік тарелка антеннасын («ыдыс») пайдаланған кезде

5. Клиент кіру нүктесімен байланыс орнатқан кезде қандай WLAN қауіпсіздік протоколы жаңа динамикалық кілтті жасайды?

а) EAP

б) PSK

в) WEP

г)WPA

6. Желіні орнату бойынша маман жаңа жалпыға ортақ сымсыз желі үшін қауіпсіздік жүйесін әзірлеуде. Жаңа желі үшін аутентификацияның қай түрі қолайлы?

а) EAP

б) WEP

в) MAC мекен-жайын сүзу

г) ашық түпнұсқалық растама

7. Сымсыз қосылысты сәтті орнату үшін клиент пен қол жеткізу нүктесінде қандай үш параметр сәйкес келуі керек? (Үш нұсқаны таңдаңыз.)

а) SSID

б) аутентификация

в) MD5 тексеру сомасы

г) шифрлау кілті

e) MAC адрес сүзгілері

8. Техника жаңа сымсыз кіру нүктесінде қауіпсіздік саясатының бұзылуын анықтайды. Конфигурацияның үш нұсқасы хакерге қол жеткізуді жеңілдетеді? (Үш нұсқаны таңдаңыз.)

a) NAT конфигурациясы

б) SSID хабар тарату

в) ашық түпнұсқалық растаманы қолдану

г) MAC адрес сүзгілерін қосу

д) ішкі IP мекенжайды пайдалану арқылы

е) IP мекенжайын беру үшін DHCP қолдану

9. Техниктен ғимараттың сымды Ethernet желісіне сымсыз қосылуды ұсыну сұралды. Қандай үш фактор кіру нүктелерінің қажетті санына әсер етеді? (Үш нұсқаны таңдаңыз.)

а) ғимараттың мөлшері

б) ғимарат ішіндегі қатты ішкі қабырғалардың саны

в) бірнеше кеңселерде микротолқынды пештердің болуы

г) сымсыз желіде қолданылатын шифрлау әдісі

д) Windows және Appletalk операциялық жүйелерін пайдалану

е) Қысқа толқынды немесе инфрақызыл сәулеленуді АР-да қолдану

10. Сымсыз желілерде қауіпсіздік неге маңызды?

a) Сымсыз желілер әдетте сымды желілерге қарағанда баяу жұмыс істейді.

б) теледидарлар мен басқа құрылғылар сымсыз құрылғылардың сигналдарына кедергі келтіруі мүмкін.

в) сымсыз желілер деректерді әуе арқылы жібереді, бұл оңай қол жеткізуді қамтамасыз етеді.

г) Найзағай сияқты экологиялық факторлар сымсыз желілерге әсер етуі мүмкін.

11. Сымсыз құрылғыдағы Wi-Fi логотипі нені білдіреді?

a) Құрылғыны электр және электроника инженерлері институты (IEEE) мақұлдады.

б) құрылғы барлық басқа сымсыз стандарттарға сәйкес келеді.

в) құрылғы осы стандарттың Wi-Fi логотипі бар басқа құрылғыларымен үйлесімді.

г) құрылғы алдыңғы барлық сымсыз стандарттарға сәйкес келеді.

12. Сымсыз көпірлер үшін қай мәлімдеме дұрыс?

а) екі желіні сымсыз қосады

б) сымсыз жергілікті желіге қосылған стационарлық құрылғы

в) сымсыз клиенттерге сымды желіге қосылуға мүмкіндік береді

г) сымсыз сигналдың қарқындылығын арттырады

13. Әдепкі бойынша кіру нүктесі аутентификацияның қандай түрін қолданады?

а**)** Ашық

б) PSK

в) WEP

г) EAP

14. Кіру нүктесі қандай аутентификация әдісін қолдана алады?

а) WEP

б) WPA

в) EAP

г) ASCII

15. Ашық түпнұсқалық растама мен алдын-ала келісілген кілттерді қолданудың қандай айырмашылығы бар?

а) ашық түпнұсқалық растама парольді қажет етеді. Алдын ала келісілген кілттер құпия сөзді қажет етпейді.

б) ашық аутентификация сымсыз желілерде қолданылады. Алдын ала келісілген кілттер сымды желілерде қолданылады.

в) алдын-ала келісілген кілттер шифрланған құпия сөзді қолдануды талап етеді. Ашық түпнұсқалық растама құпия сөзді пайдалануды қажет етпейді.

г) алдын-ала келісілген кілттер MAC мекен-жайларының кіру нүктесіне бағдарламалық түрде жазылуын талап етеді. Ашық түпнұсқалық растама мұндай бағдарламалауды қажет етпейді.

16. Сымсыз кіру нүктесінің қауіпсіздігін арттыру үшін қандай әдіс ұсынылады?

а) қалқымалы блокаторды іске қосу

б) әдепкі IP мекенжайын өзгерту

в) антивирустық анықтамаларда жаңарту

г) кіру нүктесі мен клиент арасындағы кабельдің физикалық қауіпсіздігі

17. Сымсыз технологияның сымды технологиядан үш артықшылығын сипаттаңыз. (Үш нұсқаны таңдаңыз.)

а) қауіпсіздіктің жоғары деңгейі

б) үлкенірек диапазон

в) кез-келген уақытта, кез-келген жерде қосылу мүмкіндігі

г) орнатудың қарапайымдылығы мен төмен құны

д) лицензиялық жиіліктер диапазонын пайдаланудың қарапайымдылығы

е) қосымша құрылғыларды қосудың қарапайымдылығы

**3-жаттығу Қолданбалы тапсырмалар**



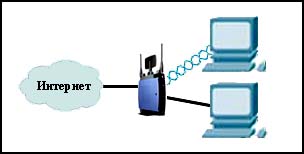
1. Суретке қараңыз. Суретте келтірілген ақпарат негізінде қай сөз тіркесі жарамды?

a) АР кіру нүктесіне қосылған барлық сымсыз құрылғыларға SSID **"University"** атауы тағайындалуы керек.

б) АР кіру нүктесіне қосылған кез-келген сымсыз клиенттің бірдей IP мекенжайы және SSID болуы керек.

в) ұсынылғанАР кіру нүктесінде физикалық сымды LAN байланысы жоқ.

г) бұл конфигурация тек арнайы ad-hoc сымсыз желіде болады.



1. Суретке қараңыз. Жеке IP-мекен-жайларды Интернетке жіберуге болатын IP мекен-жайларға түрлендіру үшін Linksys интегралды маршрутизаторында қандай функцияны орнатуға болады?

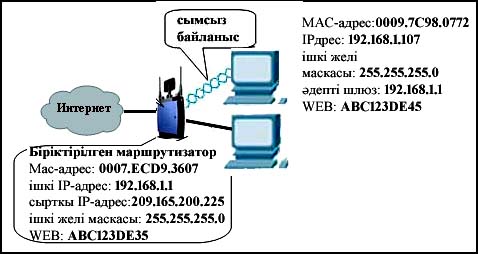
а) DHCP

б) NAT

в) WEP



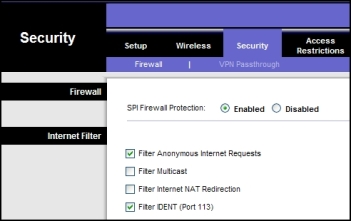
1. Суретке қараңыз. Берілген желідегі қате конфигурацияны көрсетіңіз.



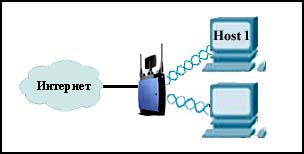
1. Суретке қараңыз. Сымсыз хост Интернетке қол жетімді емес, бірақ сымды хост қол жеткізеді. Мәселе неде?



1. Суретке қараңыз. Берілген желідегі қате конфигурацияны көрсетіңіз.



1. Суретке қараңыз. Linksys біріктірілген маршрутизаторының қауіпсіздік мәзіріндегі SPI Firewall Protection қорғау опциясы үшін "Enabled" опциясын не қамтамасыз етеді?



7. Суретке қараңыз. Linksys біріктірілген маршрутизаторында NAT және DHCP орнатылған. Жергілікті компьютерге (Host1 түйіні) қандай IP-мекен-жай тағайындалады?

а) 10.0.0.17

б) 128.107.1.2

в) 192.135.250.0

г) 209.165.201.1

## Ұсынылған әдебиттер тізімі

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 672 с.
2. Программа Сетевой академии CISCO CCNA 3 и 4. Вспомогательное руководство.: Пер с англ. – М.: ООО «И.Д.Вильямс», 2007.
3. Леинванд А. Пински Б. Конфигурирование маршрутизаторов Cisco.: - Вильямс 2001. – 368 с.
4. **Брайан Хилл** Полный справочник по Cisco(рус**).: Вильямс, 2006. – 1088 с.**
5. Брэдли Дансмор, Тоби Скандьер Справочник по телекоммуникационным технологиям: Вильямс, Серия: Cisco Press. – 2004. – 630 с.
6. Хьюкаби Д. Маршрутизаторы Cisco. Руководство по конфигурированию Вильямс Диалектика .- 2012. – 736 с.
7. Лукас М.В. Маршрутизаторы CISCO для отчаявшихся администраторов. Простые методы управления маршрутизаторами и коммутаторами: БХВ-Петербург, 2010 . – 160 с.
8. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822: Диалектика Вильямс, 2013. – 720 с.

