Міністерство освіти і науки України
Сумський державний університет
Факультет електроніки та інформаційних технологій

6039 Методичні вказівки
до лабораторних робіт
на тему **«Списки контролю доступу та динамічна маршрутизація»**
з дисципліни **«Мережі операторів та системи мобільного зв'язку»**
для здобувачів спеціальності 122 *«Комп'ютерні науки»*
освітнього ступеня «бакалавр»
усіх форм здобуття вищої освіти

Суми
Сумський державний університет
2024

Методичні вказівки до лабораторних робіт на тему «Списки контролю доступу та динамічна маршрутизація» з дисципліни «Мережі операторів та системи мобільного зв’язку» / укладач: Д. В. Великодний. – Суми : Сумський державний університет, 2024. – 30 с.

Кафедра комп’ютерних наук факультету ЕлІТ

ЗМІСТ

С.

ВСТУП

Розглянуті в методичних вказівках протоколи та технології надають здобувачам розуміння принципів функціонування та логіки налаштування на мережевому обладнанні Cisco найбільш популярних і практично затребуваних сервісів. Виконуючи лабораторні роботи в мережевому симуляторі Cisco Packet Tracer, студенти мають можливість на практиці закріпити теоретичний матеріал лекцій і набути практичних навичок у налаштуванні комп'ютерних мереж. Інструкції до лабораторних робіт описують покроковий шаблонний алгоритм налаштування мережевого обладнання, водночас комплексна лабораторна робота за варіантами дає можливість перевірити рівень засвоєння здобувачами вивченого матеріалу та оцінити творчий підхід до вирішення поставлених завдань.

І хоча ці методичні вказівки написані з орієнтацією на виконання лабораторних робіт у симуляторі Cisco Packet Tracer, більшість лабораторних робіт можна з легкістю повторити на реальному мережевому обладнанні, тим самим отримавши безцінний досвід роботи з «живим» залізом.

1 СПИСКИ КОНТРОЛЮ ДОСТУПУ

До початку виконання завдань відкрити файл із заздалегідь налаштованою мережею (Шаблон 1) – ця мережа буде використовуватися як тренажер для відпрацювання подальших сценаріїв налаштування списків контролю доступу Access Control List (ACL).

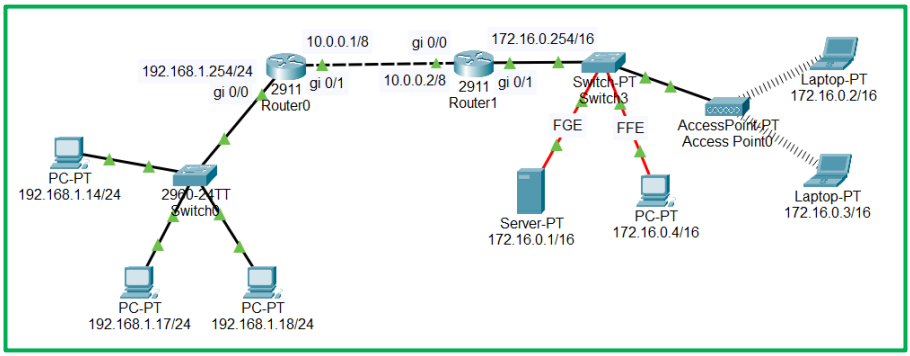


Рисунок 1.1 – Налаштована мережа (Шаблон 1)

Завдання 1.1

Налаштування стандартного ACL

Формат конфігурації стандартного ACL:

"access-list <номер (1-99)> <дія (deny|permit)> <адреса джерела>"

Приклад налаштування стандартного списку доступу (Standart Access List) на Router 1 (правий роутер) на вхідному інтерфейсі gi 0/0 для обмеження доступу від PC із IP-адресою 192.168.1.14 до правої мережі.

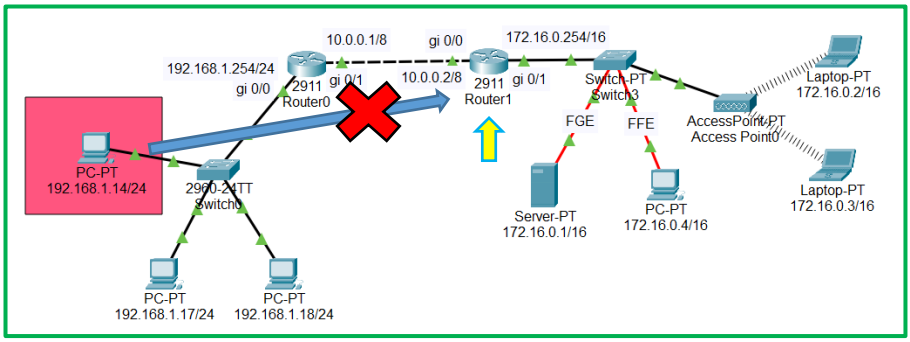


Рисунок 1.2 – Налаштування стандартного списку доступу

Команди конфігурації стандартного ACL:

1) Router(config)#access-list 10 deny 192.168.1.14
2) Router(config)#access-list 10 permit any
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 10 in

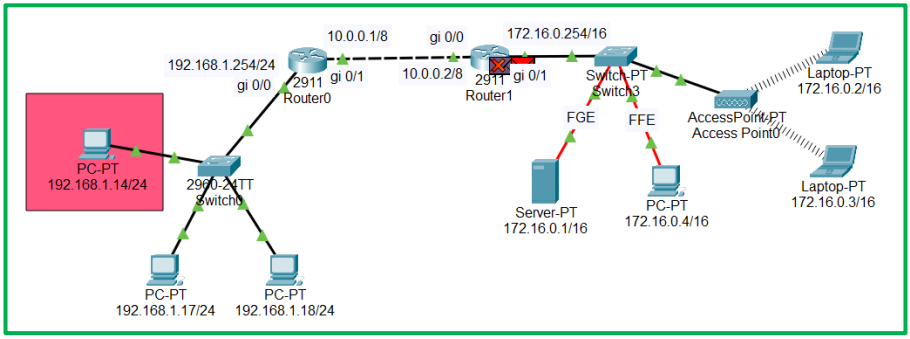


Рисунок 1.3 – Перевірка роботи стандартного списку доступу у режимі симуляції

Налаштування розширених ACL

Розширені списки контролю доступу дозволяють більш тонко налаштовувати доступ між мережами та окремими вузлами, а також дозволяють блокувати такі типи протоколів, як: IP, TCP, UDP, ICMP, GRE, або IGRP.

