



Д.Б. Кенебаева  
Д.Б. Бекенова

# КОМПЬЮТЕРЛІК ЖЕЛІЛЕР

## ОҚУ ҚҰРАЛЫ



Нур-Султан, 2021

Кенебаева Д.Б., Бекенова Д. Б.

**КОМПЬЮТЕРЛІК ЖЕЛІЛЕР**

Оқу құралы

69364

Нұр-Сұлтан, 2021

ӘОЖ 004.77  
КБЖ 32.971.3  
К 35

**Пікір берушілер:**

Оразбаев Б. Б. - т.ғ.д., профессор, Л.Н.Гумилев атындағы ЕҰҰ,  
Тазабеков И.И. - т.ғ.д., профессор, С.Сейфуллин атындағы ҚазАТУ,  
Еслямов С.Г. - т.ғ.к., профессор, «Тұран-Астана» университеті

Кенебаева Д. Б.  
К 35 Компьютерлік желілер. Оқу құралы/ Д.Б. Кенебаева, Бекенова Д.Б.  
Нұр-Сұлтан қаласы: «Тұран-Астана» университеті, 2021.-105 бет.

ISBN 978-601-7616-29-8

Оқу құралы 5В070300-"Ақпараттық жүйелер", 5В070400-"Есептеу техникасы және бағдарламалық қамтамасыз ету" мамандықтары бойынша бакалаврларды оқыту бағдарламасының оқу жоспарында қарастырылған жұмыс бағдарламасына сәйкес әзірленген.

Оқу құралы Cisco бойынша зертханалық жұмыстардан (Cisco Packet Tracer интерфейсі, симуляция режимі, Желілік қызметтер, Cisco IOS операциялық жүйесінің негізгі командалары, статикалық маршруттау, VLAN виртуалды жергілікті желілері, ACL (Access Control List) қатынауды басқару) тұрады.

ӘОЖ 004.77  
КБЖ 32.971.3

ISBN 978-601-7616-29-8

© Д.Б.Кенебаева, Д.Б.Бекенова, 2021 ж.  
© «Тұран-Астана» университеті

## Мазмұны

Кіріспе	5
1 Бөлім. Cisco Packet Tracer интерфейсі	8
1.1. Cisco Packet Tracer негізгі терезесі	8
1.2. Cisco Packet Tracer байланыс жабдықтары мен желілері	10
1.3. Жабдықтың физикалық жиынтығы	14
Бақылау сұрақтары	16
2 Бөлім. Симуляция режимі	17
Зертханалық жұмыс №1. Cisco Packet Tracer-де симуляция режимі	17
Бақылау сұрақтары	22
3 Бөлім. Желілік қызметтер	23
Зертханалық жұмыс №2. Желілік сервистерді баптау	24
Бақылау сұрақтары	29
4 Бөлім. Cisco IOS операциялық жүйесінің негізгі командалары	30
Зертханалық жұмыс №3. IOS командаларымен танысу	32
Бақылау сұрақтары	37
5 Бөлім. Статикалық маршруттау	38
Зертханалық жұмыс №4. Статикалық маршруттауды реттеу	40
Зертханалық жұмыс №5. Маршруттау кестелерін құру	43
№ 1 өзіндік жұмыс	44
Бақылау сұрақтары	44
6 Бөлім. Динамикалық маршруттау	46
Зертханалық жұмыс №6. Rip протоколын теңшеу	47
Зертханалық жұмыс №7. Корпоративтік желіде RIP хаттамасын теңшеу	49
№2 өзіндік жұмыс	51
Зертханалық жұмыс №8. OSPF протоколын теңшеу	53
Бақылау сұрақтары	54
7 Бөлім. NAT қызметі	55
Зертханалық жұмыс №9. NAT желілік жекен-жайын түрлендіру	57
Бақылау сұрақтары	60
8 Бөлім. VLAN виртуалды жергілікті желілері	61
Зертханалық жұмыс № 10. Бір Cisco коммутаторында VLAN орнату	64
Зертханалық жұмыс № 11. Екі Cisco коммутаторларында VLAN теңшеу	70
Зертханалық жұмыс № 12. Корпоративтік желіде VLAN орнату	76
№ 3 өзіндік жұмыс	81
Бақылау сұрақтары	81
9 Бөлім. Бірнеше жұмыс режимі	82
Зертханалық жұмыс № 13. Бірнеше жұмыс режимі	84
№ 4 өзіндік жұмыс	90
Бақылау сұрақтары	90



10 Бөлім. ACL (Access Control List) қатынауды басқару тізімі	91
Зертханалық жұмыс № 14. Кіру тізімі	95
№5 өзіндік жұмыс	97
№ 6 өзіндік жұмыс	98
№7 өзіндік жұмыс	99
№ 8 өзіндік жұмыс	100
Бақылау сұрақтары	101
Қорытынды	102
Қолданылған әдебиеттер тізімі	103

## Кіріспе

Оқу құралы Cisco бойынша зертханалық жұмыстардан (Cisco Packet Tracer интерфейсі, симуляция режимі, Желілік қызметтер, Cisco IOS операциялық жүйесінің негізгі командалары, статикалық маршруттау, VLAN виртуалды жергілікті желілері, ACL (Access Control List) қатынауды басқару) тұрады.

Cisco Packet Tracer - Cisco компаниясы құрған желі эмуляторы.

Бұл бағдарлама әртүрлі хаттамаларды қолдайтын еркін топологияларда әртүрлі жабдықтарда желілерді құруға мүмкіндік береді.

Cisco Packet Tracer бағдарламалық шешімі әртүрлі желілік құрылғылардың; маршрутизаторлардың, коммутаторлардың, сымсыз қатынау нүктелерінің, дербес компьютерлердің, желілік принтерлердің, IP-телефондардың және т.б. жұмысын имитациялауға мүмкіндік береді.

Параметрлер, өз кезегінде, құрылғылардың сипатына байланысты: кейбіреулерін Cisco IOS операциялық жүйесінің командаларын қолдана отырып конфигурациялауға болады, басқаларын веб-графикалық интерфейс көмегімен конфигурациялауға болады, ал басқаларын операциялық жүйенің командалық сызығы немесе графикалық мәзірлер арқылы конфигурациялауға болады.

Корнекілендіру режимі сияқты Cisco Packet Tracer мүмкіндігінің арқасында қолданушы желідегі мәліметтердің қозғалысын, IP-пакеттерінің жылдамдығы мен жолын, желілік құрылғылар арқылы өтетін кезде IP пакеттік параметрлерінің өзгеруін бақылай алады. Желіде болып жатқан оқиғаларды талдау оның жұмыс механизмін түсінуге және ақауларды анықтауға мүмкіндік береді.

Cisco Packet Tracer тренажер ретінде ғана емес, сонымен қатар Интернет арқылы нақты желі арқылы виртуалды желіні модельдеуге арналған желілік қосымша ретінде де қолданыла алады. Әр түрлі компьютерлердің пайдаланушылары, орналасқан жеріне қарамастан, бір желілік топологияда жұмыс істей алады, оны конфигурациялайды немесе проблемаларды шешеді. Бұл Cisco Packet Tracer Multiuser мүмкіндігін топтық жұмысты ұйымдастыру үшін пайдалануға болады.

Cisco Packet Tracer-де пайдаланушы логикалық ғана емес, сонымен қатар желінің физикалық моделін құра алады, демек дизайнгерлік дағдыларды игереді. Желілік диаграмманы нақты қолданыстағы ғимараттың немесе тіпті қаланың сызбасына қоюға болады және оның барлық кабельдерін салуға арналған, құрылыстарды әртүрлі ғимараттар мен үй-жайларға орналастырады, мысалы, салынатын кабельдің ұзындығы мен түрі немесе сымсыз қамту аймағының радиусы сияқты физикалық шектеулерді ескере отырып.

Симуляция, визуализация, бірнеше режим және жобалау мүмкіндігі Cisco Packet Tracer желілік технологияларды оқыту үшін бірегей құрал жасайды.

Cisco Packet Tracer Cisco компаниясымен әзірленген және телекоммуникациялық желілер мен желілік жабдықтарды зерттеу кезінде, сондай-ақ жоғары оқу орындарында зертханалық жұмыстар бойынша сабақтар өткізу үшін пайдалану ұсынылады.

Cisco Packet Tracer негізгі мүмкіндіктері:

1. Графикалық интерфейс (GUI), бұл желіні ұйымдастыруды, құрылғының жұмыс принциптерін жақсы түсінуге көмектеседі;

2. Real-time режимінде модельдеу (нақты уақыт);

3. Симуляция режимі;

Алайда, бұл Packet Tracer барлық артықшылықтары емес: симуляция режимінде студент пайдаланылатын хаттамаларды бақылап қана қоймай, OSI моделінің жеті деңгейінің қайсысын, сондай-ақ пакеттің мазмұнын, оның пішімін көре алады.

Packet Tracer әр түрлі мақсаттағы құрылғылардың көп санын, сондай-ақ әр түрлі байланыс түрлерін модельдеуге қабілетті, бұл кез келген көлемді желіні жоғары күрделілік деңгейінде жобалауға мүмкіндік береді:

1) Модельдеуші құрылғылар:

- үшінші деңгейлі коммутаторлар:

1. Router 2620 XM;

2. Router 2621 XM;

3. Router-PT.

-екінші деңгейлі коммутаторлар ол:

1. Switch 2950-24;

2. Switch 2950T;

3. Switch-PT;

4. Bridge-PT типті "көпір" байланысы.

5. Желілік концентраторлар:

- Hub-PT;

- қайталау Repeater-PT.

2) Шегкі құрылғылар:

1. PC-PT жұмыс станциясы;

2. Server-PT сервері;

3. Printer-PT принтері.

4. Сымсыз құрылғылар:

5. Accesspoint-PT кіру нүктесі.

Сондай-ақ, студент бақылай алатын хаттамаларды келтіру орынды:

- ARP;

- CDP;

- DHCP;

- EIGRP;

- ICMP;

- RIP;

- TCP;

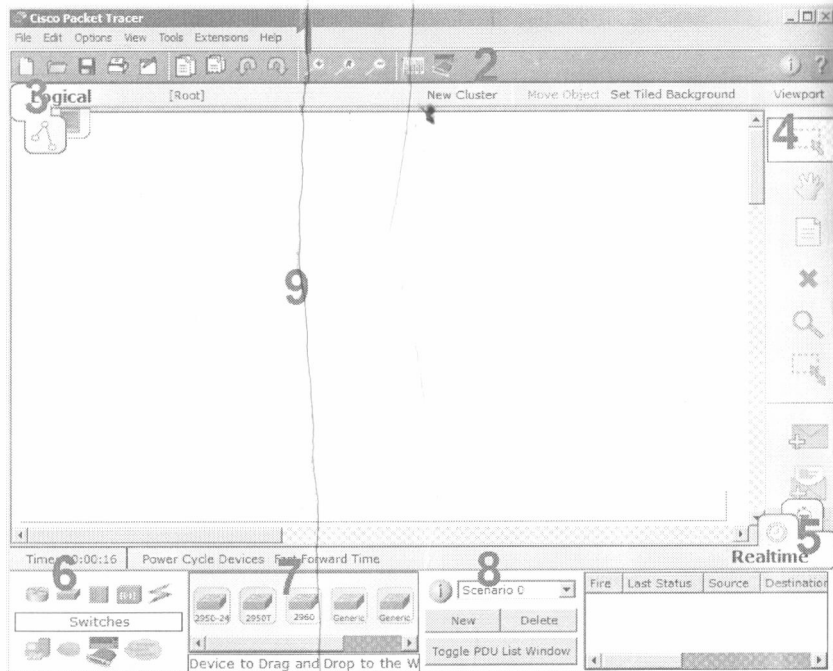
- UDP.

Packet Tracer деректерді беру желілерін модельдеудің ыңғайлы құралы болып табылады. Симулятормен жұмыс істеу әр түрлі құрылғылардан тұратын нақты желіні күйге келтірудің шынайы сезімін береді. Желі жабдықтарын баптауды Cisco IOS операциялық жүйесінің командалары арқылы да, графикалық интерфейс арқылы да жүргізуге болады. Симуляция режимі арқылы деректерді желі арқылы жылжытуды, деректерді желілік құрылғылар арқылы оту кезінде пакеттер параметрлерінің пайда болуын және өзгеруін, пакеттердің жылдамдығы мен жылжу жолдарын байқауға болады. Желідегі оқиғаларды талдау оның жұмыс механизмін түсінуге және ақауларды анықтауға мүмкіндік береді.

# І БӨЛІМ. CISCO PACKET TRACER ИНТЕРФЕЙСІ

## 1.1. Cisco Packet Tracer негізгі терезесі

1.1 суретінде облыста бөлінген бағдарлама интерфейсі ұсынылған.



Сурет 1.1 - Cisco Packet Tracer бағдарламасының интерфейсі

1. Келесі мазмұнмен бағдарламаның басты мәзірі:

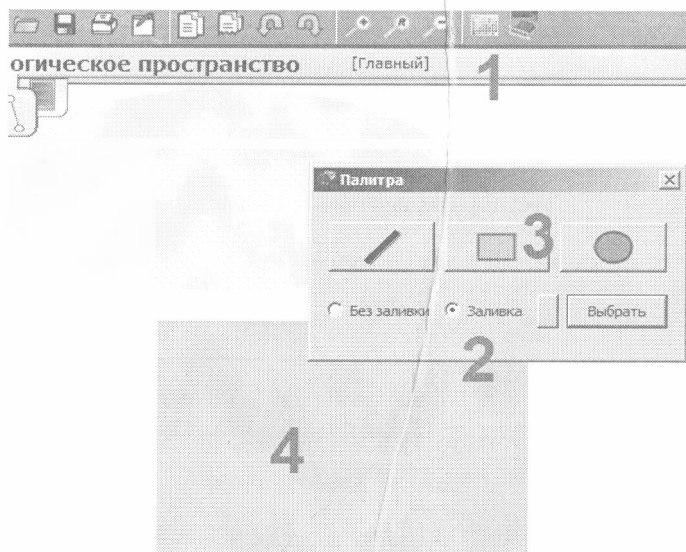
- Файл-құжаттарды ашу/сақтау операцияларын қамтиды;
- Өңдеу-Стандартты операциялар " көшіру/кесу, болдырмау/қайталау";
- Параметрлер- өзі үшін сойлейді;
- Көрініс-жұмыс аймағы мен құралдар тақтасының ауқымы;
- Құралдар-түстер палитрасы және соңғы құрылғыларды кастомизациялау;

- Кеңейту деген СРТ-тен дардай зертхана жасай алатын бірнеше режимы бар жобалар мастеры;

- Көмек - онда не бар екенін таппайсыз;

1. Мәзір тармақтарын қайталайтын құралдар тақтасы;

2. Логикалық және физикалық ұйым арасындағы қосқыш;
  3. Тағы бір құралдар панелі, нысандарды бөлу, жою, жылжыту, масштабтау, сондай-ақ еркін пакеттерді қалыптастыру құралдарын қамтиды;
  4. Нақты режим (Real-Time) мен симуляция режимі арасындағы қосқыш;
  5. Соңғы құрылғылар мен байланыс желілерінің топтары бар панель;
  6. Соңғы құрылғылардың өздері, мұнда барлық мүмкін коммутаторлар, тораптар, кіру нүктелері, өткізгіштер бар.
  7. Теңшелетін сценарийлерді жасау панелі;
  8. Жұмыс кеңістігі.
- Түсті аймақтарын орналастыру мысалы (сурет.1.2), мысалы, бір-бірінен көзбен бөлуге мүмкіндік береді.



Сурет 1.2 - Түсті аймақтарын орналастыру мысалы

Түсті аймақтарды орнату үшін келесі кадамдарды орындаңыз:

- 1- Құралдар тақтасында тиісті белгішені таңдаңыз;
- 2- "Толтыру" аймағын таңдаңыз, мысалы;
- 3- Түсі мен пішінін таңдаңыз;
- 4- Жұмыс кеңістігінде аймақты сызыңыз.

Сондай-ақ, қолтаңбаны қосуға және осы аймақты жылжытуға/масштабтауға болады.

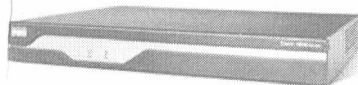
## 1.2. Cisco Packet Tracer байланыс жабдыктары мен желілері

### Маршрутизаторлар

Маршрутизаторлар маршруттаудың арнайы алгоритмдері негізінде деректерді берудің оңтайлы маршрутын іздеу үшін пайдаланылады, мысалы транзиттік тораптардың ең аз саны бар маршрутты (жолды) таңдау.



Сурет 1.3 - Маршрутизаторлар



Сурет 1.4 -Маршрутизаторлардың түрлері

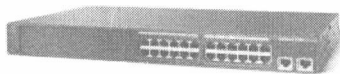
OSI моделі желілік деңгейде жұмыс істейді.

### Коммутаторлар



Сурет 1.5 - Коммутаторлар

Коммутаторлар-OSI моделінің арналық деңгейінде жұмыс істейтін және желінің бір немесе бірнеше сегменттерінде бірнеше тораптарды біріктіруге арналған құрылғылар. Сонымен қатар, ол барлық порттарда қайталанбайды (концентратор сияқты), ол арналған MAC - мекен-жайына ғана жүреді.



Сурет 1.6 – Коммутаторлар түрлері

## Концентраторлар



Сурет 1.7 - Концентраторлар

Концентратор барлық қалған порттарда бір портта қабылданған пакетті қайталайды.

## Сымсыз құрылғылар



Сурет 1.8 - Сымсыз құрылғылар

Wi-Fi сымсыз технологиялары және олардың негізінде желілер. Қол жеткізу нүктелерін қамтиды.

## Байланыс желісі




Сурет 1.9 - Байланыс желісі








Бұл компоненттердің көмегімен тораптарды бірыңғай схемаға қосу жасалады. Packet Tracer желілік қосылымдардың кең ауқымын қолдайды (1.1 кестені қараңыз).

Кабельдің әрбір түрі тек белгілі бір интерфейстермен жалғануы мүмкін.

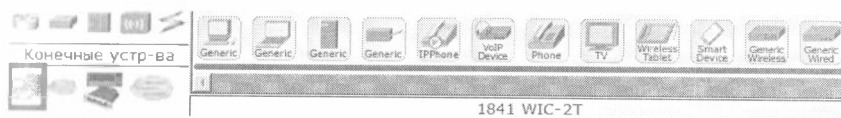
### 1.1 кесте-Кабель түрлері

Кабель түрі	Сипаттамасы
Консоль 	Консоль қосылымы ДК мен маршрутизаторлар немесе коммутаторлар арасында орындалуы мүмкін. ДК-мен консольдік сеанстың жұмысы үшін кейбір талаптар орындалуы тиіс: қосудың жылдамдығы бірдей болуы тиіс, екі жақ үшін 7 бит деректер (немесе 8 бит) болуы тиіс, ашықтықты бақылау бірдей



	болуы тиіс, 1 немесе 2 табан бит болуы тиіс (бірақ олар бірдей болуы міндетті емес), ал деректер ағыны екі тарап үшін кез келген болуы мүмкін.
Мыс түзу 	Бұл кабельдің түрі OSI түрлі деңгейлерінде жұмыс істейтін құрылғыларды қосу үшін стандартты Ethernet беру ортасы болып табылады. Ол порттардың келесі түрлерімен қосылуы тиіс: мыс 10 Мбит/с (Ethernet), мыс 100 Мбит/с (Fast Ethernet) және мыс 1000 Мбит/с (Gigabit Ethernet).
Мыс кроссовері 	Бұл кабельдің түрі OSI бірдей деңгейлерінде жұмыс істейтін құрылғыларды қосу үшін Ethernet беру ортасы болып табылады. Ол порттардың келесі түрлерімен қосылуы мүмкін: мыс 10 Мбит/с (Ethernet), мыс 100 Мбит/с (Fast Ethernet) және мыс 1000 Мбит/с (Gigabit Ethernet).
Оптика 	Оптикалық талшықты орта оптикалық порттар арасында қосылу үшін қолданылады (100 Мбит/с немесе 1000 Мбит/с).
Телефондық 	Телефон желісі арқылы қосылу модемдік порттары бар құрылғылар арасында ғана жүзеге асырылуы мүмкін. Модемдік қосылыстың стандартты көрінісі - бұл желілік бұлтқа хабарланатын соңғы құрылғы (мысалы, ДК).
Коаксильдық 	Коаксиалды орта Packet Tracer бұлт қосылған кабельдік модем сияқты коаксиалды порттар арасында қосылу үшін қолданылады.
Сериялық DCE  Сериялық DTE 	Тізбекті порттар арқылы қосылыстар жиі WAN байланыстары үшін қолданылады. Мұндай байланыстарды орнату үшін DCE құрылғысының жағында синхрондауды орнату қажет. DTE синхронизациясы таңдау бойынша орындалады. DCE жағын порт жапындағы "cahat" шағын белгішесі бойынша анықтауға болады. Serial DCE қосылым түрін таңдағанда, қосылым қолданылатын бірінші құрылғы DCE құрылғысына айналады, ал екіншісі - автоматты түрде DTE жағына айналады. Serial DTE қосылым түрі таңдалса, тараптардың кері орналасуы да мүмкін.

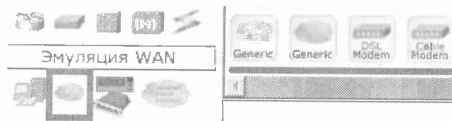
Соңғы құрылғылар



Сурет 1.10- Соңғы құрылғылар

Мұнда соңғы тораптар, хостар, серверлер, принтерлер, телефондар және т. б. бар.

### Интернеттің эмуляциясы



Сурет 1.11 - Интернеттің эмуляциясы

Мысал жаһандық желі эмуляциясы. DSL, "бұлт" және т. б. модемі. Копколданушы жұмысқа арналған қолданушы құрылғылар және бұлт



Сурет 1.12 -Пайдаланушы қосылғыштар

Құрылғыны өзіңіз жинақтауға болады. Ерікті байланыс жасауға болады.

### 1.3. Жабдықты физикалық жинақтау

Жұмыс өрісіне Cisco 1841 роутер орнату роутердегі баптауларда оның физикалық конфигурациясын ашамыз (сурет 1.13).

Сол жақта, біз көріп отырғанымыздай, осы роутер жинақтауға болатын модульдер тізімі (2 Сан). Қазір онда 2 бос (3 саны). Оларға осы модульдерді салуға болады. Әрине, бұл операцияны ажыратылған тамактану кезінде жүргізу керек (1 Саны).

WIC (HWIC, VWIC) модульдері бұл құрылғының функционалын арттыратын кеңейту платалары:

- WIC - WAN interface card. the first original models.

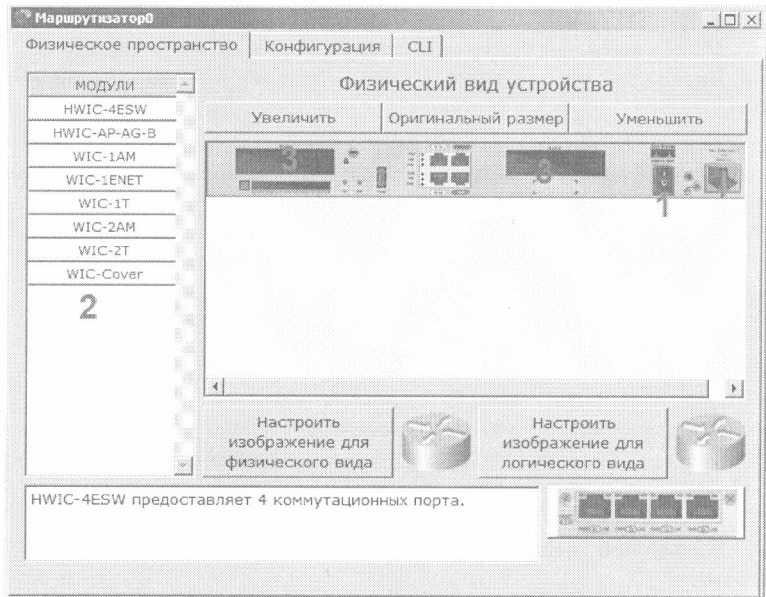
- HWIC- high-speed wan interface card- the evolution of wic that is now in use on the ISR routers.

VIC - voice interface card, support voice only.

VIC2 - evolution of the above

VWIC - voice and wan interface card. An E1/T1 card that can user for voice or data.

VWIC2 - evolution of the above



Сурет 1.13-Құрылғының физикалық конфигурациясы

Мысалы, компьютер үшін PCI шинасына (TV тонерлер, дыбыстық карталар, USB тармақтағыштар, желілік карталар) қосылатын платалар бар. Жалпы, Cisco құрылғысы-Бұл өзінің операциялық және көптеген желілік карталарымен бірдей жүйелік блок, ол тек желімен ғана бірдене жасай алады.

Төменде әрбір модуль туралы ақпарат бар:

- HWIC - 4ESW - 4-ші Ethernet коммутациялық порттары бар жоғары өнімді модуль RJ-45 ажыратқышы. Маршрутизаторда коммутатордың мүмкіндіктерін үйлестіруге мүмкіндік береді.