## Тексеру жұмыстарының жауаптары

**Тексеру жұмыстары № 1**

|  |  |
| --- | --- |
| 1 | 1)Д 2) Е 3)Б 4) Ж 5) А 6) З 7) В |
| 2 | 1)б 2) г 3) а 4) б 5) г 6) а 7) в 8) г 9) б 10) в |
| 3 | 1) Ия 2) Жоқ 3) Жоқ 4) Ия 5) Ия 6) Жоқ 7) Жоқ 8) Ия 9) Жоқ 10) Ия 11) Жоқ 12) Ия 13) Ия 14) Ия 15) Ия 16) Жоқ 17)Ия 18) Ия |
| 4 | 1 Себеп желілік адаптер драйверінің дұрыс орнатылмауы болуы мүмкін  2 Мәселе принтер драйверінде. Бастапқы драйверді орнату керек |

**Тексеру жұмыстары № 2**

|  |  |
| --- | --- |
| 1 | 1)Г 2) Е 3) В 4) З 5) А 6) Д 7) Б |
| 2 | 1)б 2)в 3)а 4)в 5)б 6) в 7) г 8) б 9) б 10) а |
| 3 | 1) Жоқ 2) Жоқ 3) Ия 4) Жоқ 5) Ия 6) Жоқ 7) Жоқ 8) Ия 9) Ия 10) Жоқ 11) Ия 12) Жоқ |
| 4 | а) қайталағыш; б) модем; в) маршрутизатор; г) шлюз; д) модем; е) шлюз |

**Тексеру жұмыстары № 3**

|  |  |
| --- | --- |
| 1 | 1)Д 2) Е 3) З 4) Ж 5) В 6) А 7) Б |
| 2 | 1)а 2)б 3) г 4) в 5) а 6) г 7) г 8) в 9) в 10) б |
| 3 | 1) Жоқ 2) Жоқ 3) Ия 4) Жоқ 5) Ия 6) Ия 7) Ия 8) Жоқ 9) Ия 10) Жоқ |
| 4 | * + 1. 255.240.0.0     2. а) в) г)     3. а) г)     4. резервтік DNS серверлерін жасаңыз |

**Тексеру жұмыстары № 4**

|  |  |
| --- | --- |
| 1 | * 1. Г 2) Б 3) Д 4) Е 5) В |
| 2 | 1)д 2) в 3) г 4) г 5) г 6) б 7) в 8) г 9) в 10) б |
| 3 | 1) Жоқ 2) Ия 3) Жоқ 4) Жоқ 5) Ия 6) Жоқ 7) Жоқ |
| 4 | 1. Серверде жалдау уақытын 20 күнге орнату керек 2. 2. Сіз компьютердің атауымен қосыла аласыз (NetBIOS атауы) 3. Тұрақты LNHOSTS файлын орнатыңыз 4. B және C желілерінде DHCP агентін теңшеңіз 5. 172.30.20.10 ішкі ғаламдық мекен-жайы |

**Тексеру жұмыстары № 5**

|  |  |
| --- | --- |
| 1 | 1)А 2) Б 3) Е 4) В 5) Д |
| 2 | 1)г 2) а 3) б 4) б 5) а 6) а 7) г 8) а 9) а 10) а |
| 3 | 1) Ия 2) Ия 3) Ия 4) Жоқ 5) Жоқ 6) Ия 7) Жоқ 8) Ия 9) Ия 10) Ия |
| 4 | 1. Екi 2 C – әдепкі шлюзмен белгіленген хосттан маршрутизаторға өту. |

**Тексеру жұмыстары № 6**

|  |  |
| --- | --- |
| 1 | * 1. а 2) а 3) г 4) в 5) в |
| 2 | * 1. **switchport mode trunk** 2) **encapsulation dot1Q 5** командасында жарамсыз VLAN бар. |

**Тексеру жұмыстары № 7**

|  |  |
| --- | --- |
| 1 | 1)Е 2) В 3)Б 4) Г 5) А |
| 2 | 1. г 2) а 3) б 4) в 5) г 6) г 7) а,б,г 8)б,в,д 9) а,б,в 10) в 11) в 12) а 13) а 14) в 15) в 16) б 17)в,г,е |
| 3 | 1) а 2) б 3) Сымды қосылымға арналған кабель түрі дұрыс емес. 4) Жарамсыз WEP хост кілті 5) Хосттың IP мекенжайы жарамсыз. 6) Ішкі хосттың сұраныстарына жауап беру үшін маршрутизаторға келетін пакеттерді талап етеді. 7) а |

**МАЗМҰНЫ**

[Желілерінің негіздері 3](#_Toc29730315)

[1.1 Желіні пайдалану 3](#_Toc29730316)

[1.2. Желілік технологиялар 14](#_Toc29730317)

[1.3. TCP/IP хаттаманының стегі 27](#_Toc29730318)

[Коммутация және маршрутизация 35](#_Toc29730319)

[2.1. IP маршрутизация (бағыттау) 35](#_Toc29730320)

[2.2 Мекен-жайларды анықтау 51](#_Toc29730321)

[2.3. Қолданбалы деңгейдің хаттамалары 61](#_Toc29730322)

[2.4. Корпоративтік желідегі коммутация және бағыттау 80](#_Toc29730323)

[2.5. Коммутатор базасы бойынша виртуалды желі 87](#_Toc29730324)

[2.6. Ағаштарды байланыстыратын протокол және кіру тізімдері 98](#_Toc29730325)

[Сымсыз желілер 111](#_Toc29730326)

[3.1. Сымсыз байланыс тұжырымдамалары 112](#_Toc29730327)

[Ұсынылған әдебиттер тізімі 153](#_Toc29730328)

[Тексеру жұмыстарының жауаптары 154](#_Toc29730329)

[Тесттер 156](#_Toc29730330)

## Тесттер

$$$ 1

“Концентратор” желісінің топологиясын не жақсы сипаттайды?

A) желіні басқару мен басқаруды орталықтандырады

В) ондай топология жоқ

C) барлық компьютерлерге бірдей қол жетімділік

D) дұрыс жұмыс істеу үшін терминаторлар қажет

E) басқа қызметтерге қарағанда кабель шығынын аз талап етеді

$$$ 2

Сақина топологиясын не жақсы сипаттайды?

A) желіні басқару мен басқаруды орталықтандырады

В) беру ортасы арзан және оңай жұмыс істейді

C) барлық компьютерлерге бірдей қол жетімділік

D) дұрыс жұмыс істеу үшін терминаторлар қажет

E) ондай топология жоқ

$$$ 3

Автобус желісінің топологиясын не жақсы сипаттайды?

A) желіні басқару мен басқаруды орталықтандырады

В) желідегі компьютерлер саны оның жұмысына әсер етпейді

C) барлық компьютерлерге бірдей қол жетімділік

D) тарату құралы арзан және оңай жұмыс істейді

E) ондай топология жоқ

$$$ 4

Жұлдыздар желісінің топологиясын не жақсы сипаттайды?

A) желіні басқару мен басқаруды орталықтандырады

В) бір кабельді ажырату желіні тоқтатады

C) барлық компьютерлерге бірдей қол жетімділік

D) тарату құралы арзан және оңай жұмыс істейді

E) ондай топология жоқ

$$$ 5

Желілік шина топологиясы бар желідегі кабельді кеңейтуге қандай құрал көмектеседі?

A) желілік адаптер картасы

В) терминатор

C) деректерді беру орталығында қосылу модулі

D) баррель қосқышы

E) концентратор

$$$ 6

Қай топология пассивті?

A) жұлдыз

B) сақина

C) шина

D) жұлдызды сақина

E) жұлдыз шинасы

$$$ 7

Компьютер мен принтердің бірге жұмыс істеуіне не мәжбүр етеді?

A) жүргізушілер

В) пакеттік процессор

C) хаттамалар

D) HCL

E) желілік тақта

$$$ 8

Компьютерлерге желіде бірге жұмыс істеуге не мүмкіндік береді?

A) жүргізушілер

В) пакеттік процессор

C) хаттамалар

D) HCL

E) желілік тақта

$$$ 9

OSI Project 802 стандарттарын қандай модель деңгейлері үшін анықтайды?

A) Қолданбалы және өкілді

В) Физикалық және арна

C) Желі және арна

D) Көлік және желі

E) Өкіл және көлік

$$$ 10

Қол жетімділікті басқару деңгейі қандай OSI деңгейіне жатады?

A) Физикалық

B) Арналық

C) Желілік

D) Көліктік

E) Өкілдік

$$$ 11

Деректерді жібермес бұрын, компьютер деректерді жіберетіндігін хабарлайды. Ол қандай қатынау әдісін қолданады?