Формат конфігурації розширеного ACL:

"access-list <номер (100-199)> <дія (permit|deny)> <протокол> <адреса джерела> <адреса одержувача> <порт>"

Завдання 1.2.

Block host to host

Якщо у вас раніше були створені інші списки доступу - видаліть їх / або відкрийте чистий Шаблон 1.

Легенда до завдання. У вашій компанії з'явився новий співробітник, адреса його комп'ютера 192.168.1.14. Критично важлива інформація знаходиться на сервері 172.16.0.1. Завдання: блокувати доступ нового співробітника до сервера, але при цьому дозволити йому доступ до всіх інших комп'ютерів мережі.

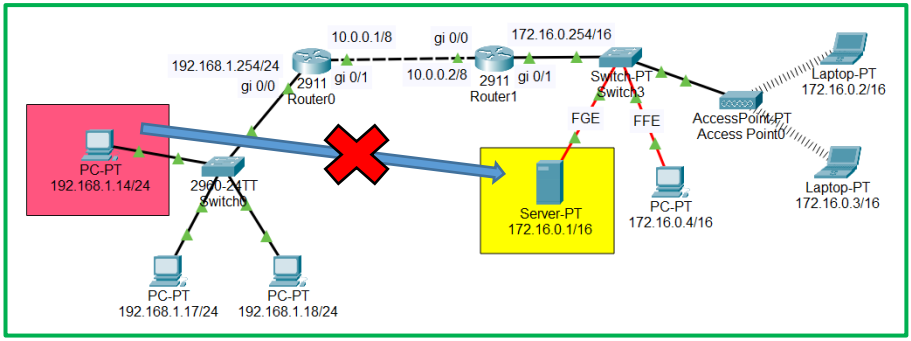


Рисунок 1.4 – Block host to host

Приклад налаштування розширеного списку доступу (extended access list) на Router 1 на інтерфейсі gi 0/0

1) Router(config)#access-list 101 deny ip host 192.168.1.14 172.16.0.1 0.0.0.0 – *блокування IP із хоста 192.168.1.14 до хоста 172.16.0.1*
2) Router(config)#access-list 101 permit ip any any – *доступ до інших хостів дозволено*
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 101 in

Завдання 1.3.

Block host to network

Необхідно блокувати доступ вузла 192.168.1.14 до мережі 172.16.0.0.

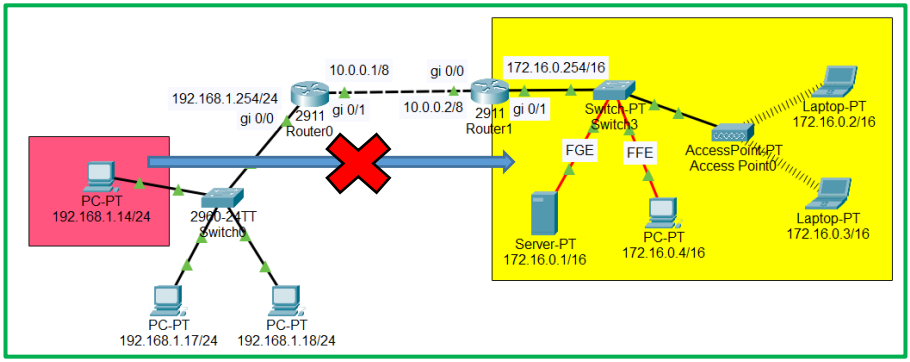


Рисунок 1.5 – Block host to network

Приклад налаштування розширеного списку доступу (extended access list) на Router 1 на інтерфейсі gi 0/0

1) Router(config)#access-list 102 deny ip host 192.168.1.14 172.16.0.0 0.0.255.255 – *блокування IP із хоста 192.168.1.14 до мережі 172.16.0.0*
2) Router(config)#access-list 102 permit ip any any – *доступ інших вузлів до мережі дозволено*
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 102 in

Завдання 1.4

Block Network to host

Необхідно блокувати доступ мережі 192.168.1.0 до вузла 172.16.0.1.

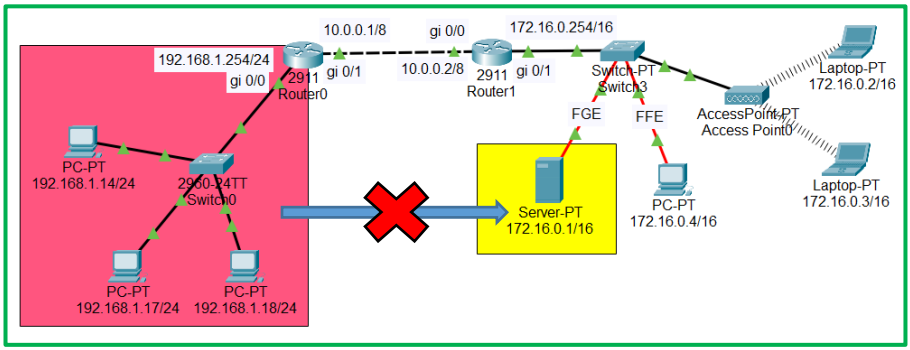


Рисунок 1.6 – Block Network to host

Приклад налаштування розширеного списку доступу (extended access list) на Router 1 на інтерфейсі gi 0/0

1) Router(config)#access-list 104 deny ip 192.168.1.0 0.0.0.255 172.16.0.1 0.0.0.0
2) Router(config)#access-list 104 permit ip any any
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 104 in

Для виконання наступних завдань необхідно відкрити файл із заздалегідь налаштованою мережею (Шаблон 2).