- HWIC-AP-AG-B - бұл Cisco 1800 (модульдік), Cisco 2800 және Cisco 3800 сызғыштарының роутерлеріне арналған кірістірілген кіру нүктесінің функционалын қамтамасыз ететін жоғары жылдамдықты WAN-карта. Бұл модуль Single Band 802.11 b/g немесе Dual Band 802.11 a/b/g радио арналарын қолдайды.

- WIC-1AM базалық телефон қызметіне қосылу үшін пайдаланылатын RJ-11 (телефон) қосқышын қамтиды. Карта телефон желісімен қосылу үшін бір портты пайдаланады, екіншісі модем тоқтаған кезде қоңырау шалу үшін аналогтық телефонға қосылуы мүмкін.

- WIC-1ENET - бұл 10BASE-T Ethernet LAN үшін бір портты 10 Мб/с Ethernet картасы.

- WIC-1T қашықтағы кеңселерге немесе SDLC концентраторларына, сигнал беру жүйелеріне және packet over SONET (POS) құрылғыларына қатысты ескірген сериялық желілік құрылғыларға бір портты тізбекті қосылым береді.

- WIC-2AM базалық телефон қызметіне қосылу үшін пайдаланылатын екі RJ-11 қосқышы бар. WIC - 2AM-де екі модемдік порт, бұл екі арнаны бір уақытта қосуға мүмкіндік береді.

- WIC-2T - 2-порттық синхронды/асинхронды сериялық желілік модуль әр портты синхронды немесе асинхронды режимге жеке реттеумен көптеген хаттамаларға икемді қолдау көрсетеді. Синхронды / асинхронды қолдау үшін қолдану ұсынады:

- төмен жылдамдықты агрегация (128 Кб/с дейін);

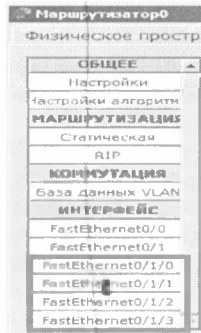
- dial-up модемдерді қолдау;

- басқа жабдықты басқару порттарына синхронды немесе асинхронды қосылыстар және Bi-sync және SDLC типті ескірген хаттамаларды беру.

- WIC-Cover - WIC слоттың қабырғасы электрондық компоненттерді қорғау үшін және салқындатқыш ауа ағынының айналымын жақсарту үшін қажет.

Жабдықты жинақтауды өзгерту үшін:

- қуат көзін өшіру, қуат түймесіне тінтуірмен басу, 4ESW модульін еркін слотқа сүйреп, қуат көзін қосу. Роутерді жүктеудің аяқталуын күту. GUI конфигурациясында пайда болған 4 жаңа интерфейссті көре аламыз (сурет 1.14).



Сурет 1.14-Құрылғы интерфейстерін конфигурациялау

Қалған құрылғылар үкесі жиынтықталады. Жаңа Ethernet модульдері (10/100/1000), бірнеше типті оптикалық талшықты қосқыштар, сымсыз желі адаптерлері қосылады. Жұмыс компьютеріне құлаққап микрофон, деректерді сақтау үшін қатты диск сияқты қосу мүмкіндігі бар.

#### Бақылау сұрақтары:

1. Кірістірілген кіру нүктесінің функционалын кеңейтудің қандай ақысы қамтамасыз етеді?
2. Қашықтағы кеңселерге немесе ескірген сериялық желілік құрылғыларға бір портты тізбекті қосылымды қандай кеңейту ақысы береді?
3. 4-ші Ethernet коммутациялық порттары бар жоғары өнімді модуль қалай аталады?
4. WAN желілеріне қосылуға мүмкіндік беретін желілік карталарды атаңыз?
5. Кластерді құру кезінде интерфейстің қандай түрін таңдау керек?
6. Үшінші деңгейлі коммутаторлардың модельдерін атаңыз?
7. Роутерлерді бір-бірімен жалғаған кезде кабельдің қандай түрін пайдалану керек?
8. Магистральды маршрутизаторлар сериясын көрсетіңіз.
9. Қандай жағдайларда SERIAL интерфейсін қолданылады?
10. Екі магистральді маршрутизатордың байланысын қалай ұйымдастыруға болады?
11. Cisco Packet Tracer бағдарламасының барлық ықтимал жұмыс режимдерін атаңыз?
12. Екінші деңгейлі коммутаторлардың модельдерін атаңыз?
13. Cisco Packet Tracer-де қолданылатын барлық байланыс түрлерін атаңыз және олардың мақсатын көрсетіңіз.

## 2 БӨЛІМ. СИМУЛЯЦИЯ РЕЖИМІ.

Cisco Packet Tracer желі жұмысының жай-күйін және кез келген желілік оқиғаларды имитациялауға және симуляциялауға болатын желі жұмысын симуляциялау құралын қамтиды. Мысалы, желінің іркіліс жағдайында қалай әрекет ететінін немесе мысалы, қандай да бір кабельді ажыратып немесе желілік құрылғылардың бірінің қорегін өшірсе не болатынын қадағалауға болады.

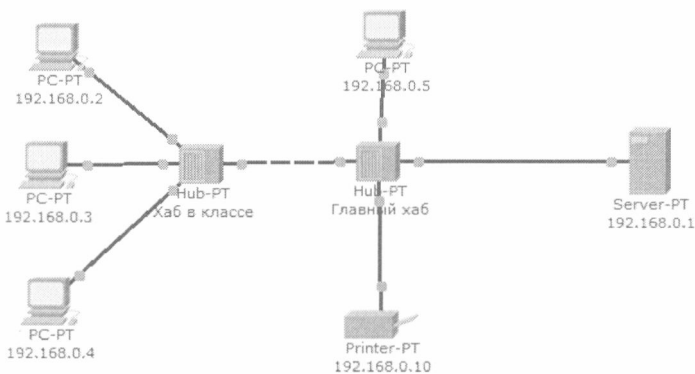
Симуляция режимі пакеттің құрылымын бақылауға және OSI моделінің деңгейлері бойынша пакеттің қандай параметрлерімен өтетінін көруге мүмкіндік береді.

Симулятор режимі келесі мүмкіндіктер мен технологияларды қамтиды:

- маршруттау, арналарды моделдеу жүйесі, IP-сузу;
- пакеттер түрлері: ICMP, UDP, TCP, сондай-ақ төмен деңгейлі ARP сұраулары;
- интерфейс және сокет тұжырымдамасы (қарапайым, дейтаграммды және ағындық);
- хостердің, екінші деңгейлі коммутаторлардың және концентраторлардың эмуляциясы;
- арнада кедергі деңгейін орнату.

### Зертханалық жұмыс №1. Cisco Packet Tracer-де симуляция режимі.

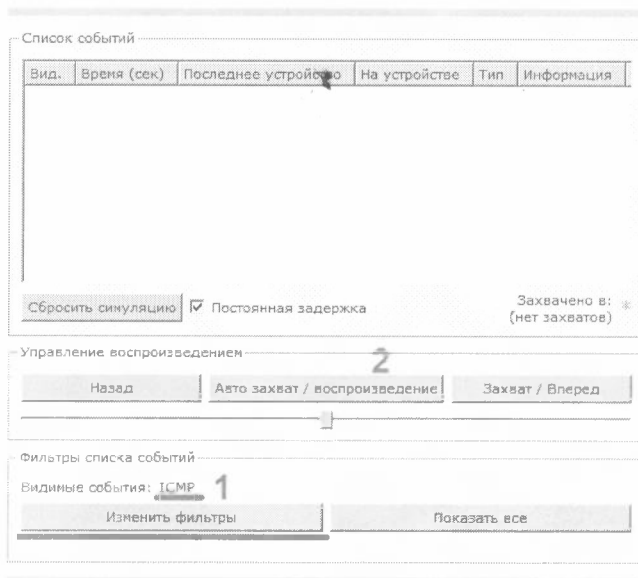
Желі рамасы: 4 қапсырма, сервер, принтер, 2 концентратор.  
Концентраторлар өзара байланысқан кроссовер кабелі (Сурет 2.1).



Сурет 2.1-Желі схемасы

Симуляция режиміне (Shift+S) оту керек немесе жұмыс кеністігінің оң жақ төменгі бұрышында симуляция белгісіне басу керек. Мұнда біз оқиға терезесін көреміз, қалпына келтіру батырмасы (оқиғалар тізімін тазартады), ойнатуды басқару және хаттамалар сүзгісі. Көптеген хаттамалар ұсынылды, бірақ тек ICMP сүземіз, бұл тораптар арасындағы кездейсоқ трафикті болдырмайды.

Келесі оқиғаға оту үшін "алға" немесе автоматика (сурет 2.2).

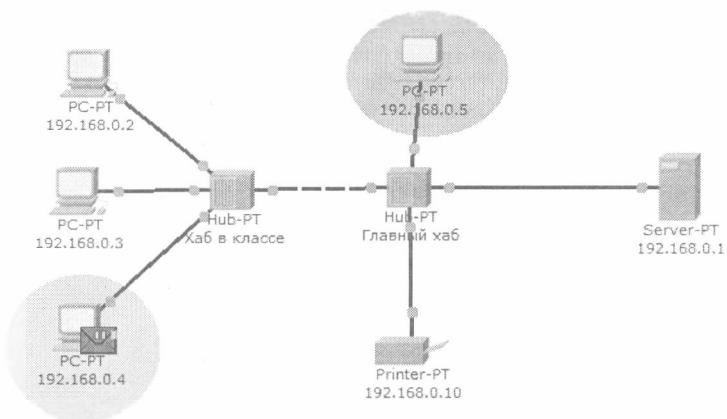


Сурет 2.2-Симулятор интерфейсі

PING-сұрауды жібереміз.

Түйіндердің бірінен басқа түйінді өткізуге тырысамыз. Желі бойынша пакеттердің симуляция режимінде қалай өтетінін көру үшін алыс орналасқан тораптарды таңдаймыз. Сонымен, 4 түйінге кіреміз және 5 торапқа пинг-сұранысын жібереміз.

Қызғылт түйінмен жасыл пингүем. Қызғылт түйінде пакет (конвертик) пайда болды, ол күтеді (онда үзіліс белгісі). Пакетті желіге симуляция терезесіндегі "Алға" батырмасын басу арқылы іске қосуға болады (сурет 2.3).



Сурет 2.3-Симулятордың жұмысын көрсету

Сонымен қатар, симуляция терезесінде осы пакетті көріп, оның түрін (ICMP) және көзін (192.168.0.4) белгілейміз – сурет 2.4.

Сурет 2.4-Хаттамалар жұмысының мониторингі

Симулятордың "Список событий" (Event List) терезесінің скриншоты. Таблицада бір оқиға көрсетілген:

Вид	Время (сек)	Последнее устройство	На устройстве	Тип	Информация
	0,000	--	192.168.0.4	ICMP	

Терезенің басқа бөліктері:

- Сбросить симуляцию:
- Постоянная задержка
- Захвачено: 0,000 с
- Управление воспроизведением: Назад, Авто захват / воспроизведение, Захват / Вперед
- Фильтры списка событий: Видимые события: ICMP, Изменить фильтры, Показать все

Сурет 2.4-Хаттамалар жұмысының мониторингі

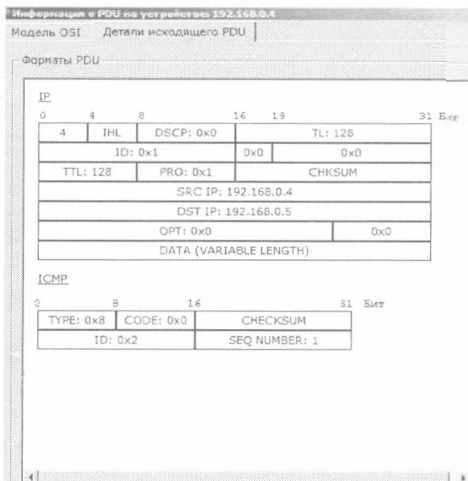


Пакеттегі клик бізге толық ақпаратты көрсетеді. Бұл ретте біз OSI моделін көреміз. 3-ші деңгейде (желілік) шығыс бағытта бума пайда болғанын бірден көруге болады, ол екінші деңгейге дейін, содан кейін бірінші деңгейге дейін, физикалық ортаға және келесі торапқа жіберіледі (сурет 2.5).



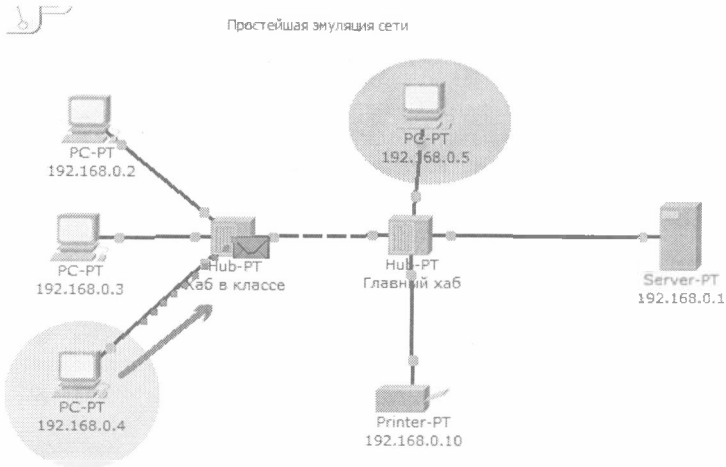
Сурет 2.5-OSI моделіндегі жұмыс мониторингі

Ал басқа қойындыда пакет құрылымын көруге болады (сурет 2.6).



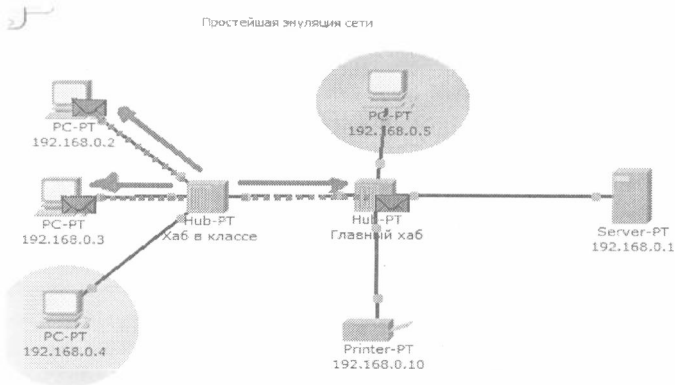
Сурет 2.6-Пакеттің құрылымы

"Алға" батырмасын басыңыз. Және пакет бірден концентраторға аумсады. Бұл жағынан жалғыз желілік байланыс ( сурет 2.7).



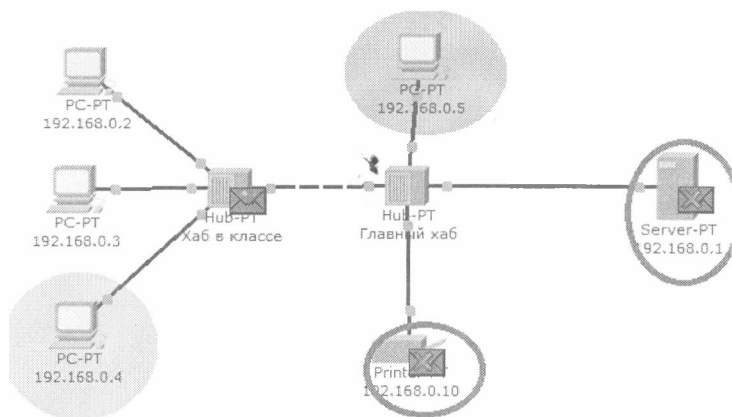
Сурет 2.7-Пакеттің отуі. Бірінші кезең

Концентратор пакеті барлық порттарда үмітпен қайталайды, оның бірінде адресат барына, (сурет 2.8).



Сурет 2.8-Пакеттің өтуі. Екінші кезең

Егер пакеттер қандай да бір тораптарға арналмаған болса, олар оларды елемейді (сурет 2.9).



Сурет 2.9-Пакеттің өтуі. Үшінші кезең

Пакет қайта оралғанда, қосылыстың растауын көреміз.

#### Бакылау сұрақтары:

1. Симуляция режимі не үшін колданылады?
2. OSI моделінің деңгейлері бойынша пакеттің өтуін қалай көруге болады?
3. Болады, себебін анықтау үшін жіберілген режимінде симуляциялар пакеті жетпеді дейін адресаттың қай кезеңінде ауытқу болды желі?
4. Жіберушінің және алушының IP мекенжайы пакетінің құрамында көрсетіңіз.
5. Оқиғалар тізімінің сүзгілерін қалай өзгертуге болады?
6. Симуляция режимінде желі жұмысына қандай хаттамалар қатыстырылғанын қалай анықтауға болады?
7. Желі арқылы өту кезінде бума мазмұнының өзгеруін қалай бакылауға болады?
8. Симуляция режимінің негізгі мүмкіндіктерін атаңыз.

### 3 БӨЛІМ. ЖЕЛІЛІК ҚЫЗМЕТТЕР

Желілік қызмет дегеніміз-серверлік және тұтынушы бөлігін операциялық жүйеде компьютерлік желі арқылы ұсынуды айтады. Кредиттік тип ресурстарының жинағы. Желілік қызмет қолданушыға желінің кейбір қызмет көрсету жиынтығымен таныстырады. Бұл қызмет көрсету жиынтығы кей кездерде желілік сервис деп те аталады. Ағылшынның «service» терминінен шыққан сөз. Бұл термин кейбір техникалық әдебиеттерде «сервис», «қызмет көрсету» немесе «қызмет» деп аударылып жазылған. Осылайша, сервис-бұл қызмет көрсетуді тұтынушымен жеткізуші арасындағы интерфейс. Әрбір қызмет желілік ресурстардың анықталған типімен және осы ресурстар мен жұмыс істеуге мүмкіндік туғызатын тәсілмен байланысты болады. Мысалға баспаға шығару қызметі желінің қолданушыларын бөліктелген принтерларда қолдануға мүмкіндік туғызады, ал пошталық қызмет көрсету желінің ақпараттық ресурсымен, яғни электрондық хаттармен жұмыс істеуге мүмкіндік туғызады. Ресурстармен жұмыс істеумен мүмкіндік апаратын тәсіл, мысалы қашықтатылған мүмкіндік туғызу қызметі-ол компьютерлік желі қолданушыларын телефонды каналдар арқылы оның барлық ресурстарына мүмкіндік ашу. Қандай да бір ресурсқа қашықтатылған мүмкіндік ашу үшін, мысалы принтерға қашықтатылған мүмкіндік ашу қызметі баспаға шығару қызметімен өзара әрекеттеседі.

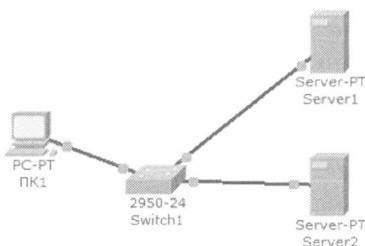
Желілік операциялық жүйе қолданушылар үшін файлдық және баспаға басу қызмет көрсетулері маңыздырақ. Желілік қызмет көрсету ортасы жәй қолданушыға емес администраторға бағытталған. Мұндай қызмет ұйымдастырылған желілік жұмыста қолданылады. Мысалы: Novel Wetware 3x операциялық жүйесіндегі Bindery қызметі компьютерлік желідегі мәліметтер базасында жұмыс істеуге администраторға рұқсат етеді. Орталықтанған анықтамалық қызметті құру тиімдірек болып табылады немесе басқаша айтқанда барлық желінің қолданушылары желідегі мәліметтерін қорын жүргізуге арналған каталогтар емес сонымен қатар оның барлық программалық және аппараттық компоненттерінің қызметі болып табылады. Қызмет каталогының сапалы мысалдары NDS компаниясында, NOVELL және STREET TALK BANUAN компанияларында мысал ретінде келтіріледі. Желілік қызметтің басқаша мысалдары ретінде желілік трафикті жаулап алуға және талдауға мүмкіндік беретін желінің мониторинг қызметін, желілік кілтті тексеру арқылы кіретін логикалық процедураларының орындалуын қамтамасыз ететін қауіпсіздік қызметі және резервтік көшіріп алу және архивтеу қызметтерін қарастыруға болады. Осыншама байлығымен қамтамасыздандыру жиынтығы операциялық жүйеге ақырғы қолданысын ұсынады, ал оның администраторлық желісі және қосымша қолданылуы оның позициялық операциялық жүйемен байланысты.

Желілік қызмет өзінің табиғатында клиентті-серверлі система болып табылады. Жүзеге асырумен бірге кез-келген желілік сервистің нағыз сұраныстардың қайнар көзі (клиент) және сұраныстар орындаушысы және басқада желілік қызметтер екі симметриялық емес клиенттік және серверлік бөлікті құрайды. Операциялық жүйеде желілік қызмет осы екі клиенттік және серверлік бөліктермен түсіндіріледі немесе тек қана екеуінің біреуімен ғана. Кейбір кездерде сервер өзінің ресурстарын клиенттеріне ұсынады, ал клиент оны қолданады

Cisco Packet Tracer эмуляторы желі серверінің құрамында HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP сияқты желілік сервистерді баптауға мүмкіндік береді. Олардың кейбірін баптауды қарастырайық.

### Зертханалық жұмыс №2. Желілік сервистерді баптау.

3.1 суреттегі желінің келесі схемасын жасаңыз:



Сурет 3.1-Желі схемасы

Тапсырма:

Желіні келесідей баптау:

1-Server 1-DNS және Web сервер;

2-Server 2-DHCP сервер;

3-ДК1 компьютері TCP/IP с DHCP серверінің протоколы параметрлерін алады және сайтты ашады www.rambler.ru серверде.

1 кезең.

ДК 1 және серверлерде TCP/IP протоколдарының параметрлерін орнатыңыз.

ДК 1 конфигурациясына кіріңіз және IP параметрін DHCP сервері арқылы орнатыңыз.

Сервер конфигурациясында келесі IP параметрлерін теңшеңіз:

Server 1: IP мекенжайы - 10.0.0.1, ішкі желі маскасы - 255.0.0.0

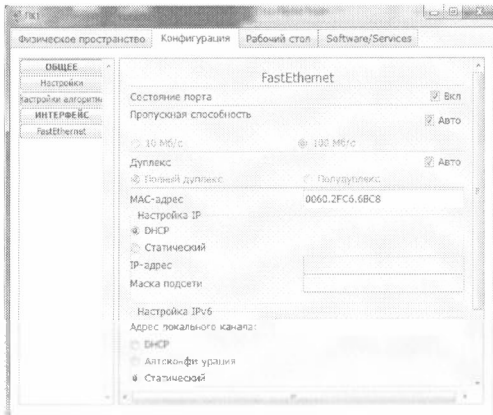
Server 2: IP мекенжайы - 10.0.0.2, ішкі желі маскасы - 255.0.0.0

2 кезең.

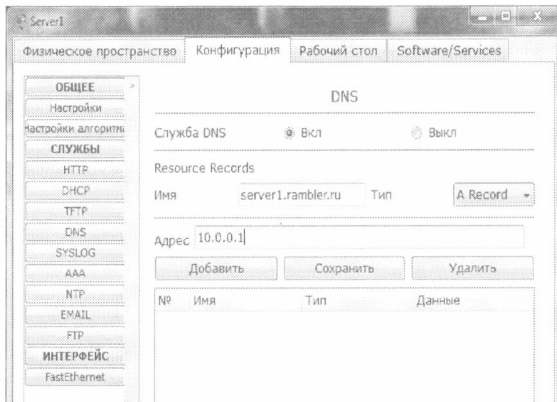
Server 1-де DNS қызметін теңшеңіз.