A) CSMA / CA

В) маркер берумен

C) сауалнаманы

D) басымдық бойынша

E) CSMA / CD

$$$ 12

Деректерді жібермес бұрын, компьютер трафиктің болуын анықтау үшін кабельді «тыңдайды». Олар қандай қатынау әдісін қолданады?

A) CSMA / CA

В) маркер берумен

C) сауалнаманы

D) басымдық бойынша

E) CSMA / CD

$$$ 13

Маркерді беруге арналған енгізу әдісі соқтығысуды мына жағдайлардың көмегімен болдырмайды:

A) маркердің соқтығысуын болдырмауға көмектесетін кодты қолдану

В) әртүрлі маршруттар бойынша қозғалатын бірнеше маркерлердің болуы

C) маркерді бір компьютермен бір уақытта қолдану

D) желілік трафиктің қарқындылығын бақылау үшін аймақтарды қолдану

E) компьютерлерді маркерсіз құлыптаудың арқасында

$$$ 14

Драйвер бұл:

A) апспаптық қамтамасызету

В) перифериялық құрылғы

C) плата

D) бағдарламалық қатамасызету

E) байланыс құрылғысы

$$$ 15

Желілік ортада желілік адаптер картасының драйвері мына жағдайлар үшін қажет:

A) желідегі басқа адаптер карталарымен байланыс үшін

В) адаптер тақтасы мен компьютердің операциялық жүйесі арасындағы байланыс үшін

C) файлдық сервер мен желідегі басқа компьютерлер арасындағы байланыс үшін

D) желідегі әр түрлі компьютерлер арасындағы байланыс үшін

E) тақта мен кабель арасындағы байланыс үшін.

$$$ 16

Принтер драйверлеріне қолданылатын мәлімдемені таңдаңыз:

A) барлық принтерлердің толыққанды жұмысын қамтамасыз ететін әмбебап принтер драйвері бар

В) бір өндіруші жасаған барлық принтерлер бірдей драйверді қолдана алады.

C) бір өндірушінің лазерлік принтер драйвері өндірушіге қарамастан барлық лазерлік принтерлердің толық функционалдығын қамтамасыз етеді.

D) принтердің әр моделі үшін осы принтер моделінің барлық функцияларын пайдалануға мүмкіндік беретін арнайы драйвер жасалады

E) драйвер барлық компьютерлерге қажет емес

$$$ 17

Әдетте Ethernet тар жолақты беріліс пен топологияны пайдаланады, оған қайсысы жатады?

A) жұлдыз

В) шина

C) сақина

D) жұлдызды сақина

E) ұяшықты

$$$ 18

Негізгі кабельдік сегментте трафикті реттеу үшін Ethernet-ке кірудің қандай әдісі қолданылады?

A) маркер беру

B) басым беріліс

C) сауалнама

D) CSMA / CA

E) CSMA / CD

$$$ 19

Token Ring желісіндегі маркер дегеніміз не?

A) биттердің алдын-ала анықталған реттілігі

В) аналогтық сигнал

C) мәліметтер

D) қабылдаушының адресі

E) қоректендіру көзінің адресі

$$$ 20

Ақаулы компьютер Token Ring желісіне қалай әсер етеді?

A) желілік үзілісті тудырады

В) маркердің қозғалысын және бүкіл желінің жұмысын тоқтатады

C) компьютер автоматты түрде сақинадан шығарылады

D) ақаулы компьютер желілік сақинадан қолмен ажыратылады

E) ақаулы компьютер маркерді өткізіп жібереді

$$$ 21

AppleTalk желілерін қалай бір үлкен желіге біріктіруге болады?

A) қайталағышты қолдану арқылы

В) қалаған аймақты таңдау арқылы

C) серверлік компьютерді қолдану арқылы

D) желілік адаптерді қолдану арқылы

E) баррель қосқышын қолдану арқылы

$$$ 22

ArcNet жұлдызды-шына топологиясына ие, сондықтан ол қандай енгізу әдісін қолданады:

A) маркер көмегімен беру

B) басым беріліс

C) сауалнама

D) CSMA / CA

E) CSMA / CD

$$$ 23

Модемнің өнімділігін қалай арттыруға болады?

A) деректерді беру жылдамдығын жоғарылату

В) телефон желісінің өткізу қабілеттілігін арттыру

C) синхронды байланысты қолдана отырып

D) деректерді сығу және кодтау әдістерін қолдану

E) асинхронды байланысты пайдалану

$$$ 24

Репетиторлар нені істей алмайды?

A) физикалық деңгейде қызымет жасау

В) сигналды күшейтуді

C) түрлі тасушыларды қолдана отырып сегменттерді қосуды

D) барлық трафикті екі бағытта да беруді

E) деректерді сүзгілеуді

$$$ 25

Көпірлерге көбірек қолданылатын мәлімдемені таңдаңыз:

A) бір уақытта бірнеше маршрутты қолданады

C) таратылатын хабарламаларды жіберімейді, оларды сүзгіден өткізеді

C) желіні сегментацияға байланысты трафикті азайту

D) белгісіз мекенжайлары бар пакеттерді өткізбеу

E) желілерді әртүрлі технологиямен байланыстырады

$$$ 26

Маршрутизаторлар келесі функцияларды орындай алады:

A) желіні қосып, деректер пакеттерін сүзгіден өткізу

В) қол жеткізуді басқарудың ішкі қабаттарының жергілікті мекен-жайларын тану

C) белгісіз мекен-жайы бар пакеттерді барлық бағытта таратады

D) желі деңгейінде және кез-келген желілік протоколдармен жұмыс істеу

E) желілерді әртүрлі технологиямен байланыстырады

$$$ 27

TCP / IP отбасы IP-нің қай деңгейінде орналасқан?

A) желілік интерфейс деңгейі

B) желілік қабат

C) көлік деңгейі

D) қолдану деңгейі

E) өкілді деңгей

$$$ 28

А класындағы мекен-жайлар желісінің идентификаторы үшін пайдаланылатын океттер саны

А) 1

В) 2

С) 3

D) 4

Е) 5

$$$ 29

В класының адрестік желінің идентификаторы үшін пайдаланылатын океттер саны

А) 1

В) 2

С) 3

D) 4

Е) 5

$$$ 30

C класының адрестік желісінің идентификаторы үшін пайдаланылатын океттер саны

А) 1

В) 2

С) 3

D) 4

Е) 5

$$$ 31

13.245.88.23 адресі қай класқа жатады?

А) А

В) В

С) С

D) D

Е) Е

$$$ 32

Келесі мекенжайлардың қайсысы алдын ала сақталған:

A) соңғы кластың мәні 240 болатын С класының адрестері

B) бірінші класстық мәні 130 болатын В класының адрестері

C) соңғы октет мәні 191 болатын В классының адрестері

D) бірінші класстық мәні 127 болатын А класындағы адрестер

E) бірінші океттің мәні 192 болатын С класының адрестері

$$$ 33

А класының желілік идентификаторлары үшін әдепкі ішкі желі маскасы қандай?

А) 0.0.0.0

В) 255.255.255.255

С) 255.255.255.0

D) 225.255.0.0

Е) 225.0.0.0

$$$ 34

В класының желілік идентификаторлары үшін әдепкі ішкі желі маскасы қандай?

А) 0.0.0.0

В) 255.255.255.255

С) 255.255.255.0

D) 225.255.0.0

Е) 225.0.0.0

$$$ 35

С класының идентификаторлары үшін әдепкі ішкі желі маскасы қандай?

А) 0.0.0.0

В) 255.255.255.255

С) 255.255.255.0

D) 225.255.0.0

Е) 225.0.0.0

$$$ 36

A класының желісі қанша түйінді торапты қалыпты ұстап тұра алады?

А) 254

В) 16 384

С) 65 534

D) 16 777 214

Е) 0

$$$ 37

В класының желісі қанша желіні қолдайды?

А) 254

В) 16 384

С) 65 534

D) 2 097 152

Е) 0

$$$ 38

С класының желісі қанша торапты қолдайды?

А) 254

В) 16 384

С) 65 534

D) 2 097 152

Е) 0

$$$ 42

ARP кэш жазбасы қанша уақытты алады?

A) 1 минут

C) 5 минут

C) 10 минут

D) 15 минут

E) 20 минут

$$$ 43

Төмендегі тұжырымдардың қайсысы сокетті ең жақсы сипаттайды?

A) Қашықтағы түйінде процестің орналасқан жерін көрсетуге қолданылатын сан

В) Қашықтағы түйінде процестің орналасқан жерін көрсету үшін қолданылатын порт нөмірі

C) Сервер құратын кездейсоқ сан, бұл қосымшаларға қашықтағы тораптағы процеске қол жеткізуге мүмкіндік береді

D) Қашықтағы түйіндегі қосымшаны немесе процеске енуді қамтамасыз ету үшін қолданылатын порт нөмірі мен IP адресінің тіркесімі

E) компьютердің адресі

$$$ 44

Төмендегі жауаптардың қайсысы ARP функцияларын дұрыс сипаттайды?