Завдання 1.5

Stop ping but can access web server

Одним із способів забезпечення безпеки WEB-серверів є заборона посилок на них ping-запитів, які потенційно можуть призвести до відмови обладнання. З цією метою необхідно створити список доступу, який фільтруватиме всі вхідні ping-запити на вхідному інтерфейсі маршрутизатора.

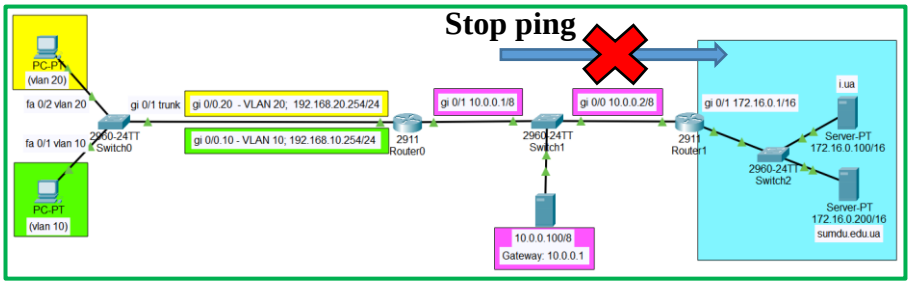


Рисунок 1.7 – Stop ping but can access web server

Приклад налаштування розширеного списку доступу (extended access list) на Router 1 на інтерфейсі gi 0/0

1) Router(config)#access-list 102 deny icmp any any echo
2) Router(config)#access-list 102 permit ip any any
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 102 in

Коректним результатом виконання завдання 1.5 буде, як і на початку, успішна робота WEB-серверів, але можливість їх пінгування з клієнтських PC буде заборонена.

Завдання 1.6

Block FTP, HTTP, etc

Для блокування протоколів прикладного рівня можна скористатися форматом розширених списків контролю доступу, у яких як параметр блокування зазначаються порти призначення транспортного рівня.

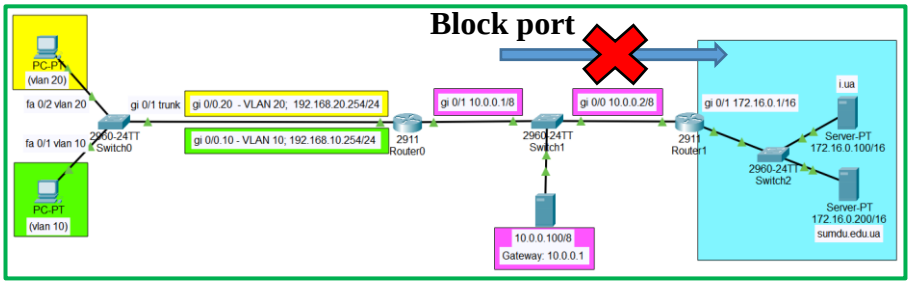
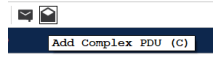


Рисунок 1.8 – Block port

Приклад налаштування розширеного списку доступу (extended access list) на Router 1 на інтерфейсі gi 0/0

1) Router(config)#access-list 102 deny tcp any any eq 21 – *значення 21 – це Well-Known Port для протоколу FTP, замість нього можна зазначити інше потрібне значення порту TCP/UDP*
2) Router(config)#access-list 102 permit ip any any
3) Router(config)#int gi 0/0
4) Router(config-if)#ip access-group 102 in

Для перевірки схеми слід використати можливості генератора пакетів 

, надіславши з клієнтських PC

на WEB-сервери у правому офісі одночасно запити за протоколом HTTP та FTP. Проаналізувати статус доставки пакетів.

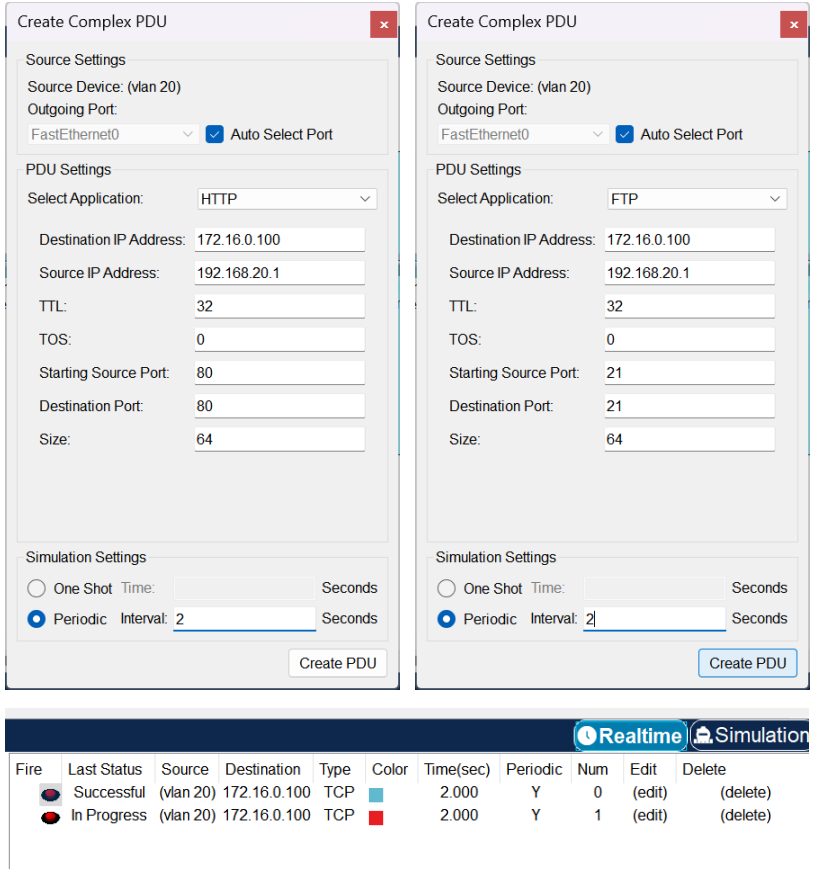


Рисунок 1.9 – Перевірка роботи блокування протоколів (портів)