Ол үшін Server 1 конфигурациясында DNS қойындысына өтіп, тікелей DNS аймағында екі қор жазбаларын орнатыңыз:

1 - ресурстық жазба түрінде компьютердің домендік атауын IP-мекен-жайымен байланыстырыңыз және 3.3 суретті салыңыз және ҚОСУ түймесін басыңыз:

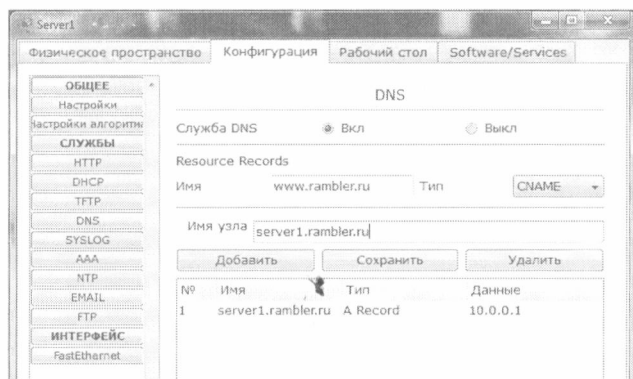


Сурет 3.2-ДК1-де IP теңшеу



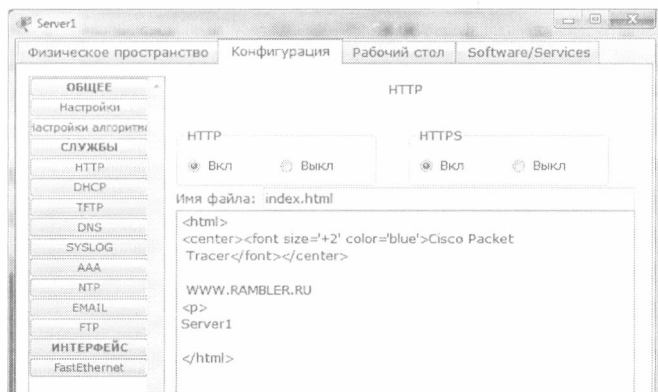
Сурет 3.3-Ресурстар түрін енгізу

2 - CNAME типті ресурстық жазбада сайттың бүркеншік атын компьютермен байланыстырыңыз (сурет 3.4.):



Сурет 3.4-CNAME типті ресурстық жазбаны енгізу

Server 1 конфигурациясында HTTP қойындысына өтіп, WWW.RAMBLER.RU сайтының бастапқы бетін орнатыңыз (Сурет 3.5):



Сурет 3.5-Сайттың бастапқы беті

Server 1-де пәрмен жолын қосыңыз және DNS қызметін тексеріңіз. DNS серверінің тікелей аймағын тексеру үшін пәрменді енгізіңіз

**SERVER>nslookup www.rambler.ru**

Егер бәрі дұрыс болса, онда сіз желідегі DNS серверінің толықтай білікті домендік атауын және оның IP мекенжайын көрсете отырып, 3.6-суретте көрсетілген жауап аласыз.

```
SERVER>nslookup www.rambler.ru
Server: [10.0.0.1]
Address: 10.0.0.1

Non-authoritative answer:
Name:   server1.rambler.ru
Address: 10.0.0.1

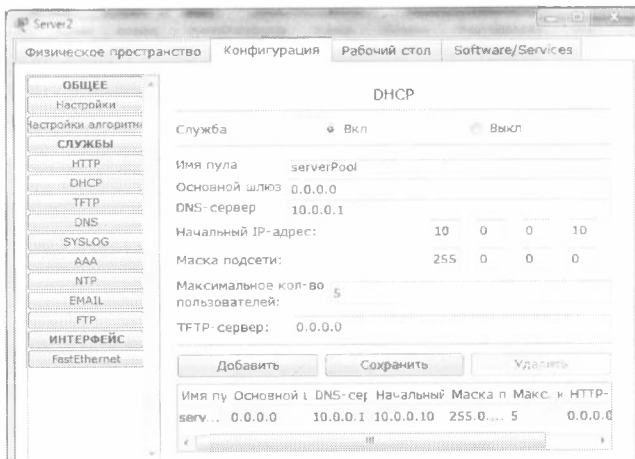
Aliases:   server1.rambler.ru
SERVER>
```

Сурет 3.6-DNS тікелей аймағын тексеру

3 кезең.

Server 2 жүйесінде DHCP қызметін теңшеңіз.

Ол үшін Server 2 конфигурациясына өтіп, DHCP қойындысында қызметті теңшеңіз (сурет 3.7):



Сурет 3.7-DHCP серверін баптау

4 кезең. Клиенттің жұмысын тексеру.

PC1 хост конфигурациясын жұмыс үстеліне енгізіңіз және TCP/IP протоколын баптаңыз.



Команда

**PC>ipconfig /release**

ескі IP мекенжайының параметрлерін қалпына келтіріп, нәрменмен орнатыңыз:

**PC>ipconfig /renew**

DHCP серверінен жаңа параметрлер алу (Сурет 3.8):

```
PC>ipconfig /release

IP Address . . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . : 0.0.0.0
DNS Server . . . . . : 0.0.0.0

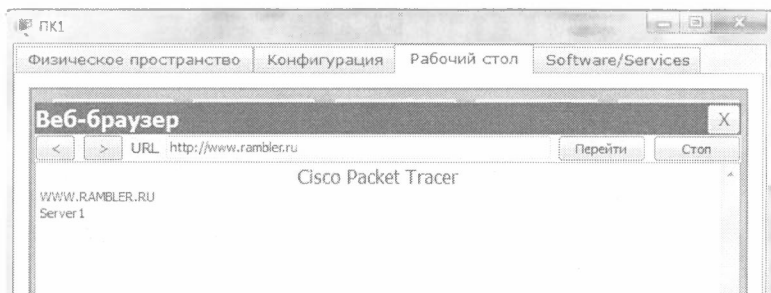
PC>ipconfig /renew

IP Address . . . . . : 10.0.0.10
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 0.0.0.0
DNS Server . . . . . : 10.0.0.1

PC>
```

Сурет 3.8-TCP / IP клиентінің конфигурациясы

Сайтты таңдау WWW.RAMBLER.RU браузерде клиентте (сурет 3.9):



Сурет 3.9-Клиенттің жұмысын тексеру

**Бақылау сұрақтары:**

1. DNS рекурсивті сұрау дегеніміз не және оның жұмыс схемасы қандай?
2. DNS тура және кері аймақтарындағы ресурстық жазбалардың типтерінің арналуын көрсетіңіз.
3. DNS серверінде басқа DNS серверге пакеттерді жіберу қалай бағталады?
4. DHCP қызметінің жұмысын сипаттаңыз.
5. DHCP клиенті қалай реттеледі?
6. Web торап және FTP сервері бар қалтаның орналасқан жерін көрсетіңіз.
7. Корпоративтік желідегі DNS сервердің кері аймақтарының құрамы қалай анықталады?
8. Cisco Packet Tracer-да DNS қызметін орнатуды көрсетіңіз?
9. Cisco Packet Tracer-де DHCP қызметін орнатыңыз ба?
10. Cisco Packet Tracer-де FTP қызметін орнатыңыз ба?
11. Cisco Packet Tracer Web Серверін орнатуды көрсетіңіз бе?

#### 4 БӨЛІМ. CISCO IOS ОПЕРАЦИЯЛЫҚ ЖҮЙЕСІНІҢ НЕГІЗГІ КОМАНДАЛАРЫ

Желілік жабдықты баптау үшін сіздің иелігіңізде Cisco IOS операциялық жүйесінің әртүрлі командалары бар.

Желілік құрылғыға кіргенде командалық жол көрінеді:

```
Switch>
```

Теңшелетін деңгейде қол жетімді командалар артықшылықты режимде қол жетімді командалардың ішкі жиыны болып табылады. Бұл пәрмендер желілік құрылғының орнатуын өзгертпей, ақпаратты экранға шығаруға мүмкіндік береді.

Командалардың толық жиынтығына кіру үшін алдымен артықшылық режимін белсендіру керек.

```
Press ENTER to start.
```

```
Switch>
```

```
Switch> enable
```

```
Switch#
```

Артықшылықты режимнен шығу:

```
Switch# disable
```

```
Switch>
```

Артықшылықты режимге өту туралы командалық жолда # белгісі түрінде шақыру пайда болуын көрсетеді.

Артықшылық деңгейден жүйенің параметрлері туралы ақпаратты алуға және интерфейсті, ішкі интерфейсті, желіні, желілік құрылғыны, маршруттар картасын және т. б. қоса алғанда, жаһандық конфигурациялау режиміне және басқа да арнайы конфигурациялау режимдеріне қол жеткізуге болады.

IOS жүйесінен шығу үшін пернетақтада exit (шығу):

```
Switch> exit
```

Келесі режимдерде жұмыс істеуге болады:

- Пайдаланушы режимі-бұл пайдаланушы тек желілік құрылғы туралы белгілі бір ақпаратты көре алатын, бірақ ештеңе өзгерте алмайтын көру режимі. Бұл режимде шақыру түрі:

```
Switch>
```

- Артықшылық режим-баптау және тестілеу пәрмендерін, желілік құрылымын егжей-тегжейлі тексеруді, конфигурациялық файлдармен манипуляцияны және конфигурациялау режиміне қатынауды қолдайды. Бұл режимде шақыру түрі:

Switch#

- Жаһандық конфигурациялау режимі-конфигурациялау міндеттерін шешетін қуатты бір жолдық командаларды іске асырады. Осы режимде шақыру түрі:

Switch(config)#

IOS кез келген режимінде командалар бірінші бірегей символмен таниды. IOS табуляциясын басқан кезде команданы толық атауына дейін өзі толықтырады.

Енгізген кезде командалық жолда кез-келген режимін атындағы командасының белгісі және мәселені (?) экранға командаға түсініктеме шығады. Бір тақбаны енгізгенде, нәтиже барлық режим командаларының тізімі болады. Экранда көптеген жолдар экрандары пайда болуы мүмкін, сондықтан кейде экранның төменгі жағында

- More-кеңестер пайда болады. Жалғастыру үшін enter немесе бос орын басу керек.

Жаһандық конфигурация режимінің командалары жүйенің жалпы тәртібін анықтайды. Сонымен қатар, жаһандық конфигурация режимдерінің командалары көпқұрылымды командаларды талап ететін конфигурацияларды жасау үшін қолданылатын конфигурациялаудың басқа режимдеріне өту командаларын қамтиды. Жаһандық теңшеу режиміне кіру үшін айрықша configure режимі қолданылады. Бұл пәрменді енгізгенде теңшеу командаларын көрсету керек:

- terminal (терминал),
- memory (энергияға тәуелді жады немесе файл),
- network (TFTP сервері (Trivial file-оңайлатылған file) желіде).

Әдепкі командалар консоль терминалынан енгізіледі, мысалы:

Switch(config)#(commands)

Switch(config)#exit

Switch#

Конфигурацияның жеке түрін белсендіруге арналған командалар жаһандық конфигурациялау командаларымен алдын ала жасалуы тиіс. Осылайша, шақыруды көрсететін интерфейс конфигурациясы үшін

Switch(config-if)#

алдымен интерфейс түрін және оның портының нөмірін анықтау үшін жаһандық команда енгізіледі:

```
Switch#conf t  
Switch(config)#interface type port  
Switch(config-if)#(commands)  
Switch(config-if)#exit  
Switch(config)#exit
```

### **Зертханалық жұмыс №3. IOS командаларымен танысу.**

#### **Желілік құрылғының негізгі командалары**

1. Router1 желілік құрылғысына кіріңіз

```
Router>
```

2. Біз осы режимде барлық қол жетімді командалар тізімін көргіміз келеді. Барлық қол жетімді командаларды қору үшін пайдаланылатын команданы енгізіңіз:

```
Router>?
```

Enter пернесін басудың қажеті жоқ.

3. Енді артықшылықты режимге кіріңіз

```
Router>enable  
Router#
```

4. Қол жетімді командалар тізімін артықшылықты режимде қарап шығыңыз

```
Router#?
```

5. Конфигурация режиміне өтіңіз

```
Router#config terminal  
Router(config)#
```

6. Желілік құрылғының хост аты жергілікті идентификациялау үшін пайдаланылады.

Желі құрылғысына кіргенде, режим (">" немесе"#") символының алдында хост атауын көресіз. Бұл атау орналасқан жерді анықтау үшін пайдаланылуы мүмкін.

"Router1" желілік құрылғының аты ретінде орнатыңыз.

```
Router(config)#hostname Router1
```

Router1(config)#

7. Кіру паролі сізге артықшылық берілген рұқсатқа кіруді бақылауға мүмкіндік беретін режим. Бұл өте маңызды құпия сөз, себебі артықшылық режимде конфигурациялық өзгерістер енгізуге болады. "Parol" кіру паролін орнатыңыз.

Router1(config)#**enable password parol**

1. Бұл құпия сөзді көрейік. Желілік құрылғыдан шығып, артықшылықты режимге кіруге тырысыңыз.

2.

Router1>**en**

Password:\*\*\*\*\*

Router1#

Мұнда белгілер: \* \* \* \* \* - бұл енгізілген құпия сөз. Бұл белгілер экранда көрінбейді.

### **Негізгі Show командалары.**

Disable командасымен теңшелетін режимге өтіңіз. Барлық қол жетімді show командаларын көру үшін пәрменді енгізіңіз.

Router1>**show ?**

1. Show version командасы желілік құрылғы платформасының түрін, операциялық жүйенің нұсқасын, операциялық жүйенің бейне файлының атауын, жүйенің жұмыс уақытын, жады көлемін, интерфейсгер санын және конфигурациялық регистр алу үшін қолданылады.

2.Уақытты қарау:

Router1>**show clock**

3. Желілік құрылғының флеш-жадында Cisco IOS операциялық жүйесінің файл-бейнесі сақталады. Оперативтік жады қарағанда, нақты құрылғыларда флеш жады қорек істен шыққан кезде де файл-бейнесі сақтайды.

Router1>**show flash**

4. Әдепкі бойынша желілік құрылғының АКЖ соңғы енгізілген 10 команданы сақтайды

Router1>**show history**

5. Екі команда бұрын енгізілген командаларға оралуға мүмкіндік береді. Жоғары көрсеткіні немесе <ctrl> P түймесін басыңыз.

6. Екі команда буферде сақталған келесі командаға өтуге мүмкіндік береді.

Төмен көрсеткіні басыңыз немесе <ctrl> N

7. Олардың барлық интерфейстерінің хостер тізімі мен IP-мекен-жайларын көруге болады

Router1>**show hosts**

8. Келесі команда әрбір интерфейс туралы толық ақпаратты шығарады

Router1>**show interfaces**

9.Келесі команда әрбір telnet сессиясы туралы ақпаратты шығарады:

Router1>**show sessions**

10. Келесі команда терминалдың конфигурациялық параметрлерін көрсетеді:

Router1>**show terminal**

11. Терминалдық желілер арқылы құрылғыға қосылған барлық пайдаланушылардың тізімін көруге болады:

Router1>**show users**

12. Команда

Router1>**show controllers** интерфейс контроллерлерінің күйін көрсетеді.

13.Артықшылықты режимге өтіңіз.

Router1>**en**

14. Барлық қол жетімді show командаларын көру үшін пәрменді енгізіңіз.

Router1#**show ?**

Артықшылығы бар режимге пайдаланушы режимінің барлық командалары және бірқатар жаңалары кіреді.

15. Желілік құрылғының жадындағы белсенді конфигурацияны көрейік. Артықшылық режимі қажет. Белсенді конфигурация автоматты түрде сақталмайды және қуат көзі істен шыққан жағдайда жоғалады. Роутер баптауларын сақтау үшін келесі пәрмендерді пайдаланыңыз:

ағымдағы конфигурацияны сақтау:

Router# **write memory**

немесе

Router# **copy run start**

Сақталған конфигурацияны қарау:

Router# **Show configuration**

немесе

Router1#**show running-config**

More жолында келесі ақпарат бетін көру үшін бос орын пернесін басыңыз.

16. Келесі команда ағымдағы хаттама жағдайын көруге мүмкіндік береді

үшінші деңгейдегі:

Router#**show protocols**

### **Интерфейстер конфигурациясына кіріспе.**

Желілік құрылғының интерфейстерін баптау командаларын қарастырайық.

1.Router 1 желілік құрылғысында теңшеу режиміне кіріңіз:

Router1#**conf t**

Router1( config)#

2. Енді біз Ethernet интерфейсін баптағымыз келеді. Ол үшін біз интерфейс конфигурациясы режиміне кіру керек:

Router1(config)#**interface FastEthernet0/0**

Router1( config-if)#



3. Осы режимде қол жетімді барлық командаларды көрейік:

```
Router1(config-if)#?
```

Жаһандық конфигурация режиміне шығу үшін exit теріңіз. Интерфейстің теңшелім режиміне қайта кіріңіз:

```
Router1(config)#int fa0/0
```

Біз қысқартылған интерфейс атауын қолдандық.

4. Әрбір команда үшін біз оған no сөзін қойған қарама-қарсы командаларды орындай аламыз. Келесі команда осы интерфейсін қамтиды:

```
Router1(config-if)#no shutdown
```

5. Сипаттама интерфейсін қосыңыз:

```
Router1(config-if)#description Ethernet interface on Router 1
```

Осы интерфейсін сипаттамасын көру үшін, артықшылықты режим және show interface командасын орындаңыз:

```
Router1(config-if)#end
```

```
Router1#show interface
```

6. Енді Router 2 желілік құрылысына қосылып, Router2-ге оның хост атын өзгертіңіз:

```
Router#conf t
```

```
Router(config)#hostname Router2
```

FastEthernet 0/0 интерфейсін кіреміз:

```
Router2(config)#interface fa0/0
```

Интерфейсті қосыңыз:

```
Router2(config-if)#no shutdown
```

Енді біздің Ethernet қосылымының екі шетінде интерфейсін қосылған кезде экранда интерфейсін күйін белсенді күйге ауыстыру туралы хабар пайда болады.

7. Тізбекті интерфейсін конфигурациясына өтіңіз. Router1-ге қошеміз.

Тізбекті байланыс желісі үшін біздің маршрутизаторымыз қандай құрылғы екенін тексереміз: DTE (data terminal equipment) соңғы құрылғысы немесе DCE (data circuit) байланыс құрылғысы):

```
Router1#show controllers fa0/1
```

Егер хабарлама көрсек:

```
DCE cable
```

біздің маршрутизатор байланыс құрылғысы болып табылады және ол деректерді беру кезінде қолданылатын тактілік импульстерді синхрондау жиілігін көрсетуі тиіс. Жиілік белгілі бір жиілік қатарынан алынады.

```
Router1#conf t
```

```
Router1(config)#int fa0/1
```

```
Router1(config-if)#clock rate ?
```

64000 жиілігін таңдаймыз

```
Router1(config-if)#clock rate 64000
```

және интерфейсті қосамыз

```
Router1(config-if)#no shut
```

### **Бақылау сұрақтары:**

1. Роутердің ағымдағы баптауларын қандай командамен көруге болады?
2. Роутердің желілік интерфейсі қандай командалармен реттеледі.
3. Коммутатордың конфигурациялық параметрлерін қалай көруге болады?
4. Вилландардың коммутатор порттары бойынша таралуын қалай анықтауға болады?
5. Коммутаторды баптау кезінде конфигурацияның негізгі режимдерін атаңыз.
6. Роутерді баптау кезінде конфигурацияның негізгі режимдерін атаңыз.
7. Роутердегі маршруттау кестесін қалай көруге болады?
8. Роутер маршруттау кестесін қандай командалар қалыптастырады?
9. Коммутатордағы вилландар қандай командалармен теңнеледі?
10. Вилландар арасындағы өзара әрекеттесуді қандай командалар реттейді?

## 5 БӨЛІМ. СТАТИКАЛЫҚ МАРШРУТТАУ

Маршрутизация хаттамалары-бұл маршрутизаторлар арасында пакеттерді тарау жолдары туралы ақпарат алмасу жүзеге асырылатын ереже. Хаттамалар жинақтылық уақытымен, шығындармен және масштабтаумен сипатталады. Қазіргі уақытта бірнеше маршрутизация протоколдары қолданылады.

Маршрутизатордың басты міндеттерінің бірі берілген адресатқа ең жақсы жолды анықтаудан тұрады. Маршрутизатор адресаттарға немесе әкімшілік енгізген статикалық конфигурациядан немесе басқа маршруттардан алынған маршруттар ақпараттың негізінде динамикалық түрде жолды (маршруттарды) анықтайды. Маршрутизаторлар маршруттық ақпаратпен маршруттау хаттамаларының көмегімен алмасады.

Маршрутизатор маршруттар кестесін жедел жағдайға сақтайды. Маршруттар кестесі-ең танымал маршруттар тізімі. Маршрутизатор бұл кестені пакетті қайда жіберуге негізін қабылдау үшін пайдаланады.

Статикалық маршруттау жағдайында әкімші қолмен межелі тораптарға маршруттарды анықтайды.

Динамикалық маршруттау жағдайында-маршруттаушылар маршруттар туралы ақпарат алмасу және ең жақсы жолды таңдау үшін маршруттау хаттамаларымен анықталатын ережелерді басшылыққа алады.

Статикалық маршруттар маршрутизатордың өзі өзгермейді. Динамикалық маршруттарды маршрутизатордың өзі көрші маршруттардан маршруттарды ауыстыру туралы ақпаратты алған кезде автоматты түрде өзгертеді. Статикалық маршрутизация аз есептеуіш ресурстарды тұтынады және арналардың адресатына бірнеше жолы жоқ желілерде пайдалы. Егер маршрутизатордан маршрутизаторға бір ғана жол болса, онда статикалық маршрутизацияны жиі қолданады.

Бұл жағдайда, маршрутизатор мысалы, Cisco IOS операциялық жүйесінің командалық жолында конфигурацияланады. Маршрутизаторға қосылу Telnet арқылы оның кез келген интерфейстерінің IP-адресіне немесе кез келген терминалдық бағдарламаның көмегімен компьютердегі маршрутизатордың консольдік портымен байланысты дәйекті порт арқылы жүзеге асырылады. Соңғы тәсіл жақсырақ, себебі маршрутизаторды конфигурациялау процесі IP-интерфейс параметрлерін өзгерте алады, бұл Telnet арқылы орнатылған байланыстың жоғалуына алып келеді. Сонымен қатар, қауіпсіздік мақсатында Telnet арқылы маршрутизаторға кіруге тыйым салу керек.

Осы күрс шеңберінде маршрутизаторлардың конфигурациясы терминал арқылы жүзеге асырылады.

Cisco IOS командалық жолында жұмыс істеу кезінде бірнеше контекст бар (командаларды енгізу режимдері).

Әдетте желі арқылы қосылғанда құпия сөз талап етіледі, ал консоль порты арқылы қосылғанда құпия сөз қажет емес. Осы мәтінменге әкімші

контекстінде енгізу ұзақ болмаған кезде командалық жол автоматты түрде ауысады. Пайдаланушы контекстінде маршрутизатордың конфигурациясына әсер етпейтін қарапайым командалар (мониторинг үшін кейбір негізгі операциялар) ғана қол жетімді. Командалық жолды шақыру түрі:

```
router>
```

Router сөзінің орнына маршрутизатор аты көрсетіледі.

Әкімші контексті ("exec" контексті) пайдаланушы контекстінде берілген enable командасымен ашылады; әдетте әкімші паролі талап етіледі. Администратордың контекстінде маршрутизатордың конфигурациясы және оның жағдайы туралы толық ақпарат алуға мүмкіндік беретін командалар, конфигурациялау режиміне көшу командалары, конфигурацияны сақтау және жүктеу командалары бар. Командалық жолды шақыру түрі:

```
router#
```

Пайдаланушы контекстіне кері ауысу disable командасы бойынша немесе белгіленген уақыт өткеннен кейін жүргізіледі. Жұмыс сеансын аяқтау-exit командасы.

Ғаламдық теңшеу контекстін әкімші контекстінде берілген config terminal ("терминал арқылы теңшеу") командасы ашады. Ғаламдық теңшеу контекстінде тікелей маршрутизаторды теңшеу пәрмендері де, мысалы, маршрутизатордың кіші жүйелерін теңшеу контекстіне оту пәрмендері де бар:

интерфейсті теңшеу контексті

interface имя\_интерфейс (мысалы, interface serial0) командасымен ашылады;

динамикалық бағыттау процесін теңшеу контексті

router командасымен ашылады номер\_процесса протоколы (мысалы, жаһандық теңшеу контекстінде берілген router ospf 1.

Көптеген басқа теңшеу контекстері бар. Кейбір теңшеу контекстері басқа теңшеу контекстерінің ішінде болады.

Ең жиі кездесетін теңшеу контекстіндегі командалық жолды шақыру түрі:

```
router (config)# / жаһандық/
```

```
router (config-if)# / интерфейс/
```

router (config-router)# /динамикалык багыттау/

router (config-line)# / терминалдык желі/

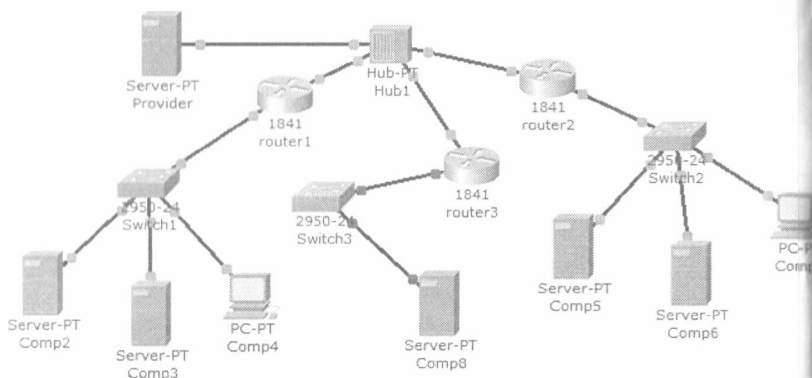
#### Зертханалық жұмыс №4. Статикалық маршруттауды реттеу.

Cisco Packet Tracer интерфейсінң графикалық шеберлерінің көмегімен статикалық маршруттауды реттеңіз.

5.1 суреттегі желі схемасын жасаңыз.

Бұл схемада келесі компоненттерден тұратын корпоративтік желі ұсынылған:

1 желісі-Switch 1 желісі бірінші ұйымның желісі тұйықталады (5.1-кесте):



Сурет 5.1-Желі схемасы

5.1 кесте-Бірінші ұйымның желісі

Компьютер	IP мекен-жайы	Функциялары
Comp 2	192.168.1.2/24	DNS және HTTP сервері
Comp 3	192.168.1.3/24	DHCP сервері
Comp 4	DHCP серверінен алынды	Желі клиенті

Бұл желіде Comp2-ге DNS және ұйым сайты бар Web сервер орнатылған.

Comp 3-те DHCP сервері орнатылған. Comp 4 компьютері DHCP серверінен IP мекен-жайын, провайдер серверінің DNS мекен-жайын (Provider сервері) және шлюзді алады.

Желідегі шлюз-192.168.1.1 / 24.