A) IP-адрестерге сәйкес келетін NetBIOS атауларын анықтау

В) пакеттерді желіге жіберу

C) биттерді байтқа түрлендіру

D) бағыттау кестесін құрады

E) IP адрестеріне сәйкес келетін аппараттық адрестерді анықтау

$$$ 42

ARP кэш жазбасы қанша уақытқа созылады?

А) 1 минут

В) 5 минут

С) 10 минут

D) 15 минут

Е) 20 минут

$$$ 43

Төмендегі тұжырымдардың қайсысы сокетті сипаттайды?

A) Қашықтағы түйінде процестің орналасқан жерін көрсетуге қолданылатын сан

В) Қашықтағы түйінде процестің орналасқан жерін көрсету үшін қолданылатын порт нөмірі

C) Сервер құратын кездейсоқ сан, бұл қосымшаларға қашықтағы тораптағы процеске қол жеткізуге мүмкіндік береді

D) Қашықтағы торапқа қосымшаны немесе қызметке кіруді қамтамасыз ету үшін қолданылатын порт нөмірі мен IP адрес тіркесімі

E) компьютердің адресі

$$$ 44

Төмендегі жауаптардың қайсысы ARP функцияларын дұрыс сипаттайды?

A) IP-адрестерге сәйкес келетін NetBIOS атауларын анықтау

В) пакеттерді желіге жіберу

C) биттерді байтқа түрлендіру

D) бағыттау кестесін құрады

E) IP адрестеріне сәйкес келетін аппараттық адрестерді анықтау

$$$ 45

TCP / IP деген не? (ең жақсы жауапты таңдаңыз)

A) Microsoft корпорациясы қарапайым пайдаланушыларға Интернеттегі ресурстарға қол жеткізуге мүмкіндік беру үшін әзірлеген хаттамалардың жиынтығы

В) Әр түрлі аппараттық платформаларда және әр түрлі желілерде жұмыс істейтін әртүрлі қосымшалармен әрекеттесуге мүмкіндік беретін хаттамалардың жиынтығы

C) Гетерогенді желілер арасында ақпаратты бағыттау үшін Майкрософт жасаған хаттама

D) IAB әртүрлі бағдарламалық және аппараттық өндірушілердің Интернетке қол жеткізе алатын протоколы.

E) АҚШ қорғаныс министрлігі өңдеге хаттама

$$$ 46

Ішкі желі маскасының ерекшеліктерін жақсы сипаттайтын жауапты таңдаңыз

A) Желілік маска TCP / IP адресіндегі IP мекенжайының бір бөлігін жасыру үшін қолданылады

В) Ішкі желі маскасы басқа TCP / IP түйіндерінің орналасуын анықтауға мүмкіндік береді

C) Ішкі желі маскасы TCP / IP хост идентификаторынан желі идентификаторын анықтауға көмектесу үшін қолданылады. Бұл басқа TCP / IP түйіндерін табуға көмектеседі.

D) TCP / IP желі идентификаторын хост идентификаторынан бөлуге көмектесу үшін ішкі желі маскасы қолданылады. Бұл басқа TCP / IP түйіндерінің IP адрестерін анықтауға көмектеседі.

E) Желілік маска TCP / IP желісіндегі басқа IP адрестерді анықтау үшін қолданылады.

$$$ 47

Сізде желіде бірнеше физикалық желілерге қосылған және маршрутизатор ретінде конфигурацияланған екі компьютер бар. Қашықтағы түйінде қай компьютер арқылы өту керектігін анықтаудың ең жақсы әдісі қандай?

A) екі компьютердің де бағыттау кестесін қарау

В) пакеттердің нақты жүретін бағытын анықтау үшін tracert қызметтік бағдарламаны іске қосыңыз

C) route утилитасын екі компьютерде де қолданыңыз

D) пакеттердегі адрестер туралы ақпаратты көру үшін көмекші мониторды іске қосыңыз

E) Ping утилитасын екі компьютерде де қолданыңыз

$$$ 48

Түйін атауларын анықтау әдістерінің қайсысы тұрақты мәтіндік файлды қолданады?

А) DNS

В) HOSTS

С) LMHOSTS

D) домендік аттар кеңістігі

Е) WINS

$$$ 49

Клиенттен келіп түскен атауды анықтауға арналған сұранысты орындау кезінде домендік атау жүйесін шарлау үшін атау сервері сұраудың қандай түрін қолданады?

A) Рекурсивті сұрау

В) Итерациялық сұрау

C) қайтару сұранысы

D) WINS

E) DNS

$$$ 50

Төменде NetBIOS атауларын анықтауға арналған алғашқы төрт қадам берілген:

1. В-сұранысын тарату

2. WINS

3. NetBIOS атауының кэші

4. LMHOSTS

Бұл қадамдар қандай ретпен орындалады?

А) 3,1,4,2

В) 2,3,1,4

С) 1,2,3,4

D) 3,2,1,4

Е) 1,2,4,3

$$$ 51

Сүзу маршрутизаторы:

A) әр хосттың аутентификациясын орындайды

B) желідегі барлық оқиғаларды түсіреді

C) ақпаратты шифрлау үшін қолданылады

D) деректерді сүзеді

E) брандмауэр компоненті

$$$ 52

Windows 2000 желілік тіркелгісінің қайсысы бірінші орнатылуы керек?

А) Guest

В) Special

С) Administrator

D) User

Е) Operator

$$$ 53

Компьютер қосылымын тексеру утилитасы дегеніміз не?

А) tracert

В) ping

С) netstat

D) IPconfig

Е) route

$$$ 54

Әдетте желідегі шлюздердің рөлі

A) арнайы құрылғылар

В) бөлінген серверлер

C) желідегі кез-келген компьютер

D) маршрутизатор

E) көпір

$$$ 55

Компания 9 бөлімшеден тұрады, олардың әрқайсысы өзінің ішкі желісін қажет етеді. Компания 130.121.0.0 желі идентификаторын алды. Құрылғыдағы 3000 түйінге дейін қолдауды қажет етеді. Сіз қандай масканы қолдануды ұсынар едіңіз?

А) 255.255.240.0

В) 255.255.255.0

С) 255.255.224.0

D) 255.255.248.0

Е) 255.255.0.0

$$$ 56

Келесі тұжырымдар қосылыстың үш сатылы ашылуының жеке кезеңдерін сипаттайды. Қай тұжырым дұрыс емес?

A) «Сізге менде ақпарат бар. Біз байланыс жасай аламыз ба?»

B) «Тамаша, мен сіздің жауабыңызды алдым. Міне, қалған ақпарат»

C) «Ия, мен байланысты ашуға дайынмын. Аударуды жалғастыру»

D) «Жоқ, мен қазір бос емеспін, сенде уақыт жоқ. Бірнеше минуттан кейін қайталап көріңіз.»

E) «Мен сіздің хабарламаңызды алдым, жалғастырыңыз.»

$$$ 57

Неліктен RIP бағыттау протоколын пайдалану кезінде маршрут ұзындығы 15 хоппен шектеледі?

A) маршрут кестесінде маршруттың ұзындығын сақтау үшін он алтылық кодтар қолданылады

В) үлкен желілер ішкі желіге бөлінеді

C) ешқандай желі ұзағырақ маршруттарды қажет етпеуі мүмкін

D) желі арқылы пакеттердің өту уақытын үнемдеуден

E) Шексіз айналымның пайда болуына жол бермеуге

$$$ 58

Сізге В класының желісін TCP / IP ішкі класына бөлу қажет. Сіз әр ішкі желіге қанша түйін қажет екенін анықтадыңыз. Желі үшін ішкі желі маскасын анықтау үшін қандай параметрді білу керек?

A) желілік топология

В) Дыбысты төмендету адресі

C) желідегі негізгі шлюздің адресі

D) маршрутизатордың адресі

E) ішкі желілердің нақты саны

$$$ 59

Сіздің компанияңыз 5 миллион тораптан тұратын жаңа интеграцияланған желі үшін IP-адресті әзірлеуде. Мұндай желіні орнатқан кезде қандай IP адрестерін пайдалану керек?

А) А класы

B) В класы

C) С класы

D) D класы

E) Е класы

$$$ 60

Сізге B ішкі сыныбында максималды түйіндер саны бар 120 ішкі желілерді қамтитын TCP / IP желісін орнату керек. Қандай ішкі желі маскасын қолдану керек?

А)255.255.192.0

В) 255.255.224.0

С) 255.255.248.0

D) 255.255.254.0

Е) 255.255.0.0

$$$ 61

Сіздің TCP / IP желіңіз әрқайсысы 4 ішкі және 30 түйіннен тұрады. Ішкі желілердің біреуі үшін IP адестерін автоматты түрде орнату керек. Сіз қандай құралды орнатып, орнатуыңыз керек?

А) DNS

В) DHCP

С) WINS

D) файл HOSTS

Е) файл LMHOSTS

$$$ 62

Сіздің компанияңызда C класты адресі бар: желіде 3 ішкі желі бар. Бір ішкі желідегі түйіндердің максималды санын қамтамасыз ететін ішкі желі маскасын таңдаңыз.