Подібні експерименти провести з іншими протоколами, наприклад POP3 (110), HTTPS (443) тощо.

2 ПРОТОКОЛИ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ

Завдання 2.1.

Протокол RIP

Налаштувати мережу, у якій маршрутизація на роутерах буде здійснюватися за протоколом RIP (Routing Information Protocol) – дистанційно-векторний протокол, який оперує хопами як метрикою маршрутизації.

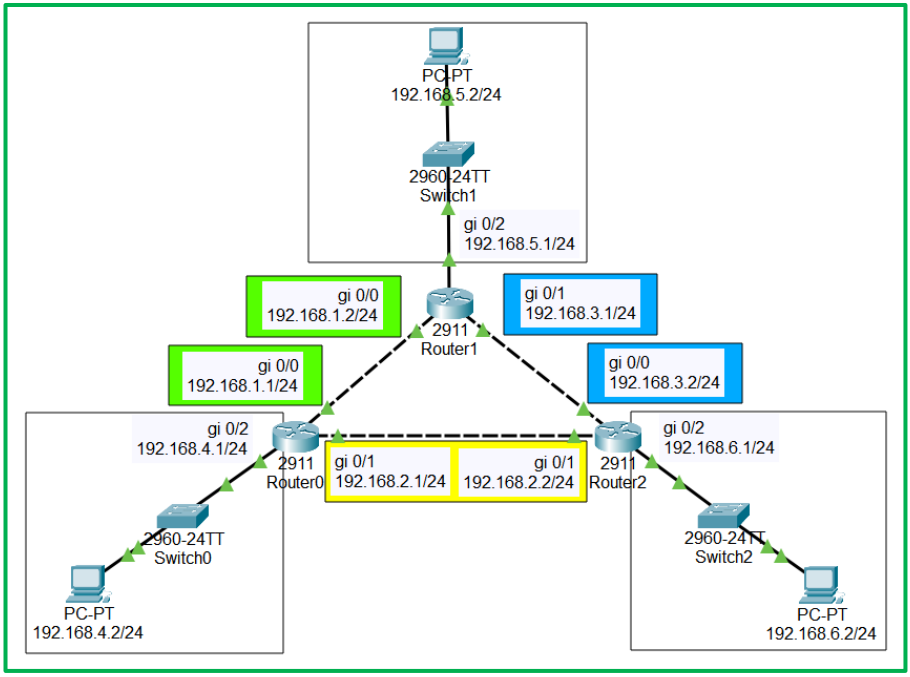


Рисунок 2.1 – Налаштування динамічної маршрутизації за протоколом RIP

На кожному маршрутизаторі потрібно налаштувати протокол RIP (у прикладі зазначено налаштування для Router1).

Під час налаштування протоколу динамічної маршрутизації перераховуються (свої) мережі, безпосередньо підключені до маршрутизатора.

1) Router>en
2) Router#conf term
3) Router(config)#router rip
4) Router(config-router)#network 192.168.1.0
5) Router(config-router)#network 192.168.3.0
6) Router(config-router)#network 192.168.5.0
7) Router(config-router)#exit
8) Router(config)#exit

Перевірка налаштувань маршрутизації здійснюється командою

9) Router#sh ip route

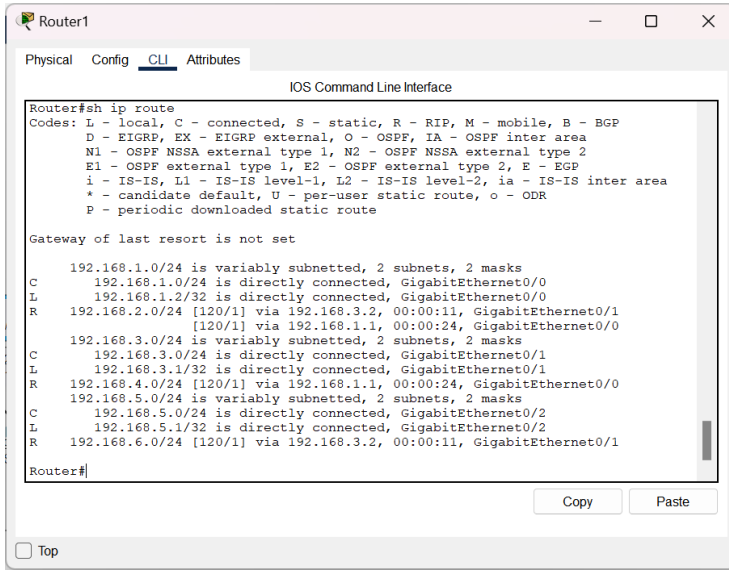
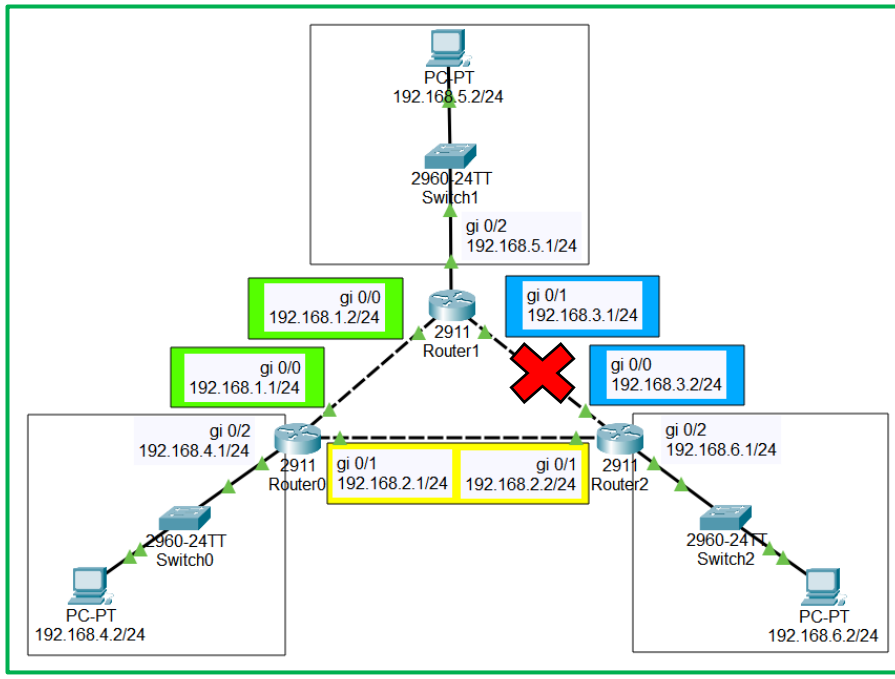