2-Желі Switch 2-ге екінші ұйымның желісі тұйықталады (5.2-кесте):

### 5.2 кесте-Екінші ұйымның желісі

Компьютер	IP мекен-жайы	Функциялары
Comp 5	10.0.0.5/8	DNS және HTTP сервері
Comp 6	10.0.0.6/8	DHCP сервері
Comp 7	DHCP серверінен алынды	Желі клиенті

Бұл желіде Comp 5-ке DNS және ұйым сайты бар Web сервер орнатылған.

Comp 4-те DHCP сервері орнатылған. Comp 7 компьютері DHCP серверінен IP мекен-жайын, провайдер серверінің DNS мекен-жайын (Provider сервері) және шлюзді алады.

Желідегі шлюз – 10.0.0.1/8.

3 желісі – Hub1 қалалық желі 200.200.0/24 тұйықталады. Желідегі барлық тораптар бойынша (Comp 2, Comp 5, Comp 8) деректерді қамтитын DNS провайдер сервері орнатылған (IP мекен-жайымен Provider компьютері -200.200.10/24).

4-Router 3 маршрутизаторы қалалық желіні Switch 3 коммутаторы арқылы интернетке шығарады (желі 210.210.210.0/24). Comp 8 (IP мекенжай 210.210.210.8 / 24, шлюз 210.210.210.3/24.) сайты бар DNS және Web сервер орнатылған.

Маршрутизаторлардың екі интерфейсі бар:

Router 1 – 192.168.1.1/24 және 200.200.200.1/24.

Router 2 – 10.0.0.1/8 және 200.200.200.2/24.

Router 3 – 210.210.210.3/24 және 200.200.200.3/24.

Тапсырма:

1-ұйымдар желісін текшеу;

2-DNS провайдер серверін текшеу;

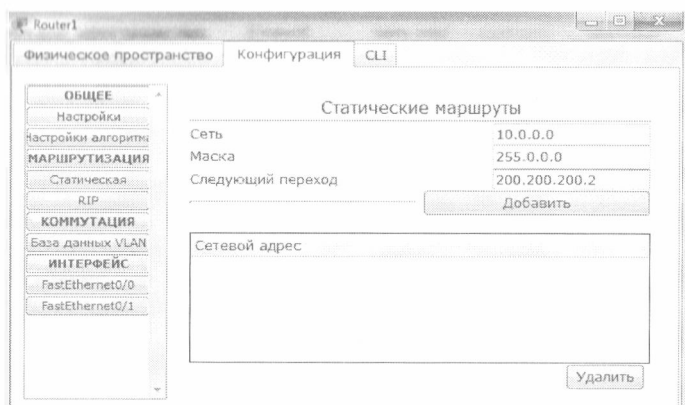
3-роутерлерде статикалық маршруттау кестелерін текшеу;

4-желі жұмысын тексеру - әрбір компьютер-Com4, Com7 және Com8. Олардың әрқайсысынан корпоративтік желінің барлық үш сайты ашылуы тиіс.

Алдығы зертханалық жұмыстарда желілік қызметтер мен сервердің DNS баптауы қарастырылды. Роутерлерде статикалық маршруттауды баптауға кірісеміз. Берілген схемада төрт желі болғандықтан, маршрутизация кестелері кем дегенде осы желілердің әрқайсысына жазулар болуы тиіс, яғни төрт жазба. Сонымен қатар, Cisco-да маршрутизацияның кестелерінен роутер интерфейстері қосылған желілерге жол жазылмайды. Сондықтан әрбір роутерде екі жазбаны енгізу қажет.

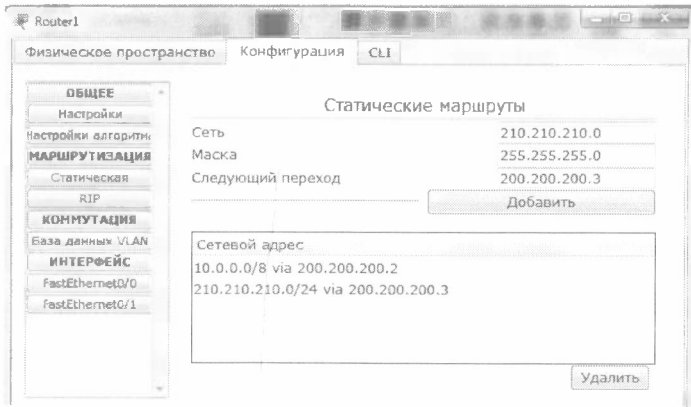
Бірінші роутерді баптаңыз.

Ол үшін маршрутизатордың конфигурациясына кіріңіз және интерфейсінде IP мекенжайы мен ішкі желі бетпердесін орнатыңыз. Содан кейін МАРШРУТИЗАЦИЯ бөлімінде статикалық қойындысын ашып, деректерді енгізіңіз (сурет 5.2) және Қосу түймесігін басыңыз:



Сурет 5.2-10.0.0.0/8 желісі үшін деректер

Нәтижесінде маршруттау кестесінде екі жазба болуы керек (сурет 5.3):



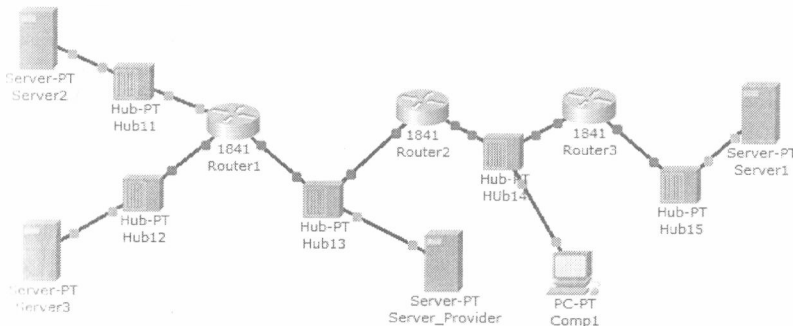
Сурет 5.3-Маршруттаудың статикалық кестесін қалыптастыру

Маршрутизация кестесінің Толық параметрін көру үшін, бүйірлік графикалық мәзірден тексеру құралын таңдаңыз (лупа пиктограммасы), роутер схемасын нұқып, ашылмалы мәзірден маршрутизация кестесі тармағын таңдаңыз.

Орнатқаннан кейін, барлық роутерлерді сіздің желі кол жетімді IP мекен-жайлары кез-келген компьютер және сіз ашу кез-келген сайт компьютерлер Comp 4, Comp 7 және Comp 8.

### Зертханалық жұмыс №5. Маршруттау кестелерін құру.

Сурет 5.4. ұсынылған желі схемасы келесі жұмысты өз бетіңше орындаңыз.



Сурет 5.4-Желі схемасы



Бес концентратор келесі бес желіні ұсынады:

Hub 11 – сеть 11.0.0.0

Hub 12 – сеть 12.0.0.0

Hub 13 – сеть 13.0.0.0

Hub 14 – сеть 14.0.0.0

Hub 15 – сеть 15.0.0.0

Router 1 опірулі роутер кезінде WIC-1ENET модулінен қосылатын қосымша желілік интерфейсі бар.

Желіде Server 1, Server 2 және Server 3 үш Web торап.

Серверлер мен компьютерлерде өз роутерлерінің шлюздері бар еркін IP мекен-жайлары бар.

Роутерлердің интерфейстері концентратордағы желімен және роутердің номірімен анықталады.

Мысалы, Router 3: 15.0.0.3 және 14.0.0.3

Тапсырма:

Comp 1 компьютері корпоративтік желі серверлерінде барлық үш сайтты ану керек. Comp 1 теншелімдерінде DNS сервері ретінде сервердің DNS сервері көрсетіледі.

#### **№ 1 өзіндік жұмыс**

15.0.0 / 8 корпоративтік желісі он шағын желіге бөлінген, оның ішінде қазіргі уақытта ұйымның алты түрлі бөлімшелерінде алты шағын желі іске қосылған.

Желі құрамы:

- үш маршрутизатор;
- алты коммутатор (әрбір бөлімде бір - бірден);
- әрбір желіде бір компьютер.

Тапсырма.

1-әрбір жеке желі ішіндегі IP мекенжайды, маска мен шлюзді есептеңіз және компьютерлерде орнатыңыз;

2-маршрутизаторларды кез келген ретпен жалғау арқылы желінің еркін топологиясын жасаңыз. Бұл ретте роутерлерді бөлімшенің штаттық коммутаторлары немесе қосымша коммутаторлар арқылы еркін-тікелей өзара жалғаңыз;

3-ping командасы корпоративтік желінің жұмысқа қабілеттілігін тексеріңіз – барлық компьютерлер қол жетімді болуы тиіс.

#### **Бақылау сұрақтары:**

1. Статикалық маршруттаудың артықшылықтары неде?
2. Маршруттаудың статикалық кестесінің параметрлеріне сипаттама беріңіз?

3. Құрылғыны орнату кезінде Cisco компаниясының маршрутизаторларына қандай кезеңдер тән, бірақ коммутаторларда жоқ?

4. Қай төменде көрсетілген командалардың кездестіруге болады интерфейсіңде командалық жолдың маршрутизатордың, бірақ коммутатор?

- cloc rate командасы;
- IP address маска мекен-жайы командасы;
- ip address dhcp командасы;
- interface vlan 1 командасы

5. Cisco компаниясының маршрутизаторы мен коммутаторының командалық жолының интерфейстері қандай?

6. Төменде көрсетілген пәрмендердің қайсысы құрылғыдағы IP мекен-жайлары мен бетбелгілерінің параметрлерін көрсетпейді?

- show running-config;
- show protocol түрі нөмірі;
- show ip interface brief;
- Show version

7. OSI моделінің деңгейлеріне сәйкес маршрутизатордың негізгі функцияларын атаңыз.

8. Қолдану саласы бойынша маршрутизаторлардың жіктелуін келтіріңіз.

9. Маршрутизаторлардың негізгі техникалық сипаттамаларын атаңыз.

10. Cisco компаниясының маршрутизаторларының негізгі серияларына сипаттама беріңіз.

11. Маршрутизация хаттамаларының тізімін келтіріңіз және оларға қысқаша сипаттама беріңіз.

12. Жергілікті және жаһандық желілер үшін маршрутизаторлар қолдайтын интерфейстер тізімін келтіріңіз және олардың мақсатын анықтаңыз.

13. Маршрутизаторлармен қолдау көрсетілетін желілік хаттамалардың тізімін келтіріңіз және олардың мақсатын анықтаңыз.

## 6 БӨЛІМ. ДИНАМИКАЛЫҚ МАРШРУТТАУ

Статикалық бағыттау үлкен, күрделі желілер үшін жарамсыз, өйткені желілерде әдетте артық сілтемелер, көптеген хаттамалар және аралас топологиялар болады.

Күрделі желілердегі маршрутизаторлар топологияның өзгеруіне тез бейімделіп, көптеген үміткерлердің ішінен ең жақсы бағытты таңдауы керек.

IP желілері иерархиялық құрылымға ие. Маршруттық желі тұрғысынан автономды жүйелер жиынтығы ретінде қарастырылады. Ірі желілердің автономды ішкі жүйелерінде басқа автономды жүйелерге бағыттау үшін әденкі маршруттар кеңінен қолданылады.

Динамикалық бағыттауды бір немесе бірнеше хаттамалардың көмегімен орындауға болады. Бұл хаттамалар көбінесе қолданылатын желілеріне қарай топтастырылады. Автономды жүйелер ішінде жұмыс істеуге арналған протоколдар ішкі шлюз хаттамалары (IGP), ал автономды жүйелер арасында жұмыс істеуге арналған хаттамалар сыртқы шлюз хаттамалары (EGP) деп аталады. IGP хаттамаларына RIP, RIP v2, IGRP, EIGRP, OSPF және IS-IS кіреді. EGP3 және BGP4 хаттамалары EGP-ге байланысты. Барлық осы хаттамаларды екі классқа бөлуге болады: қашықтық-векторлық хаттамалар және байланыс күйінің протоколдары.

### **Қашықтықтан-векторлық маршруттау.**

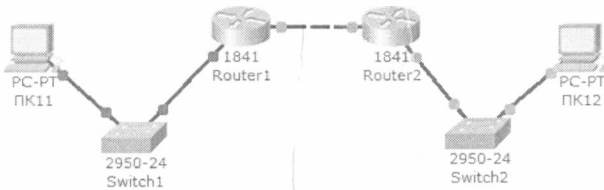
Маршрутизаторлар маршруттарды бағалау немесе өлшеу үшін метрикаларды қолданады. Маршрутизатордан тағайындалған желіге көптеген маршруттар болған кезде және олардың барлығы бірдей маршруттау протоколын қолданса, ең аз метрикалық маршрут ең жақсы болып саналады. Егер маршруттаудың әртүрлі протоколдары қолданылса, маршрутты таңдау үшін маршрутизатордың операциялық жүйесі тағайындайтын әкімшілік қашықтықтар пайдаланылады. RIP метрика ретінде өтулер санын (хоп) пайдаланады.

Қашықтық-векторлық бағыттау Белман-Форд алгоритміне негізделген. Белгілі бір уақыт өткеннен кейін маршрутизатор өзінің барлық кестесін көрші маршрутизаторларға жібереді. RIP және IGRP сияқты қарапайым протоколдар маршруттық кесте туралы ақпаратты белгілі бір көрші маршрутизатордың нақты мекен-жайын көрсетпей, хабарлау режиміндегі барлық маршрутизатор интерфейсі арқылы жай ғана тарағады.

Жақын орналасқан маршрутизатор таратылым кезінде ақпаратты қазіргі маршрут кестесімен салыстырады. Оған жаңа желілерге бағдарлар немесе белгілі желілері бар маршруттар қосылады. Жоқ маршруттарды жояды. Маршрутизатор алынған бағдарлардың өлшемдеріне өз мәндерін қосады. Маршруттың жаңа кестесі көрші маршрутизаторларға қайтадан таралады.

## № 6 зертханалық жұмыс. RIP теңшеу

6.1 суретте көрсетілген тізбекті жасаңыз.



Сурет 6.1-Желі схемасы

Схемада келесі үш желі бар:

Switch 1 – желі 10.11.0.0/16.

Switch 2 – желі 10.12.0.0/16.

Роутерлерге арналған желі - 10.10.0.0/16.

Құрылғыларда келесі адресацияны енгізіңіз:

Маршрутизаторлардың екі интерфейсі бар:

Router 1 – 10.11.0.1/16 және 10.10.0.1/16.

Router 2 – 10.10.0.2/16 және 10.12.0.1/16.

ПК 11 - 10.11.0.11/16 .

ПК 12 - 10.12.0.12/16 .

Router 1 маршрутизаторында RIP протоколын баптауды жүргіземіз.

Маршрутизатордың консоліне конфигурацияны енгізіп, келесі параметрлерді орнатыңыз (командаларды енгізу кезінде ішкі желі маскасын жіберуге болады, өйткені ол маршрутизатор интерфейсінің параметрлерінен автоматты түрде алынады):

Артықшылықты режимге кіріңіз:

```
Router1>en
```

Конфигурация режиміне кіріңіз:

```
Router1>#conf t
```

RIP протоколын теңшеу режиміне кіріңіз:

```
Router1(config)#router rip
```

Клиенттік желіні роутерге қосыңыз:

```
Router1(config-router)#network 10.11.0.0
```

Екінші желіні роутерға қосыңыз:

```
Router1(config-router)#network 10.10.0.0
```

Rip протоколының екінші нұсқасын пайдалануды орнатыңыз:  
Router 1(config-router)#**version 2**

Rip протоколын теңшеу режимінен шығыңыз:  
Router 1(config-router)#**exit**

Параметрлер консолінен шығыңыз:  
Router 1(config)#**exit**

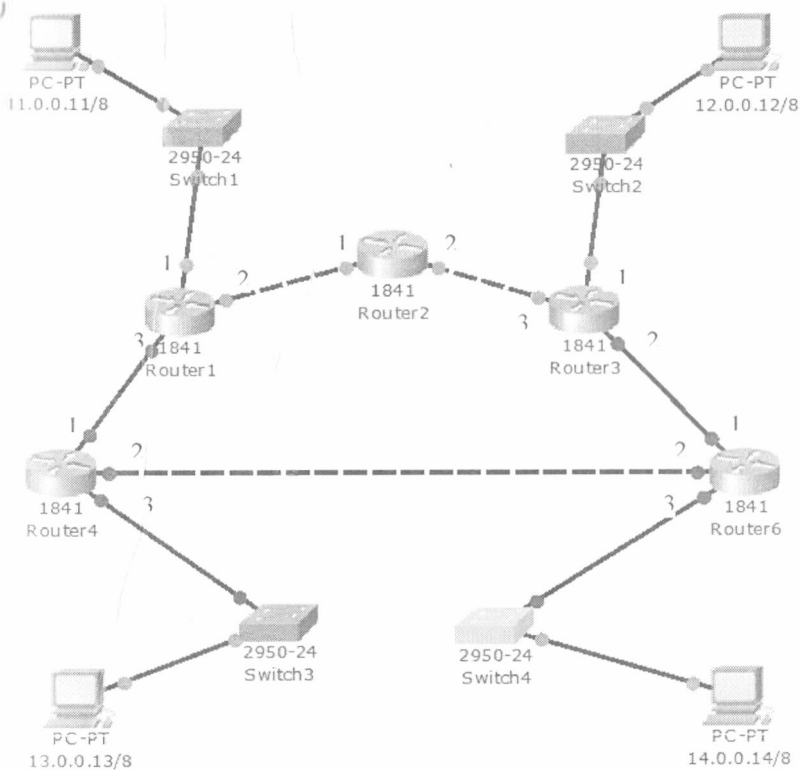
Параметрлерді маршрутизатор жадына сақтаңыз:  
Router 1>#**write memory**

Сол сияқты Router 2 маршрутизаторында RIP протоколын реттеңіз.  
ДК 11 және ДК 12 компьютерлері арасындағы ring байланысын тексеріңіз.

Егер Байланыс болса - барлық параметрлер дұрыс жасалған.

**Зертханалық жұмыс №7. Корпоративтік желіде RIP хаттамасын  
тестішеу.**

6.2. суреттегі сызбаны жасаңыз



Сурет 6.2 - Желі схемасы

Төрт желіде: 11.0.0.0/8, 12.0.0.0/8, 13.0.0.0/8 және 14.0.0.0 / 8 мекен-  
жайлары бар компьютерлер орнатылды:

Сomp 1 – 11.0.0.11, маска 255.0.0.0

Сomp 2 – 12.0.0.12, маска 255.0.0.0

Сomp 3 – 13.0.0.13, маска 255.0.0.0

Сomp 4 – 14.0.0.14, маска 255.0.0.0

Олардың арасында алты маршрутизаторы бар корпоративтік желі бар.

Маршрутизаторларда келесі интерфейстер берілген:

### 6.1 кесте-Маршрутизаторлардағы интерфейстер түрлері

Маршрутизатор	Интерфейс 1	Интерфейс 2	Интерфейс 3
Router 1	11.0.0.1/8	21.0.0.1/8	31.0.0.1/8
Router 2	21.0.0.2/8	51.0.0.2/8	
Router 3	12.0.0.3/8	61.0.0.3/8	51.0.0.3/8
Router 4	31.0.0.4/8	81.0.0.4/8	13.0.0.4/8
Router 6	61.0.0.6/8	81.0.0.6/8	14.0.0.6/8

Әрбір роутерде RIP хаттамасы бойынша маршруттауды реттеңіз.

Ол үшін:

1- №6 зертханалық жұмыста көрсетілгендей барлық маршрутизаторларды баптаңыз;

2-маршруттау кестесі бойынша маршрутизаторларды баптауды тексеріңіз.

Маршрутизатордың дұрыс конфигурацияланғанына көз жеткізу үшін маршрутизатордың RIP кестесін қараңыз. дұрыс жұмыс істейді, шоу командасын келесідей қолданыңыз:

```
Router#show ip route rip
```

Мысалы, Router6 алтыншы маршрутизаторы үшін кесте келесідей болады (сурет 6.3):

```
Router6>en
Router6#show ip route rip
R   11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R   12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R   13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R   21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
                        [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R   31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R   51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Сурет 6.3 - RIP маршруттау кестесі

Бұл кестеде 21.0.0.0 желісіне екі жол бар: Router 4 арқылы (81.0.0.0 желісі) және Router3 арқылы (61.0.0 желісі).

Желі диагностикасын жүргізіңіз:

1-әрбір компьютердің консолінде ping және tracert командаларының көмегімен дұрыс баптауды тексеріңіз;

2-Router 6 маршрутизаторы өшірілген кезде сол желіні диагностикалаңыз.

3-12.0.0.12 және 13.0.0.13 мекен-жайлары бар компьютерлер арасындағы байланысты тексеріңіз.

6 қосылған және ажыратылған роутер кезінде пакеттен оту кезіндегі аралық роутерлер саны әртүрлі болуы тиіс. Router 6 қосылған кезде ажыратылғанға қарағанда бір бірлікке аз болуы тиіс.

## **№ 2 өзіндік жұмыс**

6.4 суреттегі сызбаны жасаңыз.

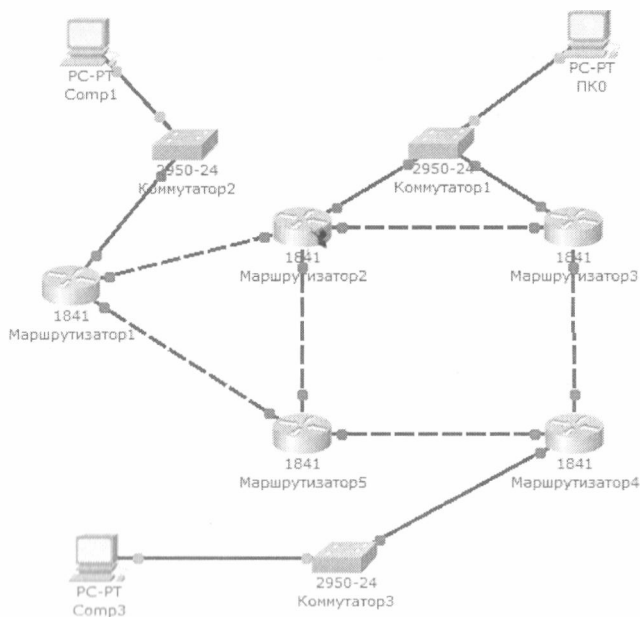
Тапсырма.

1. Корпоративтік желіні RIP протоколы арқылы реттеңіз.

2. Ping және tracert пәрмендері арқылы Comp 1 және Comp 3 компьютерлері арасындағы байланысты маршрутизатор қосулы және өшірілген кезде тексеріңіз.

3. PING және tracert командаларының көмегімен ДҚО және Comp 1 компьютерлері арасындағы байланысты тексеріңіз.





Сурет 6.4-Желі схемасы

### Байланыс жай-күйінің хаттамалары.

Бұл протоколдар қапшықтық векторлық протоколдармен салыстырғанда жақсырақ масштабталу мен конвергенцияны ұсынады. Хаттамалардың жұмысы көбінесе «бірінші қысқа жол SPF» алгоритмі деп аталатын Дикстра алгоритміне негізделген. Ең типтік өкіл - OSPF (Open Shortest Path First) протоколы.

Маршрутизатор желідегі басқа маршрутизаторлардың интерфейстерінің байланыс күйін ескереді. Маршрутизатор өз аймағындағы байлапыстың барлық күйлері туралы толық мәліметтер базасын жасайды, яғни желінің жеке картасын жасау үшін жеткілікті ақпарат бар. Әр маршрутизатор содан кейін маршрут кестесіне енетін ең жақсы жолды анықтау үшін SPF алгоритмін өз желілік картасында немесе байланыс күйлерінің деректер базасында дербес орындайды. Бұл желілер басқа желілерге жергілікті маршрутизатор түрінде шыңы бар ағашты құрайды.

Маршрутизаторлар осы аймақтағы барлық маршрутизаторларға қосылу күйі туралы хабарлайды. Бұл хабарлама LSA (сілтеме күйіндегі жарнама) деп аталады.

Қашықтықтан-векторлық маршрутизаторлардан айырмашылығы, байланыс жағдайының маршрутизаторлары өз көршілерімен арнайы қарым-қатынас жасай алады.

LSA пакеттерінің алғашқы байланыс ағындары бар, олар байланыс күйлерінің мәліметтер базасын құруда. Әрі қарай маршруттар байланыс жағдайы өзгерген кезде немесе белгілі бір уақыт аралығында өзгермеген жағдайда ғана жаңартылады. Егер байланыс күйі өзгерсе, дереу ішінара жаңарту жіберіледі. Онда маршрут кестесі толығымен емес, өзгерген сілтеме күйлерін ғана қамтиды.

Байланыс желілерін қолданумен айналысатын әкімші осы жартылай және сирек жаңартуларды қашықтық векторларының бағытына тиімді бағана деп санайды, ол бүкіл маршрут кестесін тұрақты түрде жібереді. Байланыс күйінің протоколдары қашықтық векторлық протоколдармен салыстырғанда жылдамдық конвергенцияға және өткізу қабілеттілігіне ие. Олар кез-келген мөлшердегі желілер үшін қашықтық-векторлық хаттамадан жоғары, бірақ олардың екі кемшілігі бар: маршрутизаторлардың есептеу қуаттылығына және кешенді басқаруға қойылатын талаптар.

## Зертханалық жұмыс №8. OSPF протоколын теңшеу.

6.1 суретте көрсетілген желі схемасын алыңыз.

Router 1 маршрутизаторында OSPF протоколын баптауды жүргіземіз.

Кіріңіз конфигурация бұл консоль роутера орындаңыз келесі параметрлерді (іске қосу кезінде команда ішкі желі бүркенішін көрсетпеуге болады, т. к. ол жұмыста автоматты түрде орнату процесінен интерфейс роутера):

Артықшылықты режимге кіріңіз:

```
Switch>en
```

Конфигурация режиміне кіріңіз:

```
Switch1#conf t
```

OSPF протоколын теңшеу режиміне кіріңіз:

```
Router1(config)#router ospf 1
```

Router ospf < id\_процесса> id астында әрбір процесс үшін бірегей санын мән маршрутизатордағы роутинг. Бұл мән 1-ден 65535-ке дейінгі аралықта көп болуы тиіс. OSPF-да бір аймақтың роутерлеріндегі үдерістер бір-бірі идентификаторды беру қабылданды.

Клиенттік желіні роутерге қосыңыз:  
Router1(config-router)#**network 10.11.0.0**

Екінші желіні роутерға қосыңыз:  
Router1(config-router)#**network 10.10.0.0**

OSPF протоколының екінші нұсқасын пайдалануды орнатыңыз:  
Router1(config-router)#**version 2**

OSPF протоколын теңшеу режимінен шығыңыз:  
Router1(config-router)#**exit**

Параметрлер консолінен шығыңыз:  
Router1(config)#**exit**

Параметрлерді маршрутизатор жадына сақтаңыз:  
Switch1#**write memory**

Сол сияқты Router2 маршрутизаторында OSPF протоколын реттеңіз.

#### **Бақылау сұрақтары:**

1. Топологиялық және қанықтықтан-векторлық маршруттаудың арасындағы айырмашылық неде?
2. RIP протоколының жұмыс сызбасын сипаттаңыз.
3. OSPF протоколының жұмыс сызбасын сипаттаңыз.
4. Маршрутизаторды орнатудың негізгі кезеңдерін атаңыз.
5. Маршрутизаторды жүктеудің төрт кезеңін сипаттаңыз.
6. Төменде көрсетілген хаттамалардың қайсысы қанықтықтан-векторлық алгоритм бойынша жұмыс істейді және олардың негізгі айырмашылықтары қандай?
  - RIP;
  - IGRP;
  - EIGRP;
  - OSPF
7. Маршруттау хаттамаларының кластарына сипаттама беріңіз.
8. Олардың жұмыс алгоритмдері негізінде маршрутизация хаттамаларының жіктелуін келтіріңіз.
9. Класс және сыныптан тыс маршруттау хаттамаларын салыстырыңыз.
10. Ішкі шлюзді маршруттау хаттамаларын салыстырыңыз.
11. Rip-2 маршруттау протоколын баптау кезеңдерін сипаттаңыз.

## 7 БӨЛІМ. NAT ҚЫЗМЕТІ.

NAT (Network Address Translation) - желілік мекен-жайларды аудару, IP-мекен-жайларды және желілік пакеттердегі порттарды түрлендіруге (өзгертуге) мүмкіндік беретін технология.

NAT көбінесе корпоративті желіден (үйден) Интернетке немесе керісінше Интернеттен желідегі кейбір ресурстарға қол жеткізу үшін қолданылады.

Кәсіпорын желісі әдетте жеке IP мекен-жайларында құрылады. RFC 1918 сәйкес жеке мекенжайларға үш блок бөлінді:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))  
172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))  
192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Бұл мекен-жайлар Интернетте маршрутталмайды және провайдерлер жіберушілердің немесе алушылардың осындай IP мекен-жайлары бар пакеттерді тастауы тиіс.

Жеке мекенжайларды жаһандық (интернетте маршрутталатын) етіп өзгерту үшін NAT қолданылады.

Сыртқы желіге (Интернетке) қағынау мүмкіндіктерінен басқа, NAT-ның тағы бірнеше оң жақтары бар. Мысалы, желілік мекен-жайларды тарату желінің ішкі құрылымын жасыруға және оған қолжетімділікті шектеуге мүмкіндік береді, бұл қауіпсіздікті арттырады. Сонымен қатар бұл технология жаһандық IP мекенжайларын үнемдеуге мүмкіндік береді, өйткені Интернетке көптеген хостер шыға алады.

IOS басқаруындағы Cisco маршрутизаторларында NAT теңшеу келесі қадамдарды қамтиды

1. Ішкі (Inside) және сыртқы (Outside) интерфейстерді тағайындау

Ішкі интерфейс әдетте жергілікті желі қосылған. Сыртқы-сыртқы желі қосылған, мысалы, интернет провайдер желісі.

2. Кім үшін (қандай ір мекенжай) трансляцияны жасау керек екенін анықтау.

3. Трансляцияның қай түрін пайдалану керек

4. Трансляцияларды тексеруді жүзеге асыру

Static NAT, Dynamic NAT, Overloading трансляциясының үш түрі бар.

Static NAT - статикалық NAT, IP-мекен-жайды бір-бірден аудару, яғни ішкі желінің бір мекен-жайы сыртқы желінің бір мекен-жайымен саныстырылады.

Dynamic NAT-динамикалық NAT, ішкі мекен-жайды сыртқы мекен-жай тобының біріне түрлендіру. Динамикалық трансляцияны пайдаланар алдында сыртқы мекен-жайлардың nat-пулын орнату керек.

Overloading — бірнеше ішкі мекен-жайларды біреуіне сыртқы түрлендіруге мүмкіндік береді. Бұл аударманы орындау үшін порттар қолданылады, сондықтан кейде бұл NAT PAT (Port Address Translation) деп аталады. PAT көмегімен сіз ішкі мекенжайларды пул арқылы немесе сыртқы интерфейстегі мекенжай арқылы көрсетілген сыртқы мекенжайға өзгерте аласыз.

NAT-ді баптауға арналған командалардың тізімі:

Интернет-интерфейсті белгілеу:

```
interface Fast Ethernet 0/0  
ip nat outside
```

жергілікті интерфейсін белгілеу:

```
interface Vlan1  
ip nat inside
```

NAT-қа қол жетімді IP-тізімді құру:

```
ip access-list extended NAT  
permit ip host 192.168.????.??? any
```

сыртқы интерфейсге NAT қосу:

```
ip nat inside source list NAT interface Fast Ethernet 0/0 overload
```

Сізге бар аудармаларды «show ip translations» командасымен қоруге болады.

Жоңдеу «debug ip nat» пәрменімен басталды.

Static NAT-ті теңшеу

```
router(config)#ip nat inside source static <local-ip> <global-ip>  
router(config)#interface fa0/4  
router(config-if)#ip nat inside  
router(config)#interface fa0/4  
router(config-if)#exit  
router(config)#interface s0  
router(config-if)#ip nat outside
```

Dynamic NAT-ті теңшеу

```
router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
```

```

router(config)#access-list <acl-number> permit <source-IP> [source-
wildcard]
router(config)#ip nat inside source list <acl-number> pool <name>
router(config)#interface fa0/4
router(config-if)#ip nat inside
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside

```

#### Overloading теңшеу

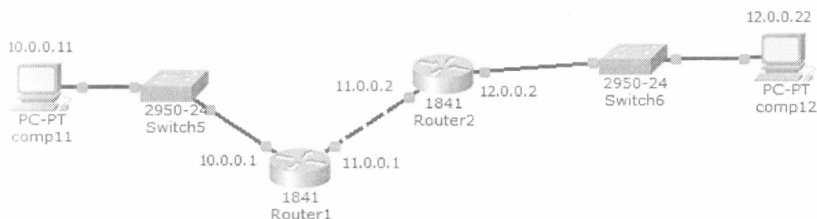
```

router(config)#access-list acl-number permit source-IP source-wildcard
router(config)#ip nat inside source list acl-number interface interface
overload
router(config)#interface fa0/4
router(config-if)#ip nat inside
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside

```

### Зертханалық жұмыс №9. NAT желілік мекен-жайын түрлендіру.

Бұл жұмыста ұйымның жергілікті желісінің компьютерлерін Интернетке шығару мәселесін шешу қажет. Жергілікті желі жеке адресацияда – 10.0.0.0 желісінде орнатылған, оның мекен-жайларында Интернетке шығу мүмкіндігі жоқ. Бұл тапсырманы шешу үшін NAT қызметін теңшеу қажет. Желі сұлбасы 7.1 суретте көрсетілген.

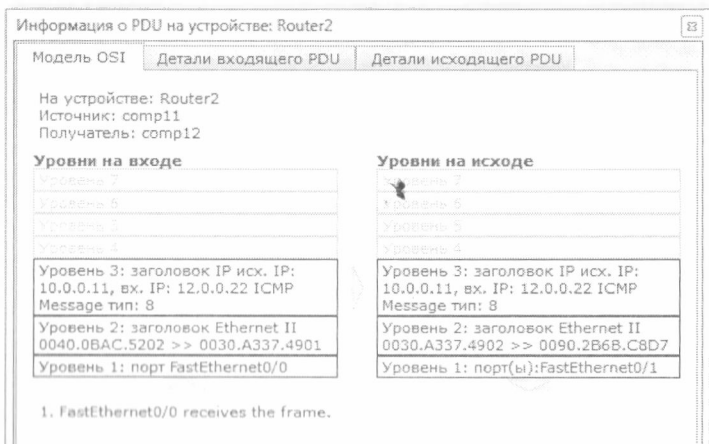


Сурет 7.1-Желі схемасы

1-суретте көрсетілген желіні құрыңыз. 1-суретте көрсетілгендей құрылғы атаулары мен мекен-жайларын орнатыңыз.

Қазіргі уақытта роутердағы NAT орнатылмаған, біз симуляция режимін пайдалана отырып, оған көз жеткізе аламыз.

Осы режимге өтіңіз және екі роутер арқылы өткен кезде пакеттің құрамын қараңыз (сурет 7.2).



Сурет 7.2-Router 2 оту кезінде бума параметрлері

Пакетті екінші маршрутизатор арқылы оту кезінде жіберушінің IP мекен-жайы өзгерген жоқ (10.0.0.11).

Nat Router 1 маршрутизаторында теңшеңіз.

Роутердегі NAT бантау үшін келесі қадамдарды орындау қажет:

1. Router1 параметрлеріне, CLI қойындысына кіру

2. Әкімші режиміне кіру үшін enable (en)

Router>en

Теңшеңу режиміне кіру үшін config t командасын енгізіңіз

Router#config t

3. Fast Ethernet 0/0 инттерфейсі жұмыс станциялары қосылған біздің ішкі инттерфейсіміз. Орнату үшін NAT арналған роутере қажет бұл анықтау параметрлері. Мұны келесі командалардың көмегімен жасауға болады:

инттерфейс параметрлеріне кіреміз:

Router(config)#**int Fast Ethernet 0/0**

инттерфейсті ішкі инттерфейспен жариялаймыз:

Router(config-if)#**ip nat inside**

инттерфейс параметрлерінен шығамыз

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

1. Сонымен қатар, провайдер желісіне қосылған FastEthernet 0/1 интерфейсін бантаймыз, ол NAT сыртқы интерфейсі болып табылады:

интерфейс параметрлеріне кіреміз:  
Router(config)#**int Fast Ethernet 0/1**

интерфейсті NAT сыртқы интерфейсімен жариялаймыз:  
Router (config-if)#**ip nat outside**

интерфейс параметрлерінен шығамыз:  
Router (config-if)#**exit**

2. Ішкі мекен-жайлар көрсетілетін сыртқы мекен-жайлар пулын тапсырамыз. Тек бір мекен – жайы бар пулды тапсыру үшін-роутер сыртқы интерфейсінің мекен-жайы-команданы енгізу қажет:

Router (config)#**ip nat pool natpool 11.0.0.0 11.0.0.1 netmask 255.0.0.0**

Мекен-жайлар пулын берген кезде пулга кіретін мекен-жай реттілігінің бірінші және соңғы мекен-жайын көрсету қажет. Егер пулда 1 мекен-жай (біздің жағдайда сияқты) оны 2 рет көрсету қажет.

3. Кіру тізімін орнатамыз:

Router (config)#**access-list 34 permit any**

**Маңызды:** 34-1-ден 99-ға дейінгі Сан кіру тізімінің № белгісін көрсетеді және әкімшімен орнатады. Алу-кілт сөз, кіру тізімі жіберушінің кез келген мекен-жайы бар пакеттерді шешеді дегенді білдіреді.

4. Соңында Router 0-де NAT қамтитын соңғы пәрменді енгіземіз. Команда, сөзсіз, пегізгі болып табылады, бірақ барлық алдыңғы параметрлерді тапсырмай, ол жұмыс істемейді.

Router (config)#**ip nat inside source list 34 pool natpool overload**

Бұл команда роутерге ішкі интерфейске алынған және рұқсат ету тізімімен рұқсат етілген барлық пакеттердің нөмірі 34, жіберушінің мекенжайы NAT пулынан "natpool" мекен-жайына таратылатынын айтады. Overload кілті бірнеше ішкі тораптарды бір IP мекен-жайына таратуға мүмкіндік беретін трансляциялар қайта жүктелгенін көрсетеді.

Енді NAT теңшелген. Кез келген жұмыс станциясынан сервердің ішкі желісіне пакетті пайдалана аламыз yandex.ru (пакет отеді). Егер біз



пакеттің отуін егжей-тегжейлі қарастыраак, онда router 1 арқылы пакетті өту кезінде жіберушінің мекен-жайы өзгергенін(NAT теңшелген) көреміз.

**Бакылау сұрақтары:**

1. NAT қызметінің барлық ықтимал жұмыс сызбаларын сипаттаңыз.
2. Әрбір мекенжай класында NAT қызметі қандай жеке IP мекен-жайларды қолданады?
3. NAT қызметінің артықшылықтары мен кемшіліктерін атаңыз.
4. NAT қызметін реттеу кезеңдерін атаңыз.
5. NAT қызметінің жұмысын тексеру сызбасын сипаттаңыз.
6. NAT сервері жұмысының негізгі мәселелерін сипаттаңыз.

## 8 БӨЛІМ. VLAN ВИРТУАЛДЫ ЖЕРГІЛІКТІ ЖЕЛІЛЕРІ.

Virtual Local Area Network (VLAN) немесе Виртуалды Жергілікті Желі – көптеген коммутаторлардың өмірін түбегейлі өзгерткен технология. Қазір бұл технология Ethernet желілеріндегі басты коммутация технологияларының бірі болып табылады. Виртуалды жергілікті желінің пайда болуы коммутация құралдарымен бір бірімен хабарласпайтын бірнеше топтарға бөліп бір коммутаторға қосылған қолданушыларды “виртуалды” бөлуге мүмкіншілік берді. Технология бір коммутатордың базасында тек қана белгілі бір топтардың қолданушылары арасында фреймдерді коммутациялай алатын бірнеше виртуалды логикалық коммутаторларды жасауға мүмкіндік бере алады. Топтар әртүрлі тәсілдер негізінде беріле алады, мысалы, MAC хост адресі бойынша немесе коммутатор портымен, не болмасы жұмыс алгоритмі келесідей көрсетілітін 802.1q хаттамасы арқылы. Бір топ ішіндегі клиент трафигі топтар арасында трафик тасымалы үшін маршрутизатор қажет болғанда, ешқандай некеуесіз коммутацияланады, коммутатордың өзінде бұл әкі сегментті байланыстыруға болмайды (ескерту: бұл жағдайда коммутатор OSI моделі бойынша үшінші дәреженің толық функционалы бола алмайды және дестелерді маршруттай алмайды).

*Виртуалды жергілікті желілердің жіктелінуі.* Виртуалды жергілікті желілердің көптеген түрлері бар, және де олардың арасындағы ерекшелігі – бұл сол не басқа станса немесе басқа құрылғы кез келген VLAN мүшесі болатын талап, бұл-мүшелікті иемдену талабы. Бірнеше мысал қарастырайық:

1) VLAN-дағы мүшелік станса қосылған порт нөмірі арқылы тағайындала алады. Осы станса хабарласатын басқа порттар да VLAN-ға қосылады.

2) VLAN нөмірі MAC құрылғы адрестерін басқара отырып белгіленуі мүмкін. Бұл жағдайда белгілі MAC адрестерінің белгілі VLAN-ға арнаулы кестені ұстау керек.

3) VLAN-ның сирек, бірақ маңызды түрлерінің бірі болып, VLAN-ға есенке қосу құрылғы беретін трафик бойынша өндірілетін желі табылады.

4) Қазір дамып жатқан бағыт қолданушылардың классификациясы және VLAN-ға тиісті логин мен пароль бойынша, бизнес-рольдер және жұмыс стансасына емес, қолданушыға қатысты басқа сипаттама бойынша олардың анықтамасы.

Есенке қосу белгісі бойынша VLAN динамикалық және статиткалық болып бөлінеді.

*Статикалық VLAN* – бұл сол немесе басқа VLAN-ға есенке қосуы коммутатордың жөнге келтірілуімен тығыз байланысты виртуалды жергілікті желі, және ол желі жүрісінің тәуелдігінен өзгере алмайды. Порт негізінде статикалық VLAN 5.1 суретте келтірілген.

Бұл жағдайда бір түсті порттарға жалғанатын стансалар өзара хабарласа алады, бірақ басқа түсті порттарға қосылған стансалармен хабарласа ала алмайды. Егер бір VLAN-ға қосылған станция басқа VLAN-ға тәуелді портқа қайта жалғанған болса, станса автоматты түрде басқа VLAN-ның мүшесі болады. Есепте VLAN бір коммутатор шегіде жұмыс істейді және MAC адресстар мәліметтер базасын коммутатордың жөнге келтіруінде қолмен жазуға тура келеді.

Статикалық VLAN-ның келесі артықшылықтары бар:

- өте тез және қарапайым конфигурациялау, ол MAC адресстардың таблица жазбасымен немесе нақтылы VLAN-ға керекті порттардың қарапайым енуімен шектеледі;

- статикалық VLAN желіде жоғары дәрежелі қорғау береді, желідегі кет келген өзгертулер коммутатордағы қайта конфигурациялаумен қосылуы керек. Қауіпсіздіктің әлсіз жері болып MAC адресстердің ауыстырылуы немесе басқа тәсілдермен жойылатын коммутаторға физикалық рұқсаттама болуы мүмкін;

- жеңіл конфигурациялау және жеткілікті қарапайым жұмыс алгоритмі, өз кезегінде мониторингтің жеңілділігін қамтамасыз етеді.

Кемшіліктер ішінде ең маңыздысы әлсіз масштабациялық болып табылады, статикалық VLAN порттар немесе MAC адресстармен бір коммутатордан артық жұмыс істемейді және stand-alone есептеуге ғана арналған, бұл желілік инфрақұрылымға компанияның осы уақыттағы талабын қайта жабады.

*Динамикалық VLAN* құрылғылардың қайта конфигурациясының топологияның өзгеруінде автоматты түрде қайта құрыла алу қабілеті бар.

Динамикалық VLAN-ды қолдау үшін әдетте мәліметтер базасының сервері қолданады, оларда барлық құрылғылар жайлы немесе желідегі қолданушы туралы ақпарат жатыр және қолданушының пайда болуында осы базаға байланысты ол өзі жататын VLAN-ға автоматты түрде түседі. Серверлерді қолданған кезде белгілі бір VLAN-ға енуінің сипаттамаларын таңдау еркі өте қатты оседі, себебі белгілі бір VLAN-дағы аутентификация мен авторизация процессін жүргізетін коммутатор емес, толықталып өзгере алатын сервердің бағдарламалық жабдықтауы. Солай, белгілі бір VLAN-ның белгілері болып тек MAC, IP адресстары немесе хаттама типі ғана емес, сол сияқты мысалға қолданушы аты, смарт-карттар, токендер, компьютер компоненттерінің сериялық нөмірлері немесе қолданушының саусақтар ізі. Белгілі бір VLAN-ға қабылдану үшін компания желісінде қауіпсіздік деңгейін өсіретін бірнеше сипаттамалар қолданылады. Коммутаторларда VLAN-ның үш түрі қолданылуы мүмкін және кеңтаралған домендер:

- база портындағы VLAN;

- MAC-адресстар базасындағы кеңтаралған домендер;

- стандарт IEEE 802.1Q қосымша кадр алаңының тапба негізіндегі VLAN.

*а) база портындағы VLAN.*

База портындағы VLAN-ды қолдану кезінде порт белгілі бір VLAN-ға беріледі, ол осы портқа қандай қолданушы не компьютер қосылғанына тәуілді емес. Бұл дегеніміз осы портқа қосылған барлық қолданушы бір VLAN-ның мүшесі болады. Порттар конфигурациясы статикалық және тек қолмен өзгере алады. Негізгі сипаттамалары:

- *көбінесе бір коммутатордың шамасында ғана қолданылады.* Егер бірнеше жұмысшы тобын үлкен емес желі шамасында бір коммутатор негізінде ұйымдастыру керек болса, мысалы, техникалық бөлім және сату бөлімін таратып жіберу қажет, сонда база портындағы VLAN шешімі берілген тапсырмаға қолайлы.

- *жөндеу қарапайымдылығы.* Порттардың топтасу негізінде виртуалды желілерді жасау әкімшіліктен үлкен көлемді қолды жұмысты сұрамайды – бір VLAN-дағы әр портқа бір идентификатор VLAN (VLAN ID) қою жеткілікті;

- *стансаның физикалық орналастыруынсыз желінің логикалық топологиясын өзгерту мүмкіндігі* – бір VLAN-нан (мысалы, техникалық бөлім VLAN-ны) екінші VLAN-ға (сату бөлімі VLAN-ны) порттар жөндеуін өзгерту жеткілікті, және жұмысшы станса тез арада ресурстарды жаңа VLAN мүшелерімен бірігіп қолдануға мүмкіншілік алады. Осылай, VLAN орналастыру, өзгерту және желі өсіруі кезіндегі икемділікті қамтамасыз етеді;

- *әр порт тек бір VLAN-ға кіре алады.* Сондықтан, виртуалды қосалқы желілерді біріктіру үшін – бір коммутатор ішіндегідей екі коммутатор арасында – IP деңгейін қолдану қажет: әр VLAN-ның бір порты маршрутизаторға қосылады және онда дестелерді бір қосалқы желіден екіншісіне қайта сілтеу үшін маршруттау кестесі құрастырылады.

Бұл шешімнің кемшілігі болып әр VLAN-ның бір портын маршрутизаторға қосу керек және бұнда порттар мен кабельдер ысырапшыл қолданылады, оған маршрутизаторға кеткен шығындар қосылады. Берілген мәселені екі жолмен шешуге болады: біріншісі, фирмалық шешім негізінде портты бірнеше VLAN-ға қосуға мүмкіндік беретін коммутаторларды қолдану керек. Екінші жолы 3-деңгейлі коммутаторларды қолдануда мәнін береді.

*б) MAC-адресстер базасындағы VLAN.*

Виртуалды желілерді жасау үшін қолданылатын екінші әдіс MAC-адресстерді топтауда негізделеді. Желіде үлкен көлемді түйіндердің болу кезінде бұл әдіс әкімшіліктен үлкен көлемді жұмысты талап етеді. Әдетте ол бірнеше коммутатор негізінде виртуалды желіні құруда порттарды топтау әдісіне қарағанда икемді болып келеді. Әр коммутаторда MAC-адресстерді желіге топтау олардың бірнеше портпен байланысының қажеттілігінен құтқарады, бірақ желіде әр коммутаторға MAC-адресстарды бүркеу үлкен көлемді қолдық операциялардың орындалуын талап етеді.

MAC-адрестер базасындағы кең таралған домендер стансалардың сол кең таралған доменде конфигурация өзгертуін өзгертпей-ақ қала отырып, оның физикалық орын ауыстыруын рұқсат етеді. MAC-адрестер негізінде виртуалды желілердің өзгертуі көп уақытты алуы мүмкін – сізге VLAN адресімен 1000 құрылғыны қосу керек болады. Одан басқа MAC-адресер құрылғыда “тас қылып қорғаулы” және үлкен территорияға таралған желіде құрылғы адресстерін анықтауға көп уақыт қажет болады.

*в) база таңбасындағы VLAN – 802.1Q стандарт.*

802.1q комитетінің жұмысы – бұл коммутация технологиясындағы үлкен жетістік деп айтуға болады, дамыған желелік құрылыммен берілген компаниялар сапы бұл нұсқаны VLAN колданады. Бұл технология көп желіге бадалақ және сыншыл болып келеді, ол кадрларды таңбалауға негізделген – коммутация туралы шешім қабылдау үшін қызметтік ақпаратта кадрларды толықтыру. Технологияны ары қарай талқылау үшін бірінен жаңа ұғымдарды енгізу керек:

- tagging – «таңбаланған» - 802.1q стандартымен VLAN-ның қатыстылығы туралы ақпаратты фреймге енгізу процедурасы;

- untagging – «таңбалабаған» - 802.1q стандартымен VLAN-ның қатыстылығы туралы ақпаратты кадрдан жою процедурасы;

- ingress port – кадрлар келетін және соңында таңбасы бар болуы мен VLAN-ға қатыстылығына және де таңбанығына туралы тексеру жүргізетін кіріс;

- egress port – таңбаланған немесе таңбалабаған туралы шешім қабылдағаннан кейінгі таңбалар бар болуына тексеруден өткен кадрлар шығатын шығыс порты.

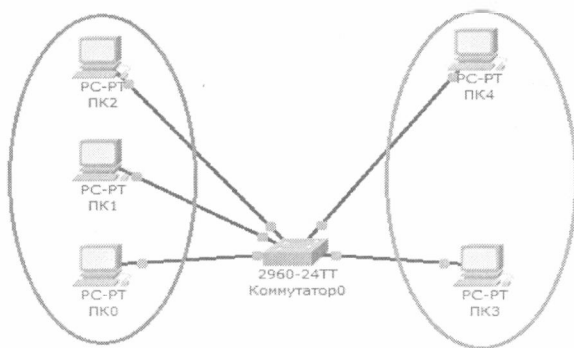
### **Зертханалық жұмыс № 10. Бір Cisco коммутаторында VLAN орнату.**

Бұл жұмыста Cisco қоя жеткізу порттарындағы VLAN-дің конфигурациясы талқыланады. 8.1 суретте логикалық топологиясы көрсетілген желіні құрыңыз. Компьютерлер Cisco 2960-24TT коммутаторы арқылы қосылады. 8.1 кестесінде компьютерлердің мекен-жайы көрсетілген.

Бұл жұмыстың мақсаты компьютерлердің екі тәуелсіз тобын құру: PC 0, PC 1 және PC 2 бір-біріне қол жетімді болуы керек, екінші тәуелсіз топ – PC 3 және PC 4 компьютерлері. Ол үшін екі бөлек VLAN құрыңыз (сурет 8.1).

VLAN 2

VLAN 3



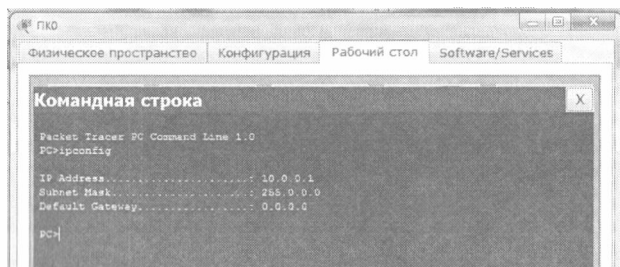
Сурет 8.1-Бір коммутатормен желі схемасы

#### 8.1 кесте- Компьютерлердің мекен-жайы

Компьютер	IP мекен-жайы	Коммутатор порты
ПК0	10.0.0.1/8	1
ПК1	10.0.0.2/8	2
ПК2	10.0.0.3/8	3
ПК3	10.0.0.4/8	4
ПК4	10.0.0.5/8	5

Есте сақтау керек келесі нәрсе – PC 0, PC 1 және PC 2 VLAN 2, ал PC3 және PC 4 VLAN 3 негізінде жасалған.

ПК 0 хост конфигурациясын тексеру үшін `ipconfig` командасын орындаңыз. 8.2 суретте команданы орындау нәтижесі. Қаласаңыз, басқа хосттарда ұқсас тексеруді орындауға болады.



Сурет 8.2-Хост конфигурациясын тексеру

PING командасын қолдана отырып, біз барлық компьютерлер арасындағы байланысты тексереміз. Қазір олар бір желіде және барлығы бір-біріне қол жетімді.

Енді коммутаторды желіні құрылымдау және оларды ретке келтіру үшін VLAN 2 және VLAN 3 теңшеуімен айналысамыз.

Бұдан әрі отелік орнату коммутатор. Оны консоль ашыңыз. Оны Packet Tracer-де орындау үшін жұмыс аймағындағы коммутатор бойынша тіптуірдің сол жақ батырмасын екі рет басыңыз.

Ашылған терезеде CLI қойындысына өтіңіз. Консоль терезесін көресіз. Пәрмендерді енгізу үшін Enter түймесін басыңыз. Қазіргі уақытта консольде көрсетілген ақпарат Fast ethernet 0/1 – FastEthernet 0/5 интерфейстері жұмыс істеп тұрғанын куәландырады.

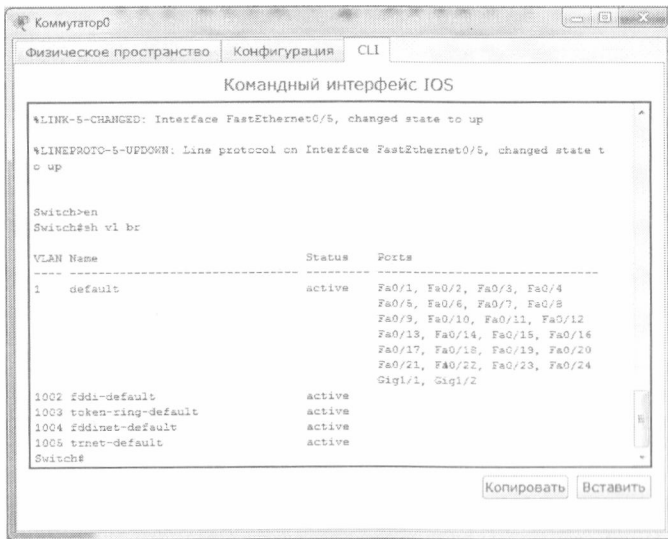
**Enable** командасын орындау арқылы артықшылықты режимге өтіңіз:

```
Switch>en  
Switch#
```

VLAN-ах коммутаторындағы бар ақпаратты қарастырайық (сурет 8.3).

Ол үшін келесі команданы орындаңыз:

```
Switch#sh vl br
```



Сурет 8.3-VLAN туралы ақпаратты коммутаторда қору

Пәрмендерді орындау нәтижесінде экранда мыналар пайда болады: VLAN нөмірлері - бірінші баған, VLAN атауы - екінші баған, VLAN мәртебесі (ол жұмыс істеп жатыр немесе жұмыс істемейді) - үшінші баған, осы VLAN-ға тиесілі порттар - төртінші баған. Көріп отырғанымыздай, әдепкі бойынша коммутаторда бес VLAN бар. Барлық ауысу порттары әдепкі бойынша VLAN 1-ге тиесілі, ал қалған төрт VLAN қызметтік және жиі пайдаланылмайды.

Біз оны іске асыру үшін коммутаторда тағы екі VLAN құрамыз. Бұл үшін артықшылықты режимде келесі пәрменді орындаңыз:

Switch#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# конфигурация режиміне оту үшін біз VLAN 2 пәрменін енгіземіз. Осы пәрменмен сіз коммутаторда VLAN 2 нөмірін жасайсыз. Кіріс көрсеткіші Switch (config) # ауыстырып қосқышқа (config-vlan) # ауысады, бұл сіз барлық коммутаторды тұтастай емес, тек жеке біреуін теңшейтіндігіңізді білдіреді. VLAN, бұл жағдайда VLAN нөмірі 2. Егер сіз «vlan x» пәрменін қолдансаңыз, онда x - VLAN нөмірі, егер коммутаторда VLAN x жасалмаса, ол автоматты түрде жасалады және оны теңшеуге кіріссіз. Сіз VLAN конфигурациялау режимінде болған кезде таңдалған виртуалды желінің параметрлерін өзгертуге болады, мысалы, атау командасын пайдаланып оның атын өзгертуге болады.



Осы лауазымда қойылған міндеттерге қол жеткізу үшін VLAN 2 теңшеу:

```
Switch (config)#vlan 2
Switch (config-vlan)#name subnet_10
Switch (config)#interface range fast Ethernet 0/1-3
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 2
```

Осы конфигурацияға талдау жасайық. VLAN 2 командасында айтылғандай, біз 2 коммутаторда жана VLAN құрамыз. Subnet\_10 атауы командасы subnet\_10 атауын виртуалды желі нөміріне 2 тағайындайды fast Ethernet 0/1-3 интерфейсі интерфейсін қолдана отырып, біз fast Ethernet 0/1, fast Ethernet 0/интерфейстерін баптауға кірісеміз. 2 және fast Ethernet 0/3 көккыштары. Бұл нәрмендегі диапазонның кілт сөзі біз бір портты емес, порттардың барлық ауқымын теңшейтінімізді білдіреді, оны жоққа шығаруға болды, бірақ содан кейін соңғы үш жолды ауыстыруға тура келеді:

```
Switch (config)#interface fastEthernet 0/1
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 2
Switch (config)#interface fastEthernet 0/2
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 2
Switch (config)#interface fastEthernet 0/3
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 2
```

**Switchport mode access** командасы таңдалған коммутатор портын (access порт) ретінде теңшейді.

Switchport access VLAN 2 командасы бұл порт VLAN нөмірі 2 үшін кіру порты екенін көрсетеді.

Конфигурациялау режимінен екі рет exit командасын теру және конфигурациялау нәтижесін көру арқылы шығыңыз (сурет 8.4) бізге таныс sh vl br командасын тағы бір рет орындап:

```

Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
2 subnet_10	active	Fa0/1, Fa0/2, Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```

Switch#

```

Сурет 8.4-VLAN-да портты орналастыру

Коммутаторда 2 нөмірімен және subnet\_10 атымен тағы бір VLAN пайда болды, ол fast Ethernet 0/1, fast Ethernet 0/2 және fast Ethernet 0/3.

Сонымен қатар, SUBNET\_192 атымен VLAN 3 жасап, оны fast Ethernet 0/4 және fast Ethernet 0/5 интерфейстеріне қатынау порттары жасайды. Нәтиже келесідей болуы керек (сурет 8.5):

```

Switch#sh vl br

```

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig1/1 Gig1/2
2 subnet_10	active	Fa0/1, Fa0/2, Fa0/3
3 subnet_192	active	Fa0/4, Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```

Switch#

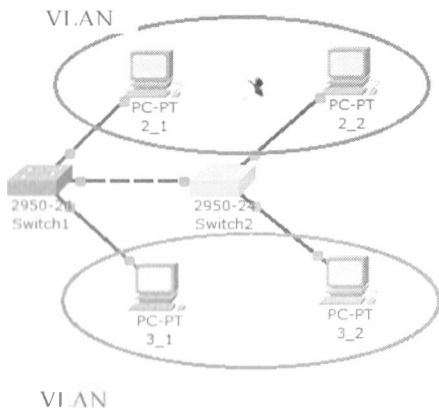
```

Сурет 8.5-VLAN-да портты орналастыру

Негізінен, бәрі дайын және біздің желі бапталған. Тек оны сынау ғана қалды. ДК 0 компьютер консоліне өтіңіз. Одан басқа желі компьютерлерін жіберіп алыңыз. ПК 1 және ПК 2 компьютерлері қол жетімді, ал ПК 3 және ПК 4 компьютерлері қол жетімді емес. Барлық бес компьютер теориялық түрде 10.0.0/8 бір ішкі желісінде болуы тиіс және бір-бірін қору керек, іс жүзінде олар әртүрлі виртуалды жергілікті желілерде болады және сондықтан өзара іс-қимыл жасай алмайды.

**Зертханалық жұмыс № 11. Екі Cisco коммутаторларында VLAN теңшеу.**

8.6 суретінде көрсетілгендей логикалық топологиясы бар желіні құрыңыз. Компьютерлер өзара Cisco 2950-24 коммутаторымен қосылған. 8.2 кестеде компьютерлердің мекен-жайлары келтірілген.



Сурет 8.6-Желі схемасы

8.2 кесте-Компьютерлердің мекен-жайлары

Компьютер	IP мекен-жайы	Коммутатор	Коммутатор порты	Вилан
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

Өрі қарай, 2\_1 және 2\_2 VLAN 20-да, ал 3\_1 және 3\_2 VLAN 30-да болады деп болжаймыз.

Алынған желінің қосылымын тексеріңіз. Мұны істеу үшін, біз барлық компьютерлерді 2\_1-тен аламыз. Осы уақытқа дейін желіде VLAN болу болмағандықтан, барлық компьютерлер қол жетімді болуы керек.

Енді желіні коммутаторларда құрылымдау үшін VLAN 20 және VLAN 30 баптаумен айналысамыз.

Switch 1 қосқышын баптауға өтіңіз. Консольді ашыңыз. Ашылған терезеде CLI қойындысына өтіп, артықшылықты режимге кіріңіз және 2-кестеге сәйкес VLAN 20 және VLAN 30 баптаңыз.

VLAN 20 коммутаторын жасаңыз. Бұл үшін артықшылықты режимде келесі пәрменді орындаңыз:

Switch1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch (config)# конфигурация режиміне өту үшін VLAN 20 және VLAN 30 теңшеу:

Switch 1(config)#vlan 20

Switch 1(config)#interface fast Ethernet 0/1

Switch 1(config-if-range)#switchport mode access

Switch 1(config-if-range)#switchport access vlan 20

Switch 1(config-if-range)#exit

Switch 1(config)#vlan 30

Switch 1(config)#interface fast Ethernet 0/2

Switch 1(config-if-range)#switchport mode access

Switch 1(config-if-range)#switchport access vlan 30

VLAN коммутаторындағы бар ақпаратты қарап шығыңыз:

Switch1#sh vl br

8.7. суретте көрсетілген нәтиже болуы керек.

```
Switch1#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1
30 VLAN0030	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch1#
```

Сурет 8.7-Switch 1 конфигурациясы

Switch 2-ді дәл осылай реттеңіз (сурет 8.8).

```
Switch2#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1
30 VLAN0030	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 usenet-default	active	

```
Switch2#
```

Сурет 8.8-Switch2 конфигурациясы

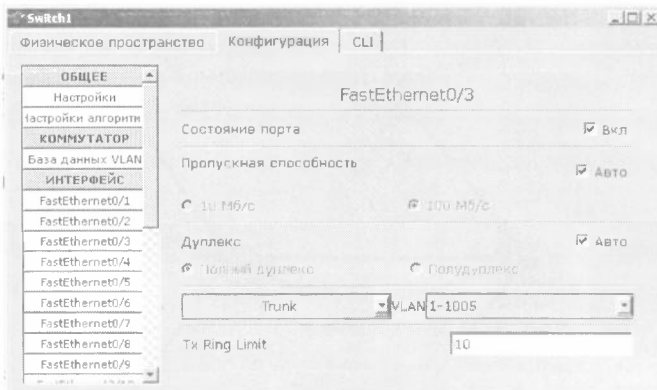
Қазіргі уақытта видалар туралы ақпарат алмасу болмағандықтан, компьютерлер тек өздерін тексереді.

Енді коммутаторлар арасында алмасу магистралін ұйымдастырамыз. Ол үшін әрбір коммутаторда үшінші портты ТРАНК ретінде баптаймыз.

Switch 1 коммутаторының консоліне кіріп, ТРАНК портын орнатыңыз:

```
Switch1>en  
Switch1#conf t  
Switch1(config)#interface fast Ethernet 0/3  
Switch1(config)#switchport mode trunk  
Switch1(config)#no shutdown  
Switch1(config)#exit
```

Коммутатор конфигурациясын Fast Ethernet 0/3 интерфейсінде ашыңыз және ТРАНК порты екеніне көз жеткізіңіз (сурет 8.9).



Сурет 8.9-Fast Ethernet 0/3 интерфейсінің конфигурациясы

Switch 2 коммутаторында Fast Ethernet 0/3 интерфейсі автоматты түрде транкалық ретінде бапталыды.

Енді бір вицланың құрамына кіретін компьютерлер пингке шығуы керек. Сізде 2\_1 және 2\_2 компьютерлері, сондай-ақ 3\_1 және 3\_2 арасында байланыс болуы керек. Бірақ басқа вицладағы компьютерлер қол жетімді болмайды.

Желі сызбасын сақтаңыз.

Енді маршрутизатор арқылы екі виртуалды желіні біріктіреміз.

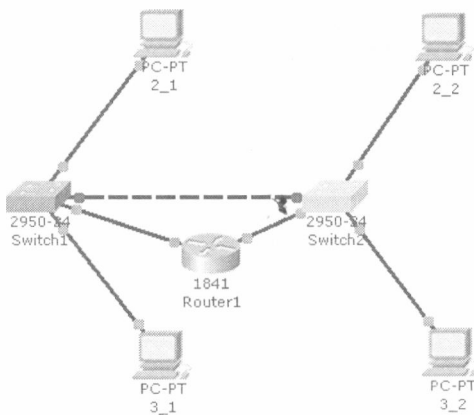
8.9 суретінде көрсетілгендей маршрутизаторды желі схемасына қосыңыз. Маршрутизатор fast Ethernet 0/4 коммутатор интерфейсімен қосылған.

Біздің 10.0.0.0 желісін екі желіге бөлшектеңіз: 10.2.0 және 10.3.0. Ол үшін 8.3-кестеде көрсетілгендей, IP мекен-жайы мен ішкі желі маскасын 255.255.0.0-ге ауыстырыңыз.

8.3 кесте- IP мекен-жайы түрлері

Компьютер	IP мекен-жайы	Коммутатор	Коммутатор порты	Вицлан
2_1	10.2.0.1/16	Switch 1	1	VLAN 20
2_2	10.2.0.3/16	Switch 2	1	VLAN 20
3_1	10.3.0.2/16	Switch 1	2	VLAN 30
3_2	10.3.0.4/16	Switch 2	2	VLAN 30

Компьютерлер бір виллан және бір ішкі желі шегінде орнатылуы тиіс.



Сурет 8.10-Желі схемасы

Коммутаторларда виртуалды желілерге маршрутизаторға қосылған интерфейстерді белгілейміз.

Бірінші Switch 1 коммутаторы конфигурациясына кіріп, төртінші порт параметрлерін орнатамыз:

```
Switch1(config)#interface fast Ethernet 0/4
Switch1(config-if)#switchport access vlan 20
```

Switch 1 бірінші коммутаторының параметрлерін тексеріңіз (сурет 8.11):

```
Switch1#sh vl br
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   VLAN0020                active    Fa0/1, Fa0/4
30   VLAN0030                active    Fa0/2
1002 fddi-default            active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default        active
Switch1#
```

Сурет 8.11-Switch 1 коммутаторының параметрлері

Екінші Switch 2 коммутаторының конфигурациясына кіріп, төртінші порт параметрлерін орнатыңыз:

```
Switch 2(config)#interface fast Ethernet 0/4
Switch 2(config-if)#switchport access vlan 30
```

Switch 2 екінші коммутаторының параметрлерін тексеріңіз (сурет 8.12):

```
Switch2#sh vl br
-----
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   VLAN0020                active    Fa0/1
30   VLAN0030                active    Fa0/2, Fa0/4
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default        active
Switch2#
```

Сурет 8.12-Switch 2 коммутаторының параметрлері

Маршрутизатор конфигурациясына кіріңіз және маршрутизатордағы IP мекен-жайды теңшеңіз:

```
Router 1 (config-if)#interface fa0/0
Router 1 (config-if)#ip address 10.2.0.254 255.255.0.0
Router 1 (config-if)#no shutdown
Router 1 (config-if)#interface fa0/1
Router 1 (config-if)#ip address 10.3.0.254 255.255.0.0
Router 1 (config-if)#no shutdown
```

Осы сәттен бастап біз екі желі арасында маршрутизацияны орнаттық. Компьютерлерде шлюздерді орнату қалды (8.4 кесте).

#### 8.4 кесте-Шлюз түрлері

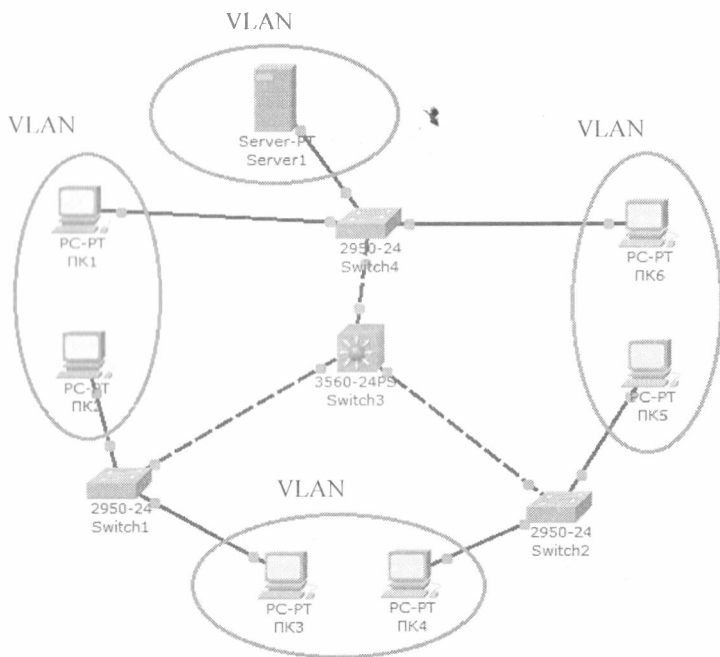
Компьютер	Gateway
2_1	10.2.0.254
2_2	10.2.0.254
3_1	10.3.0.254
3_2	10.3.0.254



Желідегі компьютерлердің болуын тексеріңіз. Енді барлық компьютерлер қол жетімді болуы керек және барлық мекен-жайлар пінгке салынуы керек.

**Зертханалық жұмыс № 12. Корпоративтік желіде VLAN орнату.**

Желінің келесі схемасын жасаңыз (сурет 8.12):



Сурет 8.12-Корпоративтік желі схемасы

Желі құрамы:

- 2950-24 екінші деңгейдегі үш коммутатор (Switch 1, Switch 2, Switch 4);
- үшінші деңгейдегі орталық 3560-24PS (Switch 3) коммутаторы, роутер рөлін атқаратын;
- сервер (Server 1);
- әрбір екі топты үш ішкі желі

Тапсырма:

Кез келген вилан үшін осы виланның тораптары мен Server1 сервері ғана қол жетімді болуы мүмкін.

8.5 және 8.6 кестелерде компьютерлер мен коммутаторлардың параметрлерін орнату үшін деректер келтірілген.

#### 8.5 кесте-Компьютер конфигурациясы

Компьютер	IP мекен-жайы	Коммутатор	Коммутатор порты	VLAN
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

#### 8.6 кесте-Коммутаторлардың порттар бойынша байланысы

Switch 3 орталық коммутатор порты	Екінші деңгейдегі тарату коммутаторының порты
1	Switch1 – 3 порт
2	Switch4 – 3 порт
3	Switch2 – 3 порт

Барлық коммутаторларды реттегеннен кейін барлық компьютерлерде және серверде шлюздерді өзіңіз орнатыңыз.

Орталық қосқышты теңшеңіз:

1 кезек.

Switch 3 орталық коммутаторының конфигурациясына өтіп, VLAN базасын жасаңыз.

1. VLAN 10 жасаңыз:

```
Switch 3>en
```

```
Switch 3#conf t
```

```
Switch 3(config)#vlan 10
```

```
Switch 3(config-vlan)#exit
```

2. VLAN 11, VLAN 12 және VLAN 13 жасаңыз.
3. VTP протоколын сервер режимінде теңшеңіз:

```
Switch 3(config)#vtp domain HOME
Switch 3(config)#vtp password HOME
Switch 3(config)#vtp mode server
```

4. VTP конфигурациясы туралы ақпаратты қараңыз:

```
Switch#sh vtp status
```

5. Барлық интерфейстерді транкка теңшеңіз:

```
Switch 3(config)#int fa0/1
Switch 3(config-if)#switchport mode trunk
Switch 3(config-if)#exit
```

екінші және үшінші интерфейстер үшін осы параметрлерді қайталаңыз.

2 кезең.

Switch 4 қосқышы конфигурациясына отіп, оны client режиміне қосыңыз:

1. VLAN 10 қосқышын жасап, access порты ретінде 1 портын орнатыңыз:

```
Switch 4>en
Switch 4#conf t
Switch 4 (config)#vlan 10
Switch 4 (config-vlan)#exit
Switch 4 (config)#int fa0/1
Switch 4 (config-if)#switchport access vlan 10
Switch 4 (config-if)#switchport mode access
Switch 4 (config-if)#no shut
```

2. VLAN 11 коммутаторын жасап, access порты ретінде 4 портын орнатыңыз.

3. VLAN 12 коммутаторын жасап, access порты ретінде 2 портын орнатыңыз.

4. Коммутаторды client режиміне көшіріңіз:

```
Switch 4 (config)#vtp domain HOME
Switch 4 (config)#vtp password HOME
```

#### Switch 4 (config)#vtp mode client

**Маңызды!** Домен мен құпия сөзді енгізгенде, қажетті регистрді сақтаныз.

3 кезең.

Switch 1 қосқышы конфигурациясына өтіп, келесі параметрлерді орындаңыз:

1. VLAN 11 коммутаторын жасап, access порты ретінде 1 портын орнатыңыз.
2. VLAN 13 коммутаторын жасап, access порты ретінде 2 портын орнатыңыз.
3. Коммутаторды client режиміне көшіріңіз.

4 кезең.

Switch 2 коммутаторының конфигурациясына өтіңіз.

1. VLAN 12 коммутаторын жасап, access порты ретінде 2 портын орнатыңыз.
2. VLAN 13 коммутаторын жасап, access порты ретінде 1 портын орнатыңыз.
3. Коммутаторды client режиміне көшіріңіз.

5 кезең.

OSI моделінің арна деңгейінде желінің жұмыс істеу қабілетін тексеріңіз.

Барлық параметрлерді орнатқаннан кейін VLAN кестесі VTP протоколы арқылы коммутаторлар арқылы кетеді.

Нәтижесінде бір вилланда орналасқан компьютерлер бір-біріне қол жетімді болады, ал басқа компьютерлер қол жетімді емес. Келесі жұптар арасындағы PING командасының байланысын тексеріңіз:

- ПК1 – ПК2;
- ПК3 – ПК4;
- ПК5 – ПК6.

Егер сіз бәрі дұрыс жасалса, онда жұптар арасындағы ping өтеді, егер жоқ болса – келесі параметрлерді тексеріңіз:

- ТРАНК порттары: Switch 3 барлық порттар, Switch 1, Switch 2 және Switch 4-үшінші порт;
- коммутаторлардағы интерфейсдерді қосу;
- әр коммутаторда домендердің атаулары мен парольдері (sh vtp status командасы);
- коммутаторларда вилландарға интерфейсдерді байланыстыру (sh vl br командасы).

6 кезең.

Орталық коммутаторда маршруттауды баптау.

Әрбір VLAN үшін интерфейстер жасаңыз.  
VLAN 10 үшін интерфейсін теңшеу (әдепкі шлюз):  
Switch 3(config)#**int vlan 10**  
Switch 3(config-if)#**ip address 10.10.0.1 255.255.0.0**  
Switch 3(config-if)#**no shut**  
Switch 3(config-if)#**exit**

Осы параметрлерді әрбір VLAN үшін IP мекен-жайымен қайталаңыз:  
10.[VLAN].0.1 және маска/ 16.

Осыдан кейін, әрбір компьютердің параметрлеріне кіріп, әдепкі шлюзді орнатыңыз. Мысалы, ПК1-10.11.0.1 үшін.

Нәрменді бағыттауды қосыңыз:  
Switch 3(config)#**ip routing**

7 кезең.

OSI моделінің желілік деңгейінде желінің жұмыс істеу қабілетін тексеріңіз.

Іске қосылғаннан кейін барлық компьютерлер кез келген хост қол жетімді болады.

8 кезең.

Жұмыстың негізгі міндетін орындайық: кез-келген вилаңга тек бірдей вилаң мен Server1 серверінің түйіндері қол жетімді.

Ол үшін желі трафигіне келесі шектеулер енгіземіз:

1 - кез келген хост пакеттерді серверге рұқсат ету.

2 - кез келген хост серверден пакеттерді рұқсат ету.

3 - Трафик Бір желіден сол желіден рұқсат етілсін.

4 - әдетті ереже: қалғандарына тыйым салу.

Желілік трафикке шектеулер кіру тізімінің access-list сүзгі нәрменін қолдану арқылы орнатылады. Бұл команда қатынасу тізімі деп аталатын қосу және ажырату параметрлерінің тізімінде сүзу шарттарын орнатады. Кіру тізімдерінде екі ереже бар: permit - рұқсат беру және deny- жокқа шығару. Бұл ережелер пакетті одан әрі желі арқылы өткізеді немесе оған қол жеткізуді бұғаттайды.

Қол жеткізу тізімі №14 зертханалық жұмыста егжей-тегжейлі қарастырылады.

Орталық коммутаторды (Switch 3) ашамыз және access-list сүзгілеу командасының көмегімен оның конфигурациясын өзгертеміз:

Switch 3(config)#**ip access-list extended 100**

(100 нөмірімен кеңейтілген кіру тізімі жасалады)

Switch 3(config-ext-nacl)#**permit ip any 10.10.0.0 0.0.0.255**

```
Switch 3(config-ext-nacl)#permit ip 10.10.0.0 0.0.0.255 any  
(желіге қол жеткізуге рұқсат етіледі 10.10.0 / 24)
```

```
Switch 3(config-ext-nacl)#permit ip 10.11.0.0 0.0.0.255 10.11.0.0  
0.0.0.255
```

```
Switch 3(config-ext-nacl)#permit ip 10.12.0.0 0.0.0.255 10.12.0.0  
0.0.0.255
```

```
Switch 3(config-ext-nacl)#permit ip 10.13.0.0 0.0.0.255 10.13.0.0  
0.0.0.255
```

(рұқсат етіледі: 10.11.0/24 желісінен сол желіге қатынау;  
10.12.0/24 желісінен сол желіге қатынау;  
10.13.0.0/24 желісінен сол желіге қатынау).

```
Switch 3(config-ext-nacl)#exit
```

Енді бұл access-list нақты интерфейске салып, кіріс трафигіне барлық VLAN-ларға қолданылады (кіріс трафигіне in опциясы, out – Шығыс трафигіне):

```
Switch 3(config)#int vlan 10
```

```
Switch 3(config-if)#ip access-group 100 in
```

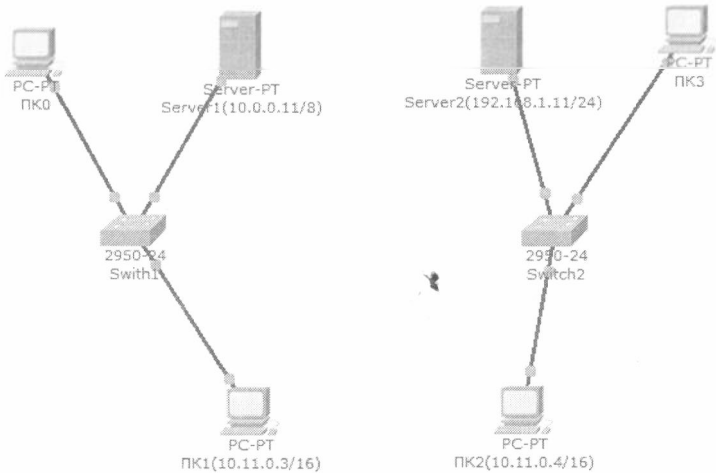
Бұл қадам әрбір VLAN үшін қайталанады.

Нәтижесінде біз мыналарды аламыз:

кез келген вилан үшін сол вилан мен Server 1 серверінің түйіндеріне ғана қол жеткізуге болады.

### **№ 3 өзіндік жұмыс.**

Компанияда екі бөлім бар, олардың желілік схемасы 8.13 суретте көрсетілген



Сурет 8.13-Кәсіпорын бөлімдері желілерінің схемасы

1 бөлім - Switch 1, 2 бөлім-Switch 2.

Әрбір желіде DHCP, DNS және HTTP қызметтері бар сервер бар (Server 1 және Server 2 серверлерінде бөлімдердің интернет-сайттары орналасқан).

Оз желілерінің DHCP серверлері бар ДК 0 және ПК 3 компьютерлері IP мекенжай және шлюз параметрлерін алады.

ДК 1 және ДК 2 компьютерлері бір VLAN жеке желісінде.

Тапсырма:

Келесі режимдерде корпоративтік желі жұмысын қамтамасыз ету үшін маршрутизатормен немесе үшінші деңгейлі коммутатормен желі сызбасын толықтырыңыз:

- 1-компьютерлер ПК 0 және ПК 3 әр бөлімнің сайттарын ашу керек;
- 2-ДК 1 және ДК 2 компьютерлері тек бір-біріне қол жетімді болуы керек.

#### Бақылау сұрақтары:

1. Виртуалды жергілікті желілер не үшін жасалады? Олардың артықшылықтары қандай?
2. VLAN және коммутатор порттары өзара қалай байланысады?
3. Әр түрлі виртуалды желілердің тораптары арасындағы қарым-қатынас қалай қамтамасыз етіледі?

4. Виртуалды Жергілікті желілерді басқару қалай қамтамасыз етіледі?

5. Бірнеше коммутаторда VLAN құруға бола ма? Оны қалай жасауға болады?

6. Кадр идентификаторы (tag) не үшін қолданылады? Қайда орналастырылады?

7. Транк дегеніміз не? Ол коммутатор мен маршрутизаторда қалай құрылады?

8. VLAN интерфейстеріне тағайындау үшін қандай командалар қолданылады?

9. ТРАНК қосылыстарын құру үшін қандай командалар қолданылады?

10. VLAN верификациясы үшін қандай командалар қолданылады?



## 9 БӨЛІМ. БІРНЕШЕ ЖҰМЫС РЕЖИМІ.

Cisco Packet Tracer бағдарламасында командалық жұмысты ұйымдастыру үшін қолданылатын бірнеше режим функциясы қолданылуы мүмкін.

Бұл жұмыс режимі Cisco Packet Tracer бағдарламасының әр түрлі сессияларында бір немесе әр түрлі компьютерлерде бір уақытта құрылған желілерге қосылуға мүмкіндік береді. Нәтижесінде, мысалы, әртүрлі компьютерлерде бірнеше жұмыс режимін пайдалана отырып, бірыңғай корпоративтік желіге біріктірілуі мүмкін корпоративтік желінің жеке сегменттері құрылуы мүмкін.

### Зертханалық жұмыс № 13. Бірнеше жұмыс режимі.

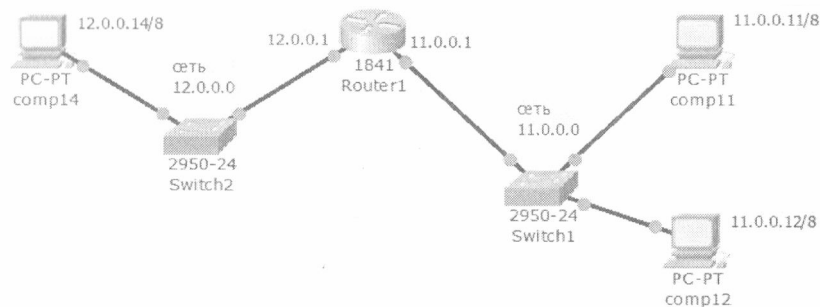
Бұл жұмыста біз бір компьютерде Cisco Packet Tracer бағдарламасының екі бөлек сессиясында құрылған екі түрлі желілер негізінде біртұтас желіні құруды көрсетеміз.

Сіз Cisco Packet Tracer бағдарламасының екі бір уақытта жұмыс істейтін сессияларын жасап, оны екі рет іске қосасыз.

Бағдарламаның бірінші ашық сессиясында екі желі құрылып, бапталады: желі 1-11.0.0.0 және желі 2 - 12.0.0.0. Бағдарламаның екінші сессиясында-11.0.0 желісі.

#### 1 сессияда жұмыс

Cisco Packet Tracer (бірінші сессия) бағдарламасын іске қосыңыз және 9.1 суреттегі сұлба бойынша екі желіні (11.0.0.0 және 12.0.0.0 желісі) құрыңыз:



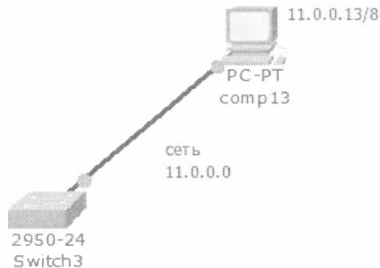
Сурет 9.1-Бірінші сессия-11.0.0.0 және 12.0.0.0.желілері

Сызбада көрсетілгендей құрылғы ағауын орнатыңыз.

Схемада көрсетілгендей, TCP/IP протоколының параметрлерін және comp 11, comp12 және comp 14 компьютерлеріне арналған шлюздерді орнатыңыз (сурет 9.1).

## 2 сессияда жұмыс 2

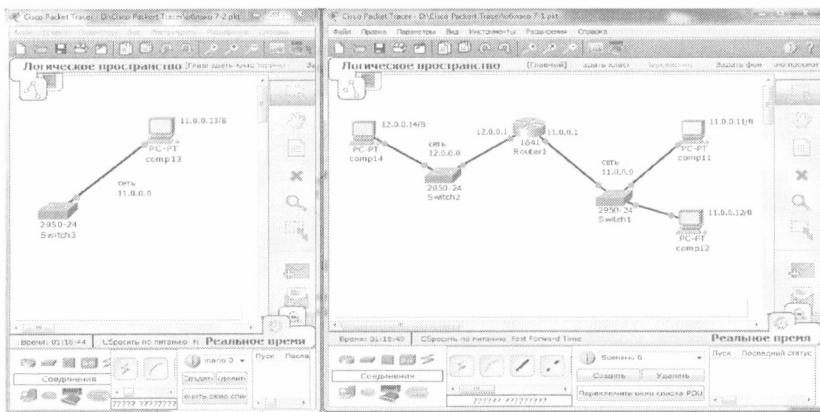
Жұмыс істеп тұрған бағдарламаның ағымдағы сессиясын өшірмей, Cisco Packet Tracer қайта іске қосып, бағдарлама жұмысының екінші сессиясын құрыңыз және 9.2 суреттегі схема бойынша желіні құрыңыз:



Сурет 9.2-Екінші сессия-11.0.0.0 желісі

Құрылғы атаулары мен схемада көрсетілгендей comp 13 компьютеріне арналған TCP/IP протоколдарының параметрлерін орнатыңыз (сурет 9.2).

Нәтижесінде Сіз Cisco Packet Tracer бағдарламасының әртүрлі сессияларында жұмыс істейтін желілерді аласыз (сурет 9.3.):



Сурет 9.3-Бастапқы параметрлер

### Бірнеше қосылысты құру.

Бірнеше пайдаланушы байланысын құру үшін Cisco Packet Tracer бағдарламасының әр түрлі сессияларында құрылған желілерді жалғау қажет. Ол үшін ортақ желі (11.0.0.0 желісі) таңдап алынады, ол арқылы байланыс порттары көрсетіледі: бір желі үшін-кіріс порты, ал екіншісі үшін-шығыс порты.

Өртүрлі сессияларда желілерді біріктіру Switch 1 (бірінші сессия) және Switch 3 (екінші сессия) коммутаторлары арқылы жүргіземіз.

Бірнеше қосылыс жасау үшін келесі баптау кезеңдерін жүргізу қажет:

1 кезең - бірнеше бұлтқа қосылу.

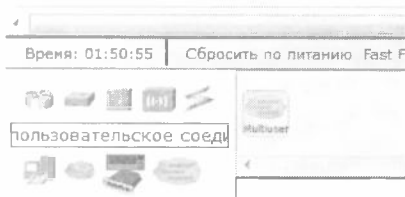
2 кезең - қосылу жүргізілетін құрылғыларда порттарды ашу (Switch 1 және Switch 3).

3 кезең - жалпы бірнеше байланыс арнасын құру.

1 кезең –бірнеше пайдаланушы бұлтқа қосылу.

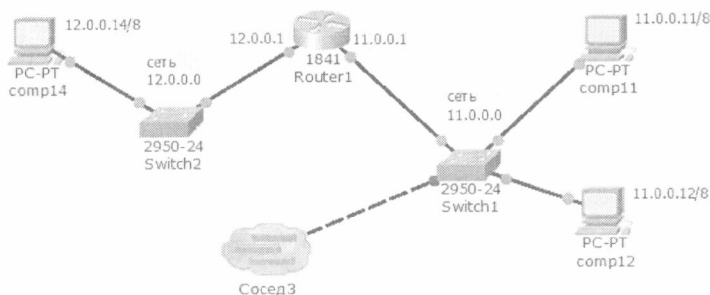
Бірінші сессияны ашыңыз.

Бірнеше қосылым жасаңыз. Ол үшін аспаптарда "пайдаланушы қосылымы" тобын таңдап, желі схемасына "Multiuser" құрылғысын енгізіңіз (сурет 9.4):



Сурет 9.4-Бірнеше қосылым жасау

Switch 1 коммутаторын жаңа құрылғымен жалғаңыз (сурет 9.5). Ол үшін "Қосылымдар" тобында "мыс кроссовери" кабелінің түрін таңдап, Fast Ethernet 0/4 коммутаторының төртінші портын бірнеше қосылыммен жалғаңыз. Жаңа арнаны жасау функциясын іске қосыңыз.

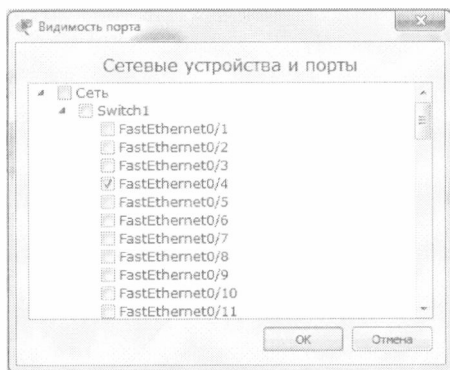


Сурет 9.5-Коммутаторды бірнеше арнаға қосу

2 кезең-байланыс жүргізілетін құрылғыларда порттарды ашу.

Енді әртүрлі сессияларда желілерді біріктіру үшін коммутаторларда порттарды ашу қажет. Switch 1 және Switch 3 төртінші порт болсын.

Ол үшін әрбір сессияда басты мәзірде "кеңейтімдер" – "қоп пайдаланушы режим" - "порттың көрінуі" таңдаңыз (сурет 9.6).



Сурет 9.6-Коммутатордың төртінші портын қосу

3-кезең-жалпы бірнеше қосылым қатынасу арнасын құру.

Жалпы қатынасу арнасын құру үшін нақты жұмыс істейтін желіні таңдау қажет. Екі нұсқа болуы мүмкін:

1-нұсқа-сіз әртүрлі компьютерлерде қоп пайдаланушымен байланыс жасайсыз;

2-нұсқа-әр компьютер сеанстарында бір компьютерде қоп пайдаланушымен байланыс жасайсыз

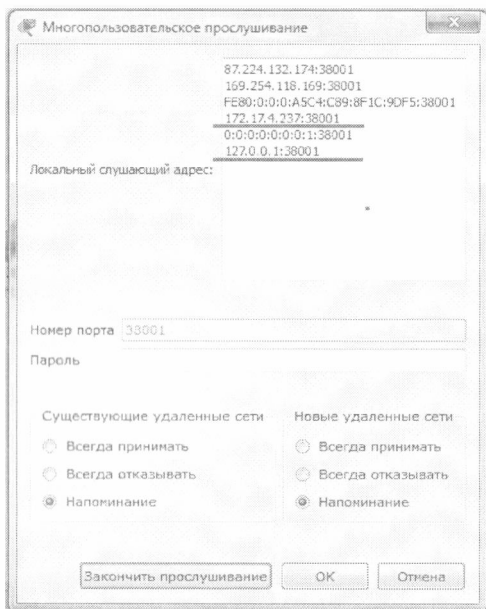
Бірінші жағдайда қосылу жергілікті желіде компьютердің нақты IP мекен-жайы арқылы жүргізіледі.

Екінші жағдайда қосудың екі нұсқасы болуы мүмкін:

- localhost мекен-жайы арқылы 127.0.0.1;
- жергілікті желіде компьютердің нақты IP мекен-жайы арқылы.

Екінші сессияға ауысыңыз.

Ол үшін басты мәзірде "кеңейтімдер" – "коп мақсатты режим" - "тыңдау" тандаңыз (сурет 9.7). Күпия сөзі алып тастаңыз және "бар қашықтағы желілер" және "жана қашықтағы желілер" бөлімдерінде ескерту режимін қосыңыз.



Сурет 9.7-Орғақ пайдалану арнасын орнату

Жоғарғы жағында тыңдалатын желілер көрсетіледі. Біздің жағдайда бұл 172.17.0 және localhost желісі.

172.17.0 желісі-біздің компьютер қосылған жергілікті желі.

Кіру нүктесі IP мекенжайы мен портпен белгіленеді: IP мекенжайы - 172.17.4.237, кіріс порты - 38001.

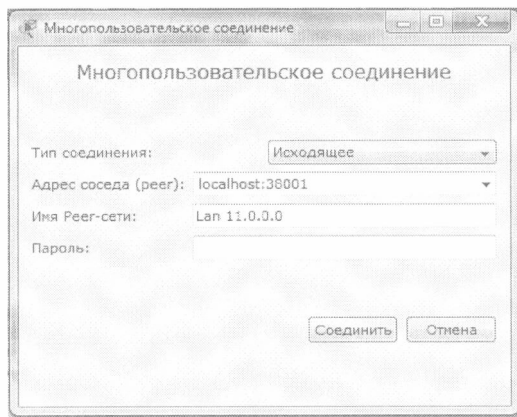
localhost - желі 127.0.0.0, IP мекен-жайы 127.0.0.1, 38001 порт.

Жергілікті хост арқылы байланыс жасайық.

Бірінші сессияға ауысу.

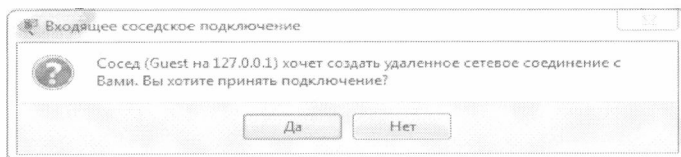
"Көрші 3" құрылғысының параметрлеріне кіріңіз.

"Шығыс" қосылымының түрін таңдап, "Lan 11.0.0" топологиясындағы жалпы желі желісінің атауын орнатыңыз, 2 - localhost:38001 желіге кіру нүктесін орнатыңыз және "Қосу" түймесін басыңыз (сурет 9.8):



Сурет 9.8-Кіру нүктесін таңдау

Нәтижесінде екінші сессияда қосылу туралы хабарлама пайда болады (сурет 9.9):

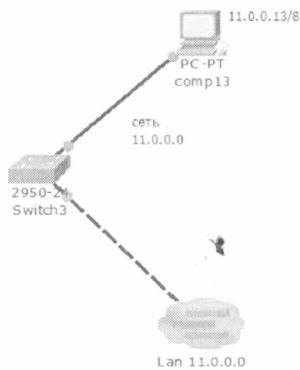


Сурет 9.9-Байланыс құру

Нәтижесінде екінші сессияда бірнеше қосылыстың бұлтты пайда болады.

Құрылған бұлтты Switch 3 коммутаторымен қосыңыз.

Ол үшін "Қосылымдар" тобында "мыс кроссовері" кабелінің түрін таңдап, Switch 3-ке Fast Ethernet 0/4 төртінші портын арнап арқылы бірнеше қосылыс бұлттымен жалғаңыз (сурет 9.10):



Сурет 9.10-Екінші сессияны жалпы арнаға қосу

Барлық желілердегі барлық компьютерлердің өзара байланысын **ping** командасын тексеріңіз.

#### № 4 өзіндік жұмыс.

Бір компьютерде екі түрлі сессиялардың бірнеше байланысын жасаңыз.

Статикалық маршруттауды пайдалана отырып, әрбір сессияда екі желі жасаңыз.

Әрбір желінің құрамы: клиенттік компьютер және сайты бар сервер.

Тапсырма: барлық компьютерлер екі сессияда да барлық сайттарды ашу керек.

#### Бақылау сұрақтары:

1. Бірнеше жұмыс режимінің негізгі мүмкіндіктерін атаңыз.
2. Бірнеше жұмыс режимінде байланыс сеансы қалай ұйымдастырылады?
3. Бірнеше жұмыс режиміндегі қосылыстардың түрлерін атаңыз?
4. Бірнеше жұмыс режимінде қандай желілік құрылғылар мен порттар арқылы байланыс ұйымдастырылады?
5. Жалпы қатынау арнасы үшін қандай желілер таңдалады?
6. Бірнеше қосылысты құру кезеңдерін сипаттаңыз.
7. Бірнеше жұмыс режимін ұйымдастыру кезінде байланыс сеансын ұйымдастыру үшін порттар қалай анықталады?

## 10 БӨЛІМ. ACL (ACCESS CONTROL LIST) ҚАТЫНАУДЫ БАСҚАРУ ТІЗІМІ.

Кіру тізімдері сізге жергілікті және корпоративтік желілерде жұмыс істейтін трафикті басқару ережелерін жасауға мүмкіндік береді.

Қол жеткізу тізімдерінің он алты түрі бар, бірақ ең жиі екі түрі қолданылады: standart – стандартты (1-ден 99-ға дейінгі нөмірлер) және extended-кеңейтілген (100-ден 199-ға дейінгі немесе 2000-нан 2699-ға дейінгі нөмірлер). Бұл екі тізімнің арасындағы айырмашылықтар пакеттерді тек IP мекенжайы бойынша ғана емес, басқа да түрлі параметрлер бойынша сүзу мүмкіндіктеріне жатады.

Стандартты тізімдер тек кіріс IP дерек көздерінің мекен-жайларын өңдейді, яғни жіберушінің IP мекен-жайы бойынша ғана сәйкестікті іздейді. Кеңейтілген тізімдер корпоративтік желінің барлық мекенжайларымен жұмыс істейді және порттар мен протоколдар бойынша трафикті қосымша сүзе алады.

Қатынау тізімінің жұмысы әрбір жолда трафикті өңдеу ережесі жазылған осы тізімдегі жолдардың жүру тәртібіне тікелей байланысты. Тізімнің барлық ережелері алғашқыдан соңғысына дейін ретпен қаралады, бірақ бірінші сәйкестік табылған соң, яғни келген бума үшін оған сәйкес келетін ереже табылды. Бұдан кейін тізімнің қалған ережелері ескерілмейді. Егер пакет ережелердің ешқайсысына түспесе, әдепкі ереже қосылады:

### **access-list номер\_списка deny any**

бұл тізім қолданылған желілік құрылғының интерфейсі бойынша бүкіл трафикке тыйым салынады.

Кіру тізімін пайдалануды бастау үшін келесі үш кезеңді орындау қажет:

- 1-тізім жасау;
- 2-тізімді трафикті өңдеу ережелерімен толтыру;
- 3-құрылғының интерфейсіне кіру немесе шығу тізімін қолдану.

Бірінші кезең-кіру тізімін жасау:

Стандартты тізім:

Switch 3(config)#ip access-list standart 10

(10 нөмірімен стандартты кіру тізімі жасалады, бұл жағдайда коммутаторда жасалады)

Кеңейтілген тізім:

Router 1(config)#ip access-list extended 100



(100 нөмірімен кеңейтілген кіру тізімі жасалады, бұл жағдайда маршрутизаторда жасалады).

Екінші кезең-ережелерді кіру тізіміне енгізу:

Кіру тізіміндегі әр ережеде үш маңызды элемент болады:

1-маршрутизатор немесе үшінші деңгейдегі коммутатор конфигурациясының басқа бөліктерінде оған жүгінген кезде тізімді сәйкестендіретін сая;

2-deny (тыйым салу) немесе permit (рұқсат ету);

3-үш нұсқаның біреуі бойынша берілетін пакеттің идентификаторы:

- желі мекенжайы (мысалы 192.168.2.0 0.0.0.255) – желі маскасының орнына желі маскасының үлгісі көрсетіледі;

- хост мекенжайы (host 192.168.2.1);

- кез келген IP мекенжайы (any).

№10 стандартты кіру тізімінің үлгісі:

**access-list 10 deny host 11.0.0.5**

**access-list 10 deny 12.0.0.0 0.255.255.255**

**access-list 10 permit any**

Бұл тізімде:

- 11.0.0.5 IP мекенжайы бар хостқа барлық трафик тыйым салынады;

- 12.0.0/8 желісіндегі барлық трафикке тыйым салынады (Ережеде ішкі желінің нақты маскасы емес, оның үлгісі көрсетіледі);

- қалған трафик рұқсат етілген.

Бұл кеңейтілген тізімінде қол жеткізу артынан көрсетілген әрекеттер кілттерімен permit немесе deny болуы тиіс параметр белгіленген хаттаманың (мүмкін хаттамалар IP, TCP, UDP, ICMP), ол көрсетеді, қалай орындалуы тексеру барлық IP пакеттерінің немесе тек пакеттерді-баптардың тақырыптарымен толықтырылсын ICMP, TCP немесе UDP. Егер тексеруге TCP немесе UDP порттарының нөмірлері жатса, онда TCP немесе UDP ХАТТАМАСЫ көрсетілуі тиіс (FTP және WEB қызметтері TCP хаттамасын пайдаланады).

Кеңейтілген тізімдерді жасау кезінде қатынау ережелерінде хаттамалар мен порттар бойынша трафикті сүзгілеуді қосуға болады. Порттарды көрсету үшін қол жеткізу ережесінде мынадай белгілер көрсетіледі (10.1 кесте):

Кесте 10.1-Порттардағы белгілер

Белгі	Іс-әрекет
lt n	Порттардың барлық нөмірлері, n-нан

	аз
gt n	Порттардың барлық нөмірлері, n-нан көп
eq n	n порты
neq n	n қоспағанда, барлық порттар
range n m	n -ден m-ге дейінгі барлық порттар

Кең таралған қосымшалар және оларға сәйкес келетін порттардың стандартты нөмірлері 10.2 кестеде келтірілген:

Кесте 10.2-Порттардың стандарттары

Порт нөмірі	Протокол	Қосымша	Access list командасындағы кілтті сөз
20	TCP	FTP	data ftp_data
21	TCP	FTP серверін басқару	ftp
22	TCP	SSH	
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtп
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp

№111 кеңейтілген кіру тізімінің үлгісі:

```
! 80 портындағы трафикке тыйым салу (www-трафик)
ip access-list 111 deny tcp any any eq 80
ip access-list 111 deny ip host 10.0.0.15 host 12.0.0.5
ip access-list 111 permit ip any any
```

```
interface ethernet0
! Шығыс трафигіне 111 кіру тізімін қолдану
ip access-group 111 out
```

Бұл тізімде сыртқы тораптар ішкі желі сайттарына жүгіне алмайды, себебі кіру тізімі интерфейстің шығуына (сыртқы тораптар үшін), сондай-ақ 10.0.15 торабына 12.0.0.5 торабына кіруге тыйым салынған

Қалған трафик рұқсат етілген.

Үшінші кезек-кіру тізімін қолдану.

Қол жеткізу тізімдері құрылғылардың екі түрі үшін пайдаланылуы мүмкін:

1-маршрутизаторда;

2-үшінші деңгейлі коммутаторға.

Әрбір интерфейсте екі қатынау тізімі қосылуы мүмкін: кіріс пакеттері үшін бір ғана кіру тізімі және шығыс пакеттері үшін бір ғана тізім.

Әрбір тізім қолданылған интерфейспен ғана жұмыс істейді және егер ол қолданылмаса, құрылғының басқа интерфейстеріне әрекет етпейді.

Бірақ бір рұқсат тізімі әртүрлі интерфейстерге қолданылуы мүмкін.

Құрылғыға кіру тізімін қолдану келесі пәрмендермен жүзеге асырылады:

```
interface Ethernet 0/0/0
```

```
ip access-group 1 in
```

```
ip access-group 2 out
```

Бұл жағдайда Ethernet 0/0/0 интерфейсіне екі қатынау тізімі қолданылған:

№1 кіру тізімі-интерфейстің кіруіне (яғни ішкі мекен-жайлар үшін);

№2 қатынау тізімі-интерфейстің шығысы (сыртқы желіге қолдану).

Барлық жасалған кіру тізімдерін қору және оларды құрылғы интерфейстеріне қолдану үшін келесі пәрмендерді пайдаланыңыз:

Кіру тізімдерін қарау командасы:

```
Router# Sh access-list
```

Құрылғының ағымдағы конфигурациясын қарау және тізімдерді интерфейстерге байланыстыру:

```
Router# Show running-config
```

Сақталған конфигурацияны қарау:

```
Router# Show configuration
```

Ағымдағы конфигурацияны сақтау:

```
Router# write memory
```

Немесе

```
Router# copy run start
```

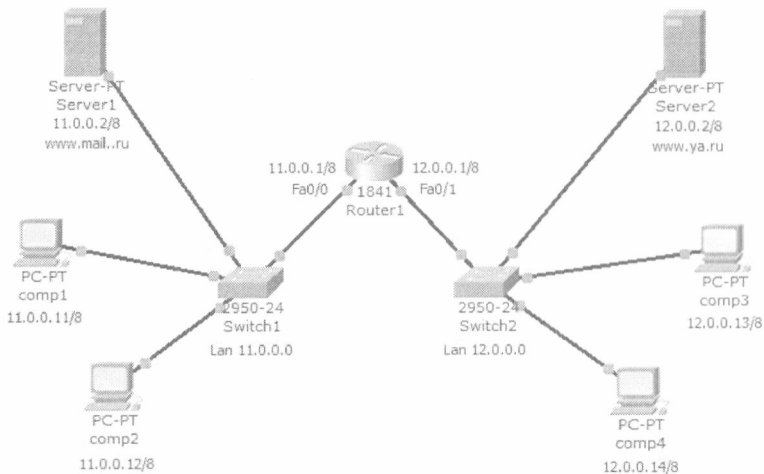
Кіру тізімін жою командасы:

**interface ethernet0/0/0** - қажетті интерфейсті таңдау

**no access-list номер\_списка** -таңдалған интерфейсте тізімді жою

### Зертханалық жұмыс № 14. Кіру тізімі.

10.1 суретте көрсетілгендей желі схемасын жасаңыз.



Сурет 10.1-Корпоративтік желі схемасы

Тапсырма:

1-компьютер comp 1 және comp 2 барлық сайттарды ашуы керек, бірақ оларға comp 3 және comp 4 компьютерлеріне кіруге тыйым салынады.

2-сomp 3 және comp 4 компьютерлері бір-біріне қол жетімді және тек өз желісінің сайтын ашу керек, олар үшін 11.0.0.0 желісі қолжетімсіз.

Стандартты кіру тізімін құрайық, онда comp 3 және comp 4 хостарына құлыптау ережелерін көрсетеміз және осы тізімді Fa 0/0 интерфейс шығысына қолданамыз.

Артықшылықты режимді қосып, роутер конфигурациясына кіріңіз:

```
Router 1>en
```

```
Router 1#conf t
```

Стандартты кіру тізімін жасап, кіру ережесін енгіземіз:

```
Router 1(config)#ip access-list standard 10
Router 1(config-std-nacl)#deny host 12.0.0.13
Router 1(config-std-nacl)#deny host 12.0.0.14
Router 1(config-std-nacl)#permit any
```

Мұнда біз 12.0.13 және 12.0.0.14 мекенжайларынан басқа барлық трафикті рұқсат еттік.

Роутер баптауларында жасалған кіру тізімін көрейік. Ол үшін роутер конфигурациясы режимінен шығып, **sh access-list** құрылғысындағы тізімдерді қарау командасын енгізу керек:

```
Router 1#sh access-list
Standard IP access list 10
  deny host 12.0.0.13
  deny host 12.0.0.14
  permit any
Router 1#
```

Fa0/0 интерфейсінің шығуы үшін жасалған тізім қолданылады:

```
Router 1#
Router 1#conf t
Router 1(config)#interface fa0/0
Router 1(config-if)#ip access-group 10 out
```

Нәтижесінде қол жеткізу тізімі 11.0.0.0 желі интерфейсінің шығысына қолданылған, біз келесі қол жеткізу саясатын алдық:

1-11.0.0.0 желісінен маршрутизаторға кіретін пакеттер екі сыртқы мекен-жайға - 12.0.0.13 және 12.0.0.14 бойынша құлыпты алады;

2 -маршрутизатордан 11.0.0.0 желісіне кіретін барлық сыртқы пакеттерге екі мекен-жайдан басқа бәріне рұқсат етілген - 12.0.0.13 және 12.0.0.14 (бұл мекен-жайларға 11.0.0.0 желісіне кіруге болмайды).

Маршрутизатор конфигурациясындағы Fa 0/0 интерфейсіне кіру тізімінің байланысуын қарастырайық:

```
Router 1(config-if)#exit
Router 1(config)#exit
Router 1#
Router 1#sh running-config
```

Осы команданы пайдалана отырып, сіз роутердің толық конфигурациясын, соның ішінде нақты интерфейске кіру тізімін байланыстыруды көресіз (бұл жағдайда интрфейстің шығуына):

```
interface FastEthernet0/0
ip address 11.0.0.1 255.0.0.0
ip access-group 10 out
duplex auto
speed auto
!
```

Желі ресурстарына қол жеткізу саясатын тексеріңіз. Келесі срежелер орындалуы тиіс:

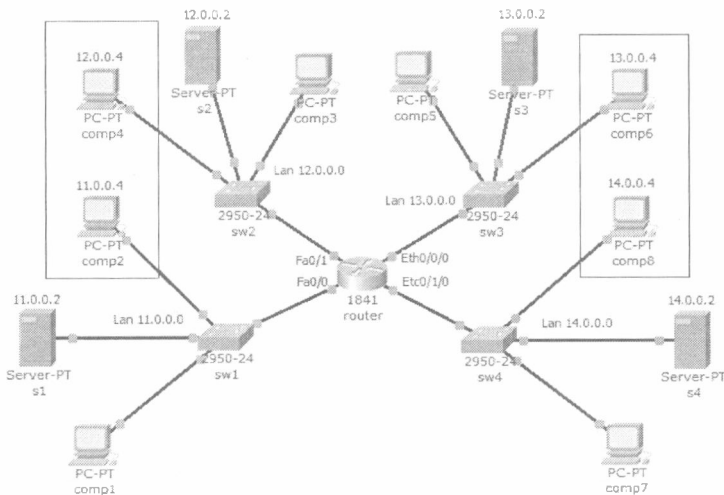
1-comp 3 және comp 4 компьютерлері бір-біріне қол жетімді және тек өз желісінің сайты ашуы керек, 11.0.0.0 желісіне кіруге тыйым салынады;

2-Server 2 сервері барлық желілік ресурстарға қол жетімді;

3-12.0.0.13 және 12.0.0.14 мекенжайларын қоспағанда, барлық ресурстарға comp1 және comp2 компьютерлері қол жетімді.

## №5 өзіндік жұмыс

10.2 суретте ұсынылған желіні жасаңыз.



Сурет 10.2-Корпоративтік желі схемасы

Корпоративтік желі төрт желіден тұрады:

желі 1 – 11.0.0.0/8;

желі 2 – 12.0.0.0/8;

желі 3 – 13.0.0.0/8;

желі 4 – 14.0.0.0/8.

Әрбір желіде серверде Web сайт орнатылған.

Тапсырма:

Компьютеру comp 2 доступны только компьютеры своей сети и comp 4.

Компьютеру comp 4 доступны только компьютеры своей сети и comp 2.

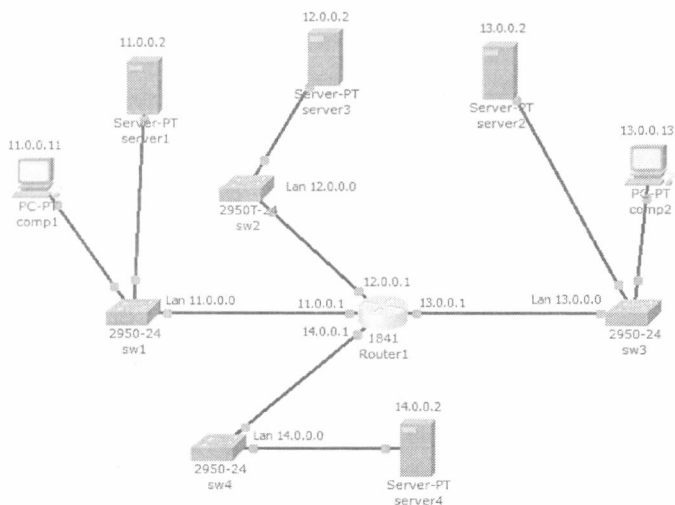
Компьютеру comp 8 доступны только компьютеры своей сети и comp 6.

Компьютеру comp 6 доступны только компьютеры своей сети и comp 8.

Comp 1, comp 3, comp 5 және comp 7 компьютерлері S1, S2, S3 және S4 серверлеріндегі барлық сайттарды ашуы керек.

### № 6 өзіндік жұмыс.

10.3 суретінде ұсынылған желіні жасаңыз.



Сурет 10.3-Корпоративтік желі схемасы

Корпоративтік желі төрт желіден тұрады:

желі 1 – 11.0.0.0/8;

желі 2 – 12.0.0.0/8;

желі 3 – 13.0.0.0/8;

желі 4 – 14.0.0.8.

Веб-сайт әр серверлік желіде орнатылған.

Тапсырма:

1-14.0.0.0 желісі 11.0.0.0 желісінен қол жетімді емес.

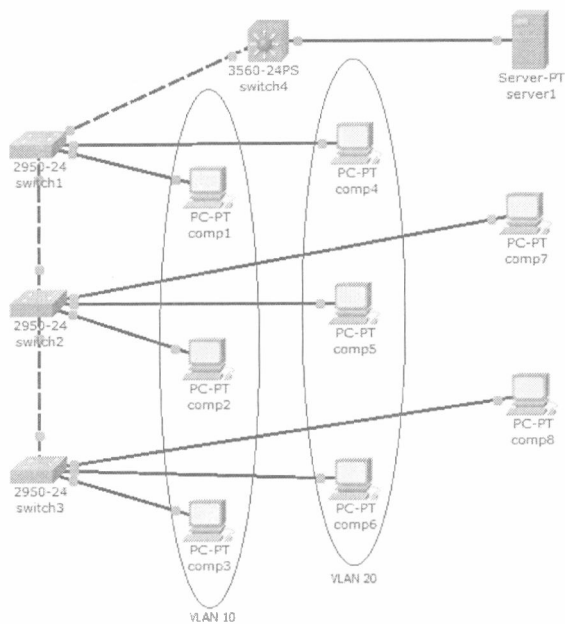
2-comp 1 және comp 2 компьютерлері server 3 тарабын ашуға рұқсат береді, бірақ ring командасы бойынша server 3 тыңдауға тыйым салады.

3-comp 1 компьютері серверге кіруге рұқсат береді, бірақ осы серверде сайтты ашуға тыйым салады.

4-comp 2 компьютері server 1 қатынауға рұқсат береді, бірақ server 1 тарабын ашуға тыйым салады, server 4 тарабын ашуға және кіруге рұқсат береді.

### №7 өзіндік жұмыс.

10.4 суреттегі желі схемасын жасаңыз. Желілер мен адресацияны еркін орнатыңыз.



Сурет 10.4-Корпоративтік желі схемасы



Тапсырма:

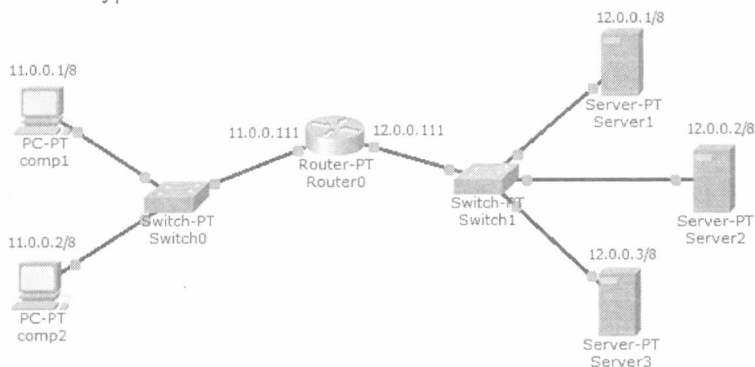
1-сomp 1, comp 2 және comp 3 компьютерлері бір VLAN 10 ішінде, тек бір-біріне қол жетімді және сервер 1 қатынасына ие.

2-сomp 4, com 5 және com 6 компьютерлері бір VLAN 20-да орналасқан, тек бір-біріне қол жетімді және сервер 1 қол жетімді.

3-сomp 7 және com 8 компьютерлері бір-біріне ғана қол жетімді және сервер1 қол жетімді.

### № 8 өзіндік жұмыс.

10.5 суреттегі желі схемасын жасаңыз.



Сурет 10.5-Корпоративтік желі схемасы

Барлық үш серверде Web және FTP қызметтері орнатылған.

Comp 1 және comp 2 компьютерлеріне арналған кіру тізімін жасаңыз:

Компьютер comp 1:

Server 1 – FTP рұқсат ету;

Server 2-Web қатынауға рұқсат беру;

Server 3-Web және FTP қатынауға рұқсат ету.

Компьютер comp 2:

Server 1-Web қатынауға рұқсат беру;

Server 2 - FTP рұқсат ету;

Server 3-Web және FTP қатынауға рұқсат ету.

### **Бақылау сұрақтары:**

1. Кеңейтілген кіру тізімдерін қандай параметрлер бақылайды?
2. Барлық веб-серверге хосттан пакеттерді жіберуге рұқсат беретін пәрменнің мысалын келтіріңіз.
3. Қатынау тізімдерінің негізгі түрлерін атаңыз.
4. Желі маскасының үлгісі дегеніміз не және оны Кіру тізімінде пайдалану мысалдарын келтіріңіз.
5. Желілік трафикті оңдеу ережесі келесі кіру тізімін анықтайды: `Ip access-list 111 deny tcp any any eq 80`
6. Жергілікті желі fa0/0 интерфейсі бойынша роутермен қосылған, ал сыртқы желі Fa0/1 интерфейсі бойынша қосылған. Жергілікті желіден сыртқы желіге кіруге тыйым салынады, ал сыртқы желіден ішкі желіде орналасқан FTP серверіне кіруге тыйым салынады. Бұл ережелерді жүзеге асыру үшін кіру тізімі жасалды. Интерфейсті атаңыз және жасалған кіру тізімін қолданатын қандай бағытта (кіру немесе шығу).
7. Қай нұсқа емес жүргізілуі мүмкін салыстыру негізінде кеңейтілген тізімін кіру IP?
  - хаттама;
  - Жіберушінің IP мекенжайы;
  - Алушының IP мекенжайы;
  - FTP хаттамасы бойынша жіберу үшін Файл атауы.
8. 10.16.0.0 желісінің беттердесі қандай үлгіге сәйкес келетінін атаңыз./12?
9. Кіру тізімінде келесі ереже бар:  
`Permit any host 192/168/1/1/it 25`  
Порттардың нөмірлері қандай?
10. 51.52.32.0 / 21 желіге кіру үшін кіру ережесін жазыңыз

## Қорытынды

Оқу құралда Cisco Packet Tracer интерфейсі, Cisco Packet Tracer байланыс жабдықтары мен желілері, Cisco Packet Tracer-де симуляция режимі тақырыптары қарастырылған.

«Компьютерлік желілер» курсы барлық оқу түрінің студенттері ақпараттық технологиялар саласындағы болашақ мамандардың ЭЕМ жүйелері мен желілерін, телекоммуникация жүйелері мен тиісті ақпараттық технологияларды, аппараттық құралдар мен бағдарламалық қамтамасыз етуді бақылау және пайдалану әдістерін, сондай-ақ оларды жаңа нарықтық жағдайда өзінің кәсіби қызметінде қолдану үшін қажетті білім алу дағдыларын қалыптастыруға ықпал етеді.

Сонымен қатар, оқу құралы:

- \* компьютерлік желілерді ұйымдастыру және конфигурациялау, компьютерлік желілер модельдерін құру және талдау, компьютерлік желілердің бағдарламалық және аппараттық компоненттерін тиімді пайдалану дағдыларын меңгеруге ықпал етеді;

- \* студенттердің дәрістерде және өзін-өзі дайындау барысында алған білімдерін тереңдетуге және бекітуге ықпал етеді;

- \* студенттердің оқу және нормативтік әдебиеттерді шығармашылық, өзіндік талдау қабілетін дамытады;

- \* меңгерілген материалды жүйелеу және жалпылау, оны сын тұрғысынан бағалау іскерлігін пысықтайды.

## Қолданылған әдебиеттер тізімі:

### Негізгі әдебиет:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание: учебник/СПб.: Питер, 2019 - 992 с.
2. Нане Б. Компьютерные сети: учебник/Пер.с англ. – М.: Бином, 2011 – 394 с.
3. Таненбаум Э., Уэзоролл Д. Компьютерные сети. 5-е издание: учебник/СПб.: Питер, 2016 – 960 с.
4. Куроуз Д., Росс К. Компьютерные сети. Нисходящий подход. 6-е издание: учебник/Москва: Издательство «Эксмо», 2016-912 с.
5. Сергеев А. Основы локальных компьютерных сетей. Учебное пособие. Издательство «Лань», 2016 – 184 с.
6. Куроуз Д., Росс К. Компьютерные сети. Настольная книга системного администратора: учебник/ Москва: Издательство «Эксмо», 2016-912 с.
7. Робачевский А. Интернет изнутри. Экосистема глобальной сети: учебник/Издательство «Альпина Паблишер», 2017 – 224 с.
8. Грингард С. Интернет вещей. Будущее уже здесь: учебник/Издательство «Альпина Паблишер», 2019 – 188 с.
9. Одом У. Официальное руководство Cisco по подготовке к сертифицированным экзаменам CCNA ICND 2 200-101. Маршрутизация и коммутация: Учебное пособие/ Москва: Издательский дом «Вильямс» 2015 – 736 с.
10. TCP/IP. Сетевое администрирование. 3-е издание: учебник/ Москва: Издательство «Эксмо», 2014-813 с.
11. Бен Пайпер: Администрирование сетей Cisco: освоение за месяц. Издательство «ДМК-Пресс», 2018 - 316 с.

### Қосымша әдебиет:

1. Одом У. Официальное руководство Cisco по подготовке к сертифицированным экзаменам CCNA ICND 2 200-101. Маршрутизация и коммутация: Учебное пособие/ Москва: Издательский дом «Вильямс» 2016 – 736 с.
2. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822. Учебное пособие/ Москва: Издательский дом «Вильямс» 2019 – 706 с.
3. Эделман Джейсон, Скотт С.Лоу, Мэтт О. «Автоматизация программируемых сетей». Издательский дом «ДМК Пресс» 2019 - 616 с.
4. Букатов А. А., Гуда С. А. Компьютерные сети. Расширенный начальный курс». Учебник для вузов. СПб.: Питер, 2019 – 496 с.
5. Ватаманок А. И. Создание, обслуживание и администрирование сетей на 100%. СПб.: Питер, 2010 – 350 с.

6. Стахнов А. А. Сетевое администрирование Linux. учебник/ СПб.: БХВ-Петербург, 2016 – 473 с.

7. Лимончелли, Хоган, Чейлап: Практика системного и сетевого администрирования. Том I. / Москва: Издательский дом «Вильямс» 2018 – 1108 с.

8. Н. Васин: Технологии пакетной коммутации. Издательство «Лань», 2019 – 884 с.

Кенебаева Динара Байтасовна  
Бекенова Дариға Бекеновна

**Компьютерлік желілер.  
Оқу құралы**

Басуға 20.02.2021 жылы қол қойылды. Қағазы көшірмелік.  
Қаріп түрі «Таймс» Пішімі 60x84/16. Баспа табағы 6,5 бет.  
Таралымы 500 дана. Тапсырыс №79  
«Тұран-Астана» университетінің баспаханасында басылған.  
Мекенжай: 010000, Нұр-Сұлтан қ., Ы. Дүкенұлы көшесі 29 үй.  
[www.turan-astana.kz](http://www.turan-astana.kz)