А) 255.255.192.0

В) 255.225.224.0

С) 255.255.255.192

D) 255.255.255.0

Е) 255.255.255.224

$$$ 63

Әрқайсысында 510 түйіннен тұратын 72 ішкі желісі бар желі үшін қай B маскасын таңдау керек?

А) 255.254.0.0.

В) 255.252.0.0.

С) 255.255.254.0

D) 255.255.252.0

Е) 255.255.255.0

$$$ 64

Сіздің TCP / IP желіңізде C класты адрес қолданылады, желіге тек бір ішкі желі қажет. Қажетті ішкі желі маскасын таңдаңыз.

А) 0.0.0.0.

В) 255.0.0.0.

С) 255.255.0.0.

D) 255.255.255.0

Е) 255.255.255.255

$$$ 66

Деректерді беруге жоғары жылдамдықты қамтамасыз етуге және оларды есту құралдарынан сақтау үшін не қажет, сіз қай кабельді таңдайсыз?

A) қалың коаксиалды

В) жұқа коаксиалды

C) бұралған жұп UTP

D) STP бұралған жұп

E) талшықты-оптикалық

$$$ 67

Пайдаланушы қосымшаларын тікелей қолдайтын қандай OSI деңгейі бар?

A) Физикалық

B) Арна

C) Желі

D) Сессия

E) Қолданбалы

$$$ 68

OSI моделінде неше деңгей бар?

A) тоғыз

C) сегіз

C) жеті

D) төрт

E) үш

$$$ 69

Сегменттерді әртүрлі желілік архитектуралармен байланыстыру қажет.Қандай желілік жабдықты таңдайсыз?

A) маршрутизатор

В) шлюз

C) көпір

D) репитор

Е) концентратор

$$$ 70

Қандай протокол мәліметтерді байланыс арқылы жібереді?

А) TCP

В) UDP

С) IP

D) ARP

Е) RARP

$$$ 71

Маршрутизатор кестесіне қандай жаңа бағдарлама қосуға болады? .

А) ping

В) trasert

С) inconfig

D) route

Е) arp

$$$ 72

Сіз Windows NT Server-де TCP / IP қолдауын орнатқыңыз келеді. Сізге орнату үшін ненің қажеті жоқ?

A) Сіз орнатқан компьютердегі жергілікті әкімшілер тобының мүшесі болуыңыз керек.

В) Сіз жеке компьютер орнатылған домен әкімшісі болуыңыз керек

C) Сіз жүйенің таралуына қол жеткізе алуыңыз керек

D) Сіз қандай параметрлерді жасау керектігін жақсы түсінуіңіз керек.

E) Сіз операциялық жүйелерді орната білуіңіз керек

$$$ 73

Берілген IP адресті 172.16.2.18 және 255.255.224.0 маскасын қолдана отырып, адрес қай класқа жататынын анықтаңыз, ішкі желі идентификаторлары мен хост идентификаторларын қаншаға орнатуға болады?

A) А класы, 14 ішкі желі және 254 түйін

B) В класы, 14 ішкі желі және 254 түйін

C) В класы, 6 ішкі желі және 8190 түйін

D) С класы, 6 ішкі желі және 8190 түйін

E) С класы, 14 ішкі желі және 8190 түйін

$$$ 74

Белгілі бір ішкі желі түйінінің IP адресі 198.65.12.67, ал осы ішкі желі үшін масканың мәні 255.255.255.192 болсын. Ішкі желі нөмірін анықтаңыз. Осы ішкі желідегі түйіндердің максималды саны қандай?

A) 64, 62 түйін ішкі торабы

B) ішкі желі нөмірі 32, 124 түйін

C) ішкі желі нөмірі 16, 132 түйін

D) ішкі желі нөмірі 96, 32 түйін

E) ішкі желі нөмірі 128, 16 түйін

$$$ 75

Желі топологиясы бар желіде жұмыс істемейді. Төмендегілердің қайсысы бұл ақаудың себебі бола алмайды?

A) желілік кабель дұрыс жалғанбаған немесе сынған

В) кабельдің созылуы сіздің желіге рұқсат етілген ең үлкен ұзындықтан асып кетті

C) желіде терминатор жоқ

D) концентратор бұзылды

E) желідегі бір компьютер бұзылған

$$$ 76

Желілік картаның қай тұжырымы дұрыс?

A) желілік карта компьютерден келетін сериялық деректерді параллель түрлендіреді

В) ең танымал 16 және 32 биттік желілік карталар

C) деректерді жіберуге көмектесетін желілік борттық компьютер барлық жадыны бөледі

D) деректер уақытша буферлік рөл атқаратын желілік тақтаның қабылдағышында уақытша сақталады

E) таратушы және қабылдайтын желілік карталар әр түрлі жылдамдықта жұмыс істей алады

$$$ 77

Windows NT желісіндегі домен деген не?

A) жалпы мәліметтер базасы мен қауіпсіздік саясатын қолданатын компьютерлердің физикалық қоры

В) оңай қол жеткізу үшін бірнеше компьютерді біріктіретін папка

C) жалпы мәліметтер базасы мен қауіпсіздік саясатын қолданатын компьютерлердің логикалық үйлесімі

D) желіде орналасқан компьютерлер адресі

E) Windows NT орнату кезінде анықталған контроллер

$$$ 78

Желінің жұмысын жақсарту үшін желіні жаңартудың қажеті жоқ

A) сервер

B) жұмыс станциясы

C) желілік адаптер карталары

D) тарату ортасы

E) домен

$$$ 79

Телефон байланысында қолданылатын аналогты желілер (стандартты дауыстық арналар) \_\_\_\_\_\_\_\_\_\_\_\_\_ желілері деп те аталады

A) комутациялық

В) тікелей сандық

C) кез-келгенімен

D) жалға алынған сызықтар

E) сандық

$$$ 80

Сығымдау арқасында деректерді жіберуге кететін уақытты азайтады, ол ненің көмегімен орындалады?

A) маршруттардың санын азайту

В) артық элементтерді алып тастау

C) сызықты интерференцияны басу

D) Беріліс арасындағы уақытты азайту

E) мәліметтерді өңдеу уақытын қысқарту

$$$ 81

Маршруттық кесте

A) жеке адреске жіберілген хабарларды қолдайды

В) пакеттерді дұрыс адресаттағы қайталаушыларға жібереді

C) компьютерлер мен желілердің адрестерін сақтайды

D) әр активтенетін компьютерге адрестер береді

E) мәліметтерді сүзеді

$$$ 82

Көпірлер мен маршрутизаторлардың басты айырмашылығы мынада

A) көпірлер көптеген маршруттардың арасынан таңдай алады

В) көпірлер Ethernet-ті қолдайды, бірақ Token Ring-ті қолдамайды

C) маршрутизаторлар Ethernet-ті қолдайды, бірақ Token Ring-ті қолдамайды

D) маршрутизаторлар көптеген маршруттардың арасынан таңдай алады

E) көпір тек маршруттық хаттамамен жұмыс істейді

$$$ 83

LMHOSTS файлын пайдалану кезінде туындауы мүмкін ақауды қай мәлімдемеде сипаттамайды?

A) LMHOSTS файлы жүйелік дискінің түбірлік каталогында орналаспайды

В) LMHOSTS файлы қате атпен сақталған немесе кеңейтімі дұрыс емес

C) файлдағы жазба қатемен жазылады

D) бірдей NetBIOS атауы үшін екі түрлі жазба бар, ал бірінші пайда болған қате.

E) \* .txt кеңейтілімімен сақталған LMHOSTS файлы

$$$ 84

DHCP қолданудың артықшылығы неде?

A) NetBIOS атауын динамикалық тіркеу

В) IP атауларын орталықтандырылумен анықтау

C) сіз қай компьютердің қай адреске жататынын әрдайым қадағалай аласыз

D) барлық операциялық жүйелер қолдайды

E) динамикалық IP параметрі

$$$ 85

DHCP жалға беру процесі қандай тәртіппен жүреді?

А) сұрау, растау, ұсыныс, таңдау

В) сұрау, ұсыныс, таңдау, растау

C) сұрау, ұсыныс, сайлау, таңдау

D) сайлауды, таңдауды, растауды сұрау

E) ұсыныс, таңдау, сұрау, растау

$$$ 86

WINS қолданудың артықшылығы неде?

A) NetBIOS атауын динамикалық тіркеу

В) IP атауларын орталықтандырылумен анықтау

C) сіз қай компьютердің қай адреске жататынын әрдайым қадағалай аласыз

D) барлық операциялық жүйелер қолдайды

E) динамикалық IP параметрі

$$$ 87

Тарату ортасына қатысты қай тұжырым дұрыс?

A) жұқа коаксиалды кабель жуанға қарағанда жеңілірек және икемді болғандықтан, сигналдарды әрі қарай әрі жылдам қабылдайды

В) талшықты-оптикалық кабель әдетте RJ-45 коннекторларын пайдаланады

C) UTP үшін максималды ұзындығы шамамен 100 м.