Рисунок 2.2 – Перевірка налаштувань динамічної маршрутизації за протоколом RIP



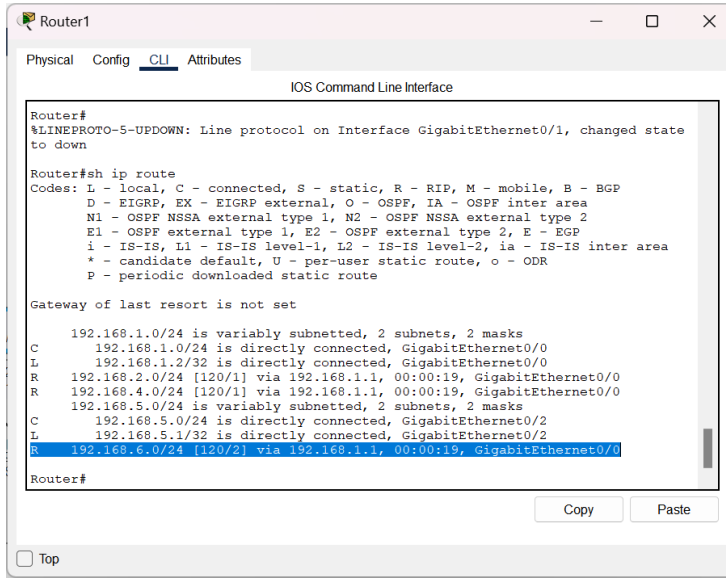


Рисунок 2.3 – Перебудова маршрутів у разі втрати з’єднання

У сучасних мережних середовищах RIP – не найкраще рішення для вибору як протоколу маршрутизації, тому що його можливості поступаються сучаснішим протоколам, таким як EIGRP, OSPF. Обмеження в 15 хопів не дає змоги застосовувати його у великих мережах. Перевага цього протоколу – простота конфігурування. Унаслідок простоти його підтримують практично всі маршрутизатори початкового рівня.

Завдання 2.2

Протокол EIGRP

Налаштувати мережу, у якій маршрутизація на роутерах буде здійснюватися завдяки протоколу EIGRP (Enhanced Interior Gateway Routing Protocol) – **пропрієтарний** протокол маршрутизації від фірми Cisco.

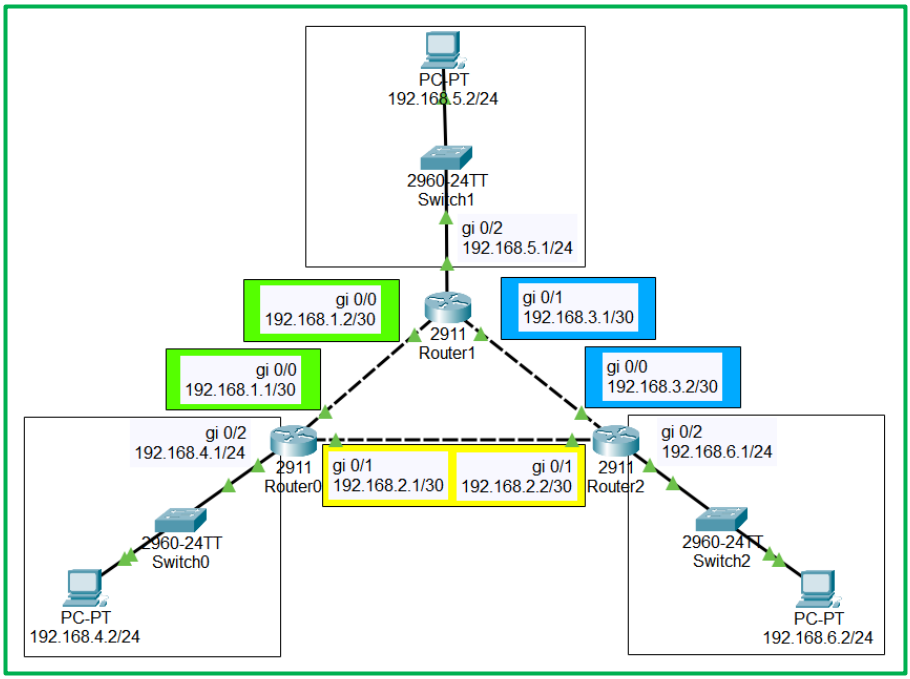


Рисунок 2.4 – Налаштування динамічної маршрутизації за протоколом EIGRP

Зверніть увагу на нестандартні маски мереж, EIGRP та OSPF, на відміну від RIPv1, їх підтримують.