D) қалың коаксиалды кабель желілік трафикті орталықтандырады

E) шашыраңқы инфрақызыл сәулемен, сигнал шағылысуының әсері алдын алады

$$$ 88

Пакеттің құрылымына қатысты қай тұжырым дұрыс?

A) пакеттік тақырыпта әдетте CRC деп аталатын қателерді тексеру туралы ақпарат болады

B) пакеттік тіркемеде баратын жердің адресі болады

C) пакетте бөлгіш қоректендіру көзінің адресі көрсетеді.

D) маркер - сақинаның айналасында айналатын пакеттің ерекше түрі

E) пакетте бастапқы адрес көрсетілмейді.

$$$ 89

Серверге негізделген желілер үшін қай мәлімдеме қабылданбайды?

А) шектеулі болуы керек ресурстар немесе мәліметтер қол жетімді

В) желі жетілдірілген деректерді қорғауды қажет етеді

C) желіде бүкіл желілік саясатты басқаратын бас әкімші бар

D) желі қызмет көрсететін пайдаланушылар саны 10-нан асады

E) пайдаланушылар желіні басқару және басқарумен дербес айналысады

$$$ 90

Ақауды шешудің қарапайымдылығы мен минималды құны қажет, осыған сәйкес Сіз қай кабельді таңдайсыз?

A) қалың коаксиалды

В) жұқа коаксиалды

C) UTP бұралған жұп

D) STP бұралған жұп

E) талшықты-оптикалық

$$$ 91

Қол жеткізу әдістеріне қатысты қай тұжырым дұрыс?

А) бірнеше компьютерлердің бір уақытта кабельге кіруіне жол бермеу үшін қол жеткізу әдістері қолданылады

В) деректерді беру кезінде CSMA / CD пайдалану кезінде бірнеше компьютер өз мәліметтерін бере алады

C) сұраныс басымдылығы бойынша қол жеткізу әдісімен, беріліс желідегі барлық компьютерлерге таратылады

D) маркерді кез-келген уақытта берудің қол жетімді әдісімен бірнеше компьютер маркерді қолдана алады

E) қол жетімділік белгісі маркермен соқтығысуды болдырмауға мүмкіндік беретін кодты қолдану арқылы қақтығыстардың алдын алады

$$$ 92

Жіңішке коаксиалды кабельдегі сегментті Ethernet 10BaseT желісіне қосқыңыз келсе, сізге қажет оңтайлы желілік жабдық пен бөлшектерді таңдаңыз:

A) баррелл-коннектор

В) репортер

C) көпір

D) маршрутизатор

E) шлюз

$$$ 93

Бірнеше сегменттер арасындағы трафикті оқшаулап, сүзгілеу қажет болса, сізге оңтайлы желілік жабдық пен бөлшектерді таңдаңыз

A) баррелл-коннектор

В) репортер

C) көпір

D) маршрутизатор

E) шлюз

$$$ 94

Егер сізге әртүрлі жүйелер арасында байланыс қажет болса, оңтайлы желілік жабдық пен бөлшектерді таңдаңыз (Microsoft-тың Novell-ге кіруі)

A) баррелл-коннектор

В) репортер

C) көпір

D) маршрутизатор

E) шлюз

$$$ 95

Желідегі ақпаратты қорғауға қатысты қай мәлімдеме дұрыс емес?

A) деректер қауіпсіздігі желілік жабдықты қорғаудан басталуы керек.

В) қол жеткізу құқығы арқылы қорғау - бұл әр пайдаланушыға белгілі бір құқықтарды беру.

C) пайдаланушының аутентификациясы процесі - бұл пайдаланушының аутентификация процесі

D) қол жеткізу құқығын тағайындаудың ең тиімді әдісі - топтарды пайдалану

E) топтарға жеке пайдаланушыларға бірдей қол жеткізу құқығы берілуі мүмкін

$$$ 96

Төмендегі мәлімдемелердің қайсысы парольмен қорғалған ортақ ресурстарды сипаттайды?

A) парольдер желілік ресурстарға тағайындалады

В) әр пайдаланушыға пароль беріледі

C) желілік қауіпсіздіктің ең жоғары деңгейін қамтамасыз етеді

D) топтық артықшылықтарды берудің қарапайым әдісі

E) желідегі әрбір компьютерге пароль беріледі

$$$ 97

Сіз DHCP серверіңізді ішкі желідегі клиенттік компьютердің IP адрестарын автоматты түрде бөлетін етіп конфигурацияладыңыз. Клиенттік компьютерлер әрдайым IP-адресін жалға алғаннан кейін дәл 1 күн өткенде оны жаңартуға тырысуы үшін не істеу керек?

A) DHCP көлемін құрыңыз, уақыт аралығын 1 күнге орнатыңыз, жаңарту кезеңі - 50%

B) DHCP көлемін құрыңыз, уақыт аралығын 2 күнге орнатыңыз және әдепкі жаңарту кезеңін қалдырыңыз

C) DHCP көлемін құрыңыз, уақыт аралығын 24 сағатқа орнатыңыз және әдепкі жаңарту кезеңін қалдырыңыз

D) DHCP көлемін құрыңыз, уақыт аралығын 2 күнге орнатыңыз және жаңарту кезеңі 100% құрайды

E) DHCP көлемін құрыңыз, уақыт аралығын 24 сағатқа орнатыңыз, және

жаңарту кезеңі - 100%

$$$ 98

Компьютер LNHOSTS файлын және WINS серверін атауларды кеңейту үшін пайдалануға келтірілген. Басқа компьютерге қалай қосылуға болады?

A) басқа компьютердің MAC адресін көрсету керек

В) желі маршрутизаторының IP адресін көрсету керек

C) басқа компьютердің шлюз адресін көрсетіңіз

D) басқа компьютердің адресін көрсетіңіз

E) басқа компьютердің NetBIOS атауын көрсетіңіз

$$$ 99

Деректер форматын аударуға және ығыстыруға жауап беретін қызметтер қандай OSI деңгейіне сәйкес келеді?

A) Қолданбалы

В) Өкіл

C) Сеансты

D) Көлік

E) Желі

$$$ 100

Бағдарламалар немесе процестер арасындағы байланысты орнатуға, қолдауға және тоқтатуға арналған қызметтер OSI қандай деңгейде?

A) Қолданбалы

В) Өкіл

C) Сеансты

D) Көлік

E) Желі

$$$ 101

Серверге негізделген желілер үшін не дұрыс?

А) тең құқылы желілерге қарағанда сенімді қорғау мен бақылауды қамтамасыз етпейді

В) пайдаланушылар саны 10-нан аспайтын желілер үшін ұсынылады

C) қуатты орталық сервер қажет емес

D) пайдаланушылар әдетте кішкене аумаққа таралады

E) мыңдаған қолданушыларды қолдауға қабілетті

$$$ 102

Жұлдызды топологиямен бұралған жұптық желіні ұзартуға қандай құрал көмектеседі?

A) желілік адаптер картасы

В) терминатор

C) дерктерді беру ортасында модулдің қосылуы

D) баррель-коннектор

E) концентратор

$$$ 103

OSI үлгісінде пакеттерді кадрларға қайта орау қай деңгейде орындалады?

A) Физикалық

B) Арна

C) Желі

D) Көлік

E) Өкіл

$$$ 104

Transport Layer қай протокол?

А) IPX

В) Telnet

С) UDP

D) IGMP

Е) FTP

$$$ 105

Деректерді жібермес бұрын, компьютер деректерді жіберу ниеті туралы хабарлама жібереді. Олар қандай қатынау әдісін қолданады?

A) CSMA / CA

B) маркер берумен

C) сауалнама

D) басымдық бойынша

E) CSMA / CD

$$$ 106

TokenRing әдетте тар жолақты беріліс пен топологияны пайдаланады.

A) жұлдыз

В) шина

C) сақина

D) жұлдызды сақина

E) ұяшық

$$$ 107

Token Ring трафикті реттеу үшін қандай қол жетімді әдісті қолданады?

A) маркер беру

B) басым беріліс

C) сауалнама

D) CSMA / CA

E) CSMA / CD

$$$ 108

Ақаулы компьютер ArcNet желісіне қалай әсер етеді?

A) желілік үзіліс бар

В) маркердің қозғалысын және бүкіл желінің жұмысын тоқтатады

C) ақаулы компьютер желілік сақинадан қолмен ажыратылады

D) желі жұмысын жалғастырады

E) ақаулы компьютер маркерді өткізіп жібереді

$$$ 109

Репетиторлар:

A) Желі деңгейінде жұмыс істейді

В) сигналды күшейтеді

C) әртүрлі технологияларды қолдана отырып сегменттерді қосады

D) барлық трафикті тек бір бағытта өткізеді

E) деректерді сүзгілейді

$$$ 110

Көпірлерге қатысты емес мәлімдемені таңдаңыз:

A) бір уақытта бірнеше маршрутты қолданады

В) хабар тарату хабарламаларын өткізіп жібереді

C) желіні сегментацияға байланысты трафикті азайтады

D) белгісіз адрестері бар пакеттерді береді

E) желілерді әртүрлі тасымалдаушыларға қосады

$$$ 111

Маршрутизаторлар келесі функцияларды орындай алмайды:

A) желіні қосып, деректер пакеттерін сүзгіден өткізуді

В) бір уақытта бірнеше маршрутты қолдануды

C) таратылатын хабарламаларды жіберіп алмау

D) Желі деңгейінде және кез-келген желілік протоколдармен жұмыс істеу

E) желілерді әртүрлі тасымалдаушыларға қосады

$$$ 112

TCP / IP құамы қай деңгейде орналасқан?