На кожному маршрутизаторі потрібно налаштувати протокол EIGRP (у прикладі зазначено налаштування для Router1).

Ідеологічно налаштування подібні до протоколу RIP (перераховуються свої мережі), але є деякі свої особливості (номер автономної системи та наявність інвертної маски мережі).

1) Router>en
2) Router#conf term
3) Router(config)#router eigrp 333 – 333 – номер автономної системи (сукупність мереж, до яких можна звертатися як до одного об’єкта)
4) Router(config-router)#network 192.168.1.0 0.0.0.3
5) Router(config-router)#network 192.168.3.0 0.0.0.3
6) Router(config-router)#network 192.168.5.0 0.0.0.255
7) Router(config-router)#exit
8) Router(config)#exit

Перевірка налаштувань маршрутизації здійснюється командою

9) Router#sh ip route

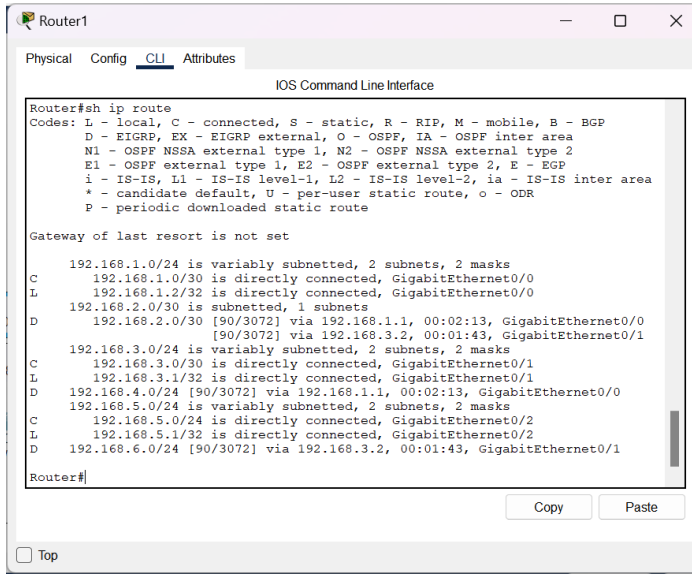


Рисунок 2.5 – Перевірка налаштувань динамічної маршрутизації за протоколом EIGRP

Якщо потрібно зазначити інтерфейс, через який не потрібно обмінюватися таблицею маршртутизації (наприклад мережа 192.168.4.0 /24 – тупікова мережа) слід використовувати команди:

10) Router#conf term
11) Router(config)#router eigrp 333
12) Router(config-router)#passive-interface gi 0/2
13) Router(config-router)#exit

Це дозволить не засмічувати мережу непотрібними повідомленнями, що підвищить її продуктивність та безпеку

Завдання 2.3.

Протокол OSPF

Налаштувати динамічну маршрутизацію на роутерах за допомогою протоколу OSPF (Open Shortest Path First) – **відкритий** протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology).

На кожному маршрутизаторі потрібно налаштувати протокол OSPF (у прикладі зазначено налаштування для Router1).

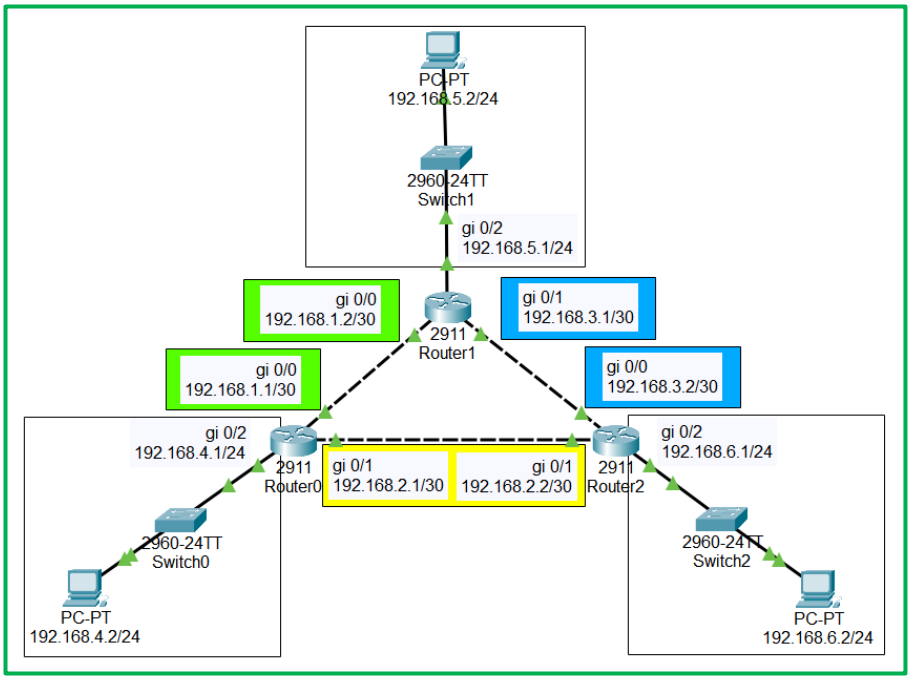


Рисунок 2.6 – Налаштування динамічної маршрутизації за протоколом OSPF

Ідеологічно налаштування подібні до попередніх налаштувань, але є можливість зазначити значення area для мереж.

1) Router>en
2) Router#conf term
3) Router(config)#router ospf 100
4) Router(config-router)#network 192.168.1.0 0.0.0.3 area 0
5) Router(config-router)#network 192.168.3.0 0.0.0.3 area 0
6) Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
7) Router(config-router)#exit

8) Router(config)#exit

Перевірка налаштувань маршрутизації здійснюється командою

9) Router#sh ip route

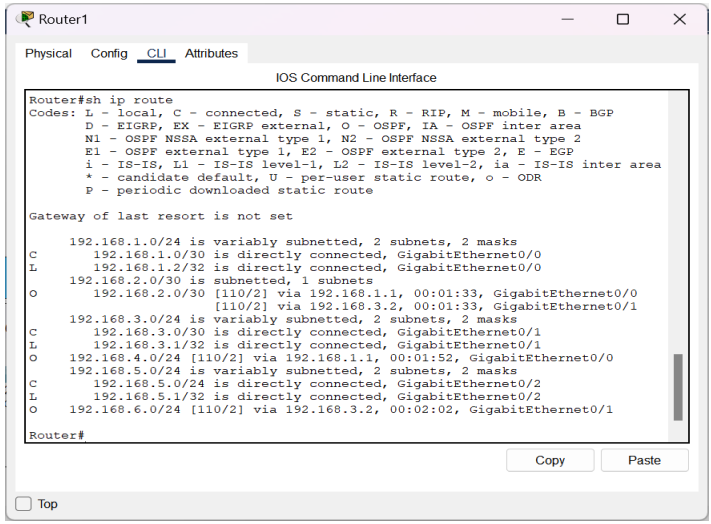


Рисунок 2.7 – Перевірка налаштувань динамічної маршрутизації за протоколом OSPF

Завдання 2.4

Протокол BGP

BGP (Border Gateway Protocol, протокол «граничного шлюзу») – на сьогодні є основним протоколом динамічної маршрутизації в інтернеті. Протокол BGP призначений для обміну інформацією про досяжність підмереж між автономними системами (АС, англ. AS – autonomous system), тобто групами маршрутизаторів під єдиним технічним та адміністративним керуванням, що використовують протокол внутрішньодоменної маршрутизації для визначення маршрутів усередні автономної системи та протокол міждоменної маршрутизації для визначення маршрутів доставки пакетів до інших АС.

Налаштуйте мережу, у якій для поєднання автономних систем із різними протоколами внутрішньої маршрутизації використовується протокол BGP.

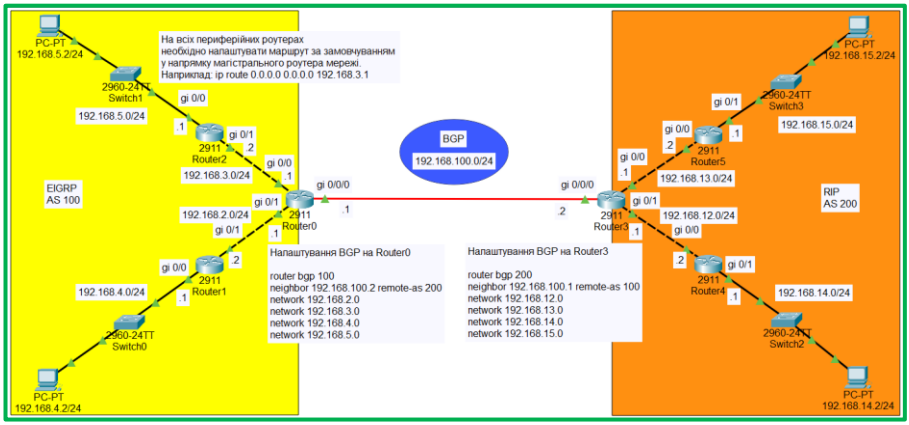


Рисунок 2.8 – Поєднання різних AS за допомогою протоколу BGP

Налаштування BGP на магістральному роутері AS 100

1) router bgp 100
2) neighbor 192.168.100.2 remote-as 200
3) network 192.168.2.0
4) network 192.168.3.0
5) network 192.168.4.0
6) network 192.168.5.0

На всіх периферійних роутерах необхідно налаштувати маршрут за замовчуванням у напрямку магістрального роутера мережі, наприклад: ip route 0.0.0.0 0.0.0.0 192.168.3.1

Перевірка налаштувань маршрутизації здійснюється командою

7) Router#sh ip route

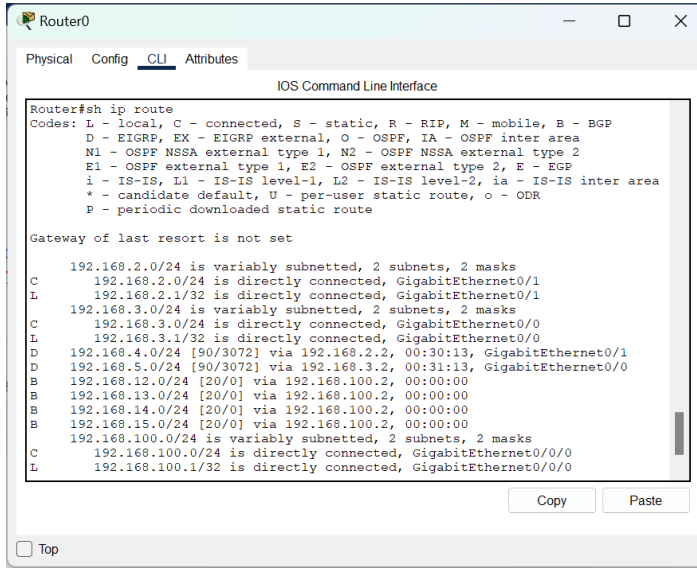


Рисунок 2.9 – Перевірка налаштувань динамічної маршрутизації за протоколом BGP EIGRP на Router0

3 КОМПЛЕКСНА ЛАБОРАТОРНА РОБОТА 1

Мета комплексної лабораторної роботи полягає у перевірці та оцінці викладачем здобутих знань та набутих навичок студентами під час виконання попередніх лабораторних робіт.