A) желілік интерфейс деңгейі

B) желілік қабат

C) көлік деңгейі

D) қолдану деңгейі

E) өкілді деңгей

$$$ 113

Windows сокет TCP / IP тобының қай деңгейінде орналасқан?

A) желілік интерфейс деңгейі

B) желілік қабат

C) көлік деңгейі

D) қолдану деңгейі

E) өкілді деңгей

$$$ 114

D класының желілік идентификаторлары үшін әдепкі ішкі желі маскасы қандай?

А) 0.0.0.0

В) 255.255.255.255

С) 255.255.255.0

D) 225.255.0.0

Е) 225.0.0.0

$$$ 115

Қай Windows 2000 желілік тіркелгісі ең аз артықшылықтарға ие?

А) Guest

В) Special

С) Administrator

D) User

Е) Operator

$$$ 116

Компьютер конфигурациясын тексеру утилитасы дегеніміз не?

А) tracert

В) ping

С) netstat

D) IPconfig

Е) route

$$$ 117

TCP / IP моделінде неше деңгей бар?

A) тоғыз

В) сегіз

C) жеті

D) үшеу

E) төрт

$$$ 118

Желідегі ақпаратты қорғауға қатысты қай тұжырым дұрыс?

A) мәліметтер қауіпсіздігі бағдарламалық қамтамасыздандырудан басталуы керек.

В) қол жеткізу құқығымен қорғау - бұл әр қолданушыға пароль беру.

C) пайдаланушының аутентификация процесі - бұл пайдаланушының аутентификация процесі

D) қол жеткізу құқығын тағайындаудың ең тиімді әдісі - топтарды пайдалану

E) топтарға жеке пайдаланушылар сияқты бірдей қол жеткізу құқығы берілмейді

$$$ 119

Модемдерге қатысты қай тұжырым дұрыс?

А) таратушы жағында модем компьютердің сандық сигналдарын аналогқа айналдырады

В) беріліс дегеніміз - телефон желісі бойынша биттік деректерді тасымалдайтын сандық толқынның модуляция жиілігін білдіреді

C) жылдамдығы секундына бит жылдамдығынан жоғары болуы мүмкін

D) сыртқы модем - бұл параллель кабель арқылы компьютерге қосылған кішкене қорап

E) коммутация байланысы үшін кәдімгі телефон байланысы желілерін ғана қолданады

$$$ 120

Модемдерге қатысты қай тұжырым дұрыс емес?

А) таратушы жағында модем компьютердің сандық сигналдарын аналогқа айналдырады

В) баған дегеніміз - телефон желісі бойынша бит деректерін тасымалдайтын дыбыстық толқынның модуляция жиілігін білдіреді

C) жылдамдығы секундына бит жылдамдығынан жоғары болуы мүмкін

D) сыртқы модем - бұл компьютерге сериялық кабель арқылы қосылған кішкене қорап

E) модемдік байланыс үшін тек кәдімгі телефон (коммутатор) және жалға алынған (жалға алынған) желілерді пайдалану

$$$ 121

Көп пайдаланушыларды басқару үшін администратор қандай есептік жазбаны жасайды?

A) пайдаланушылардың есептік жазбалары

В) топтық есептік шоттар

C) Администраторлардың есептік шоттары

D) қонақтардың есептік шоттары

E) операторлық есептік шоттар

$$$ 122

Бірыңғай желінің деректеріне толық ену қандай деңгейде орындалады?

A) домен

B) қолданушы

C) пароль

D) құрылғылар

E) ресурс

$$$ 123

Деректердің жоғалуын болдырмауға қандай әрекет көмектеседі?

A) мәліметтерді репликациялау

C) мәліметтер аудиті

C) парольмен қорғау

D) резервтік көшірме

E) мәліметтерге қол жеткізуге тыйым салу

$$$ 124

Кішкентай желіде сіз әр түрлі сегменттерге қосылған бірнеше желілік адаптері бар компьютерге серверлік ОЖ орнаттыңыз. Желілік сегменттер арасында динамикалық бағыттауды қамтамасыз ету керек. Қай әдісті қолдану керек?

А) OSPF

В) RIP

С) ROUTE

D) HOSTS

Е) DHCP

$$$ 125

Кішкентай желіде сіз әр түрлі сегменттерге қосылған бірнеше желілік адаптері бар компьютерге серверлік ОЖ орнаттыңыз. Сізге желі сегменттерінің арасында тұрақты маршруттау қажет. Қай әдісті қолдану керек?

А) OSPF

В) RIP

С) ROUTE

D) HOSTS

Е) DHCP

$$$ 126

Сіздің желіңіз компьютер атауларын анықтау үшін таратылатын хабарларды пайдаланады. Microsoft осындай хабарламаларға деген қажеттілікті қалайша шектей алады?

A) DNS серверін орнатыңыз

В) DHCP агентін орнатыңыз

C) DHCP серверін орнату

D) сенімді WINS агентін орнатыңыз

E) WINS серверін орнату

$$$ 127

Қай тұжырым дұрыс емес?

A) Желілік анализаторлар OSI Физикалық деңгейінде жұмыс істейді, өйткені осы жағдайда желілік ақаулар көп пайда болады

В) желілік ақаулардың көпшілігі OSI физикалық қабатында пайда болады

C) қателіктерді жеңуге тырысатын желілік протоколдар кейде желілік ақауларды жасыра алады

D) желіні бақылау бағдарламасы желінің жұмысындағы кейбір тенденцияларды анықтауы мүмкін

E) FTP утилитасы OSI қолданбалы қабатында жұмыс істейді

$$$ 128

Қай тұжырым дұрыс?

A) Желілік анализаторлар OSI Физикалық деңгейінде жұмыс істейді, өйткені осы жағдайда желілік ақаулар көп пайда болады

В) желілік ақаулардың көпшілігі OSI физикалық қабатында пайда болады

C) қателіктерді жеңуге тырысатын желілік протоколдар кейде желілік ақауларды жасыра алады

D) желіні бақылау бағдарламасы желінің жұмысындағы кейбір тенденцияларды анықтауы мүмкін

E) FTP утилитасы OSI қолданбалы қабатында жұмыс істейді

$$$ 129

Дауыстық коммутациялық телефонды желілер:

A) арзан бола тұра жалдамалы талшықты-оптикалық жылдамдықпен бірдей жылдамдығықа ие

В) кеңінен қолданылады, бір сеанстан екінші сеансқа дейін байланыс арнасының тұрақты сапасын қамтамасыз етпейді

C) шектеулі мөлшерде болады, сондықтан олардың құны жоғары

D) компьютерлерге қол жетімділікті қамтамасыз ету үшін синхронды модемдерді қолданады

E) компьютерлерге қол жетімділікті қамтамасыз ету үшін жоғары жылдамдықты, баррель-коннекторын пайдаланады

$$$ 130

T1 технологиясы мыналарды ұсынады:

A) Т3 қатарларын ауыстырудың арзан әдісін

В) беру жылдамдығы 45 Мбит / с

C) үнемі мыс сым негізінде АТМ үнемі қосылу

D) 1,54 Мбит / с жылдамдықпен нүктелі-нүктелі толық дуплексті беріліс

E) 54 Мбит / с беру жылдамдығы

$$$ 131

Frame relay - бұл ең үнемді маршрут бойынша \_\_\_\_\_\_\_\_\_\_\_\_\_ жіберетін нүкте-нүкте жүйесі

A) Арна деңгейіндегі айнымалы ұзындықтың рамалары

В) Арна деңгейіндегі бекітілген ұзындықтың рамалары

C) физикалық деңгейдегі айнымалы ұзындықтағы пакеттер

D) Физикалық қабаттағы ұзындықтағы пакеттер

E) Желі қабатындағы тұрақты диаграммалар

$$$ 132

ARP кэшіндегі статикалық жазбаны қандай жағдайларда жоюға болады ?

A) осы жазба үшін arp-а командасын орындау кезінде

В) осы жазба үшін arp -g командасын орындау кезінде

C) осы жазба үшін arp -s командасын орындау кезінде

D) осы жазба үшін arp -N командасын орындау кезінде

E) компьютерді сөндіргенде

$$$ 133

ARP прокси қолдану кезінде қандай адресті қолданады?

А) жергілікті адресті анықтау

В) адрестерді кинетикалық анықтау

C) қашықтағы адрестерді анықтау

D) адрестерді бағыттаушымен анықтау

E) статикалық адресация

$$$ 134

TCP / IP түйіндерін сәйкестендіру үшін түйіндер атауларын қолданудың артықшылығы неде?

А) IP-адрестерге қарағанда түйін аттарын есте сақтау оңайырақ

В) түйін атаулары бір компьютерге бірнеше IP адрес тағайындауға мүмкіндік береді

C) әріптер мен сандардан тұратын түйін атаулары IP адрестерге қарағанда мағыналы болуы мүмкін

D) компьютерлерді сәйкестендіру үшін түйін атауларын пайдалану IP адрес пен компьютердің орналасқан жерін соңғы пайдаланушы үшін айқын болуына мүмкіндік береді

E) түйін атаулары компьютерді оныңфизикалық орналасқан жеріне қарамастан табуға мүмкіндік береді

$$$ 135

Түйін атауларында қандай таңбалар жиынтығын қолдануға болмайды?

А) A-Z

В) a-z

С) 0-9

D) & ! \* \_

Е) - .

$$$ 136

Түйін атауларында қандай таңбаларды қолдануға болады?

A) сандар

В) &

С) !

D)\*

Е) \_

$$$ 137

Төмендегі командалардың қайсысы HOSTS файлын көрмейді?

А) ping

В) net view

С) telnet

D) ftp

Е) tracert

$$$ 138

WINS атаулардың қандай түрлері DNS серверін анықтауға көмектеседі?

A) FQDN

В) домендік атаулар

C) түйін атаулары

D) желілік атаулар

E) түбір атаулары

$$$ 139

Төмендегілердің қайсысы динамикалық бағыттауға қолданылмайды?

A) маршрутизаторлар мәліметтерді бөліседі

В) RIP қажет

C) OSPF талап етеді

D) Бағыттау кестелеріне қолмен қолдау көрсетіледі

E) үлкен желілерде қолдану орынды

$$$ 140

Төмендегі өрістердің қайсысы статикалық бағыттау кестесінде жоқ?

A) метрикалық

B) желінің адресі

C) ішкі желі маскасы

D) шлюз мекен-жайы

E) бастапқы түйіннің IP-адресі

$$$ 141

Қандай тұжырым жалпы адресаттың мәселелерін сипаттайды?

A) түйінде желінің дұрыс емес идентификаторы орналасқан

В) DNS түйіні қолдану үшін құрылмаған

C) түйін сол желідегі басқа түйіндер сияқты бірдей желі идентификаторын қолданады.

D) түйін WINS қолдану үшін құрымаған

E) түйін HOSTS қолдану үшін құрымаған

$$$ 142

11111001 октеттің ондық мәні қандай

A) 224

В) 249

С) 225

D) 247

Е) 248

$$$ 143

192.15.2.0 адресі қай класқа жатады?

А) А

В) В

С) С

D) D

Е) E

$$$ 144

224.5.10.1 адресі қай класқа жатады?

А) А

В) В

С) С

D) D

Е) E

$$$ 145

130.29.88.7 адресі қай класқа жатады?

А) А

В) В

С) С

D) D

Е) E

$$$ 146

Әр жауапта OSI модельдерінің деңгейі және оларға сәйкес TCP / IP модельдері берілген. Қай жауап дұрыс емес?

A) OSI: қолданбалы, өкіл, сеансты; TCP / IP: қолданбалы қабат

B) OSI: көлік; TCP / IP: көлік қабаты

C) OSI: желі; TCP / IP: желілік интерфейс қабаты

D) OSI: арна, физикалық; TCP / IP: желілік интерфейс қабаты

E) OSI: желі; TCP / IP: шлюз

$$$ 147

Пакеттік бағыттауға OSI моделінің қай деңгейі жауап береді?

A) Физикалық

B) Арна

C) Желі

D) Көлік

E) Өкіл

$$$ 148

OSI моделінің аппараттық және сигналдық ерекшеліктері қандай деңгейде анықталады?

A) Физикалық

B) Арна

C) Желі

D) Көлік

E) Өкіл

$$$ 149

192.168.24.64 адресі 255.255.255.224 маскасымен қандай түйін ішкі желіге жатпайды?

А) 192.168.24.65

В) 192.168.24.75

С) 192.168.24.85

D) 192.168.24.95

Е) 192.168.24.105

$$$ 150

202.121.74.37 адресі 255.255.255.224 маскасымен түйін арқылы біркелкі ішкі желіде қай түйінде орналасқан?

А) 202.121.74.5

В) 202.121.74.10

С) 202.121.74.15

D) 202.121.74.25

Е) 202.121.74.35

**Тесттің кілттері**

|  |  |  |
| --- | --- | --- |
| Сұрақ нөмірі | Қиындық деңгейі | Дұрыс жауап |
| 1 | 1 | В |
| 2 | 1 | С |
| 3 | 1 | D |
| 4 | 1 | А |
| 5 | 2 | D |
| 6 | 2 | С |
| 7 | 1 | А |
| 8 | 2 | Е |
| 9 | 2 | В |
| 10 | 2 | В |
| 11 | 3 | A |
| 12 | 3 | E |
| 13 | 2 | С |
| 14 | 1 | D |
| 15 | 1 | В |
| 16 | 1 | D |
| 17 | 1 | В |
| 18 | 2 | Е |
| 19 | 1 | А |
| 20 | 2 | С |
| 21 | 3 | В |
| 22 | 2 | В |
| 23 | 2 | D |
| 24 | 2 | Е |
| 25 | 3 | С |
| 26 | 3 | А |
| 27 | 2 | В |
| 28 | 1 | А |
| 29 | 1 | В |
| 30 | 1 | С |
| 31 | 1 | А |
| 32 | 3 | D |
| 33 | 2 | Е |
| 34 | 2 | D |
| 35 | 2 | С |
| 36 | 2 | D |
| 37 | 2 | В |
| 38 | 2 | А |
| 39 | 2 | С |
| 40 | 3 | В |
| 41 | 2 | Е |
| 42 | 2 | С |
| 43 | 3 | D |
| 44 | 3 | Е |
| 45 | 2 | В |
| 46 | 3 | D |
| 47 | 2 | В |
| 48 | 3 | С |
| 49 | 3 | А |
| 50 | 3 | D |
| 51 | 3 | Е |
| 52 | 2 | С |
| 53 | 2 | B |
| 54 | 3 | С |
| 55 | 3 | А |
| 56 | 3 | D |
| 57 | 3 | Е |
| 58 | 3 | Е |
| 59 | 1 | А |
| 60 | 3 | D |
| 61 | 2 | В |
| 62 | 3 | Е |
| 63 | 3 | С |
| 64 | 2 | С |
| 65 | 3 | А |
| 66 | 1 | Е |
| 67 | 1 | Е |
| 68 | 1 | С |
| 69 | 2 | В |
| 70 | 2 | A |
| 71 | 2 | D |
| 72 | 2 | В |
| 73 | 3 | С |
| 74 | 3 | А |
| 75 | 1 | D |
| 76 | 2 | В |
| 77 | 2 | С |
| 78 | 2 | Е |
| 79 | 2 | А |
| 80 | 2 | В |
| 81 | 2 | С |
| 82 | 2 | D |
| 83 | 3 | А |
| 84 | 3 | Е |
| 85 | 3 | В |
| 86 | 3 | А |
| 87 | 1 | С |
| 88 | 2 | D |
| 89 | 1 | Е |
| 90 | 1 | С |
| 91 | 1 | А |
| 92 | 1 | В |
| 93 | 1 | D |
| 94 | 1 | Е |
| 95 | 2 | С |
| 96 | 2 | А |
| 97 | 3 | В |
| 98 | 3 | D |
| 99 | 2 | В |
| 100 | 2 | С |
| 101 | 1 | Е |
| 102 | 1 | Е |
| 103 | 1 | В |
| 104 | 1 | C |
| 105 | 2 | А |
| 106 | 2 | С |
| 107 | 2 | A |
| 108 | 2 | D |
| 109 | 1 | В |
| 110 | 1 | А |
| 111 | 2 | D |
| 112 | 2 | B |
| 113 | 2 | D |
| 114 | 1 | B |
| 115 | 1 | А |
| 116 | 1 | D |
| 117 | 1 | Е |
| 118 | 1 | D |
| 119 | 1 | А |
| 120 | 1 | С |
| 121 | 1 | В |
| 122 | 2 | Е |
| 123 | 1 | D |
| 124 | 3 | В |
| 125 | 3 | С |
| 126 | 2 | Е |
| 127 | 2 | А |
| 128 | 2 | С |
| 129 | 2 | В |
| 130 | 3 | D |
| 131 | 3 | А |
| 132 | 3 | Е |
| 133 | 3 | С |
| 134 | 3 | В |
| 135 | 2 | D |
| 136 | 2 | А |
| 137 | 3 | В |
| 138 | 3 | C |
| 139 | 1 | D |
| 140 | 2 | Е |
| 141 | 3 | А |
| 142 | 1 | В |
| 143 | 1 | С |
| 144 | 1 | D |
| 145 | 1 | В |
| 146 | 2 | С |
| 147 | 1 | С |
| 148 | 1 | А |
| 149 | 3 | Е |
| 150 | 3 | Е |