Завдання

Побудувати мережу аналогічно топології, наведеній на рисунку 3.1, налаштувати динамічну маршрутизацію на роутерах за протоколами EIGRP (AS 100) та OSPF (AS 200) і поєднати їх за допомогою протоколу BGP; налаштувати три різних сценарії списків контролю доступу (рисунок 3.2).

Номери мереж зазначати відповідно до призначеного вам варіанта у таблиці 3.1.

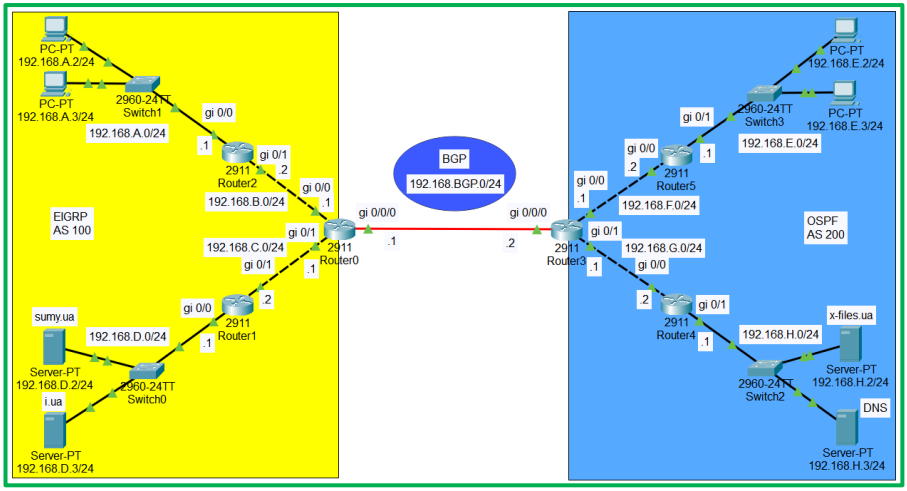


Рисунок 3.1 – Топологія мережі до комплексної лабораторної роботи 1 (на **«задовільно» та «добре»**)

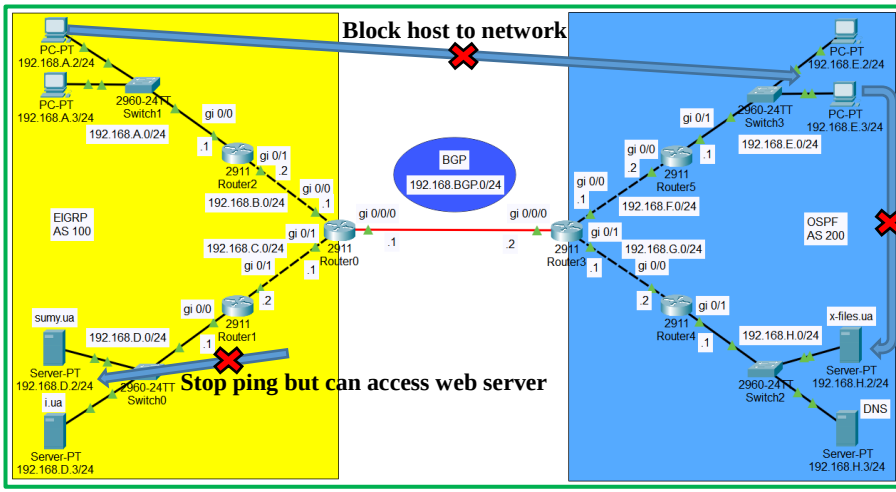


Рисунок 3.2 – Топологія мережі до комплексної лабораторної роботи 1 (**на «відмінно»**)

- Оцінку **«задовільно»** студент отримує за умови правильного налаштування динамічної маршрутизації в автономних системах за протоколами EIGRP (AS 100) та OSPF (AS 200).
- Оцінку **«добре»** студент отримує, якщо додатково до попереднього завдання за допомогою протоколу BGP поєднає AS 100 та AS 200, а також налаштує роботу WEB-серверів.
- Оцінку **«відмінно»** студент отримує, якщо додатково до попередніх двох пунктів будуть налаштовані три сценарії списків контролю доступу.

Таблиця 3.1 – Варіанти індивідуальних завдань

Варіант BGP	A	B	C	D	E	F	G	H
1	40	41	42	43	100	101	102	103
2	45	46	47	48	105	106	107	108
3	50	51	52	53	110	111	112	113
4	55	56	57	58	115	116	117	118
5	60	61	62	63	120	121	122	123
6	65	66	67	68	125	126	127	128
7	70	71	72	73	130	131	132	133
8	75	76	77	78	135	136	137	138
9	80	81	82	83	140	141	142	143
10	85	86	87	88	145	146	147	148
11	90	91	92	93	150	151	152	153
12	95	96	97	98	155	156	157	158
13	100	101	102	103	160	161	162	163
14	105	106	107	108	165	166	167	168
15	110	111	112	113	170	171	172	173
16	115	116	117	118	175	176	177	178
17	120	121	122	123	180	181	182	183
18	125	126	127	128	185	186	187	188
19	130	131	132	133	190	191	192	193
20	135	136	137	138	195	196	197	198
21	140	141	142	143	200	201	202	203
22	145	146	147	148	205	206	207	208
23	150	151	152	153	210	211	212	213
24	155	156	157	158	215	216	217	218
25	160	161	162	163	220	221	222	223
26	165	166	167	168	225	226	227	228
27	170	171	172	173	230	231	232	233
28	175	176	177	178	235	236	237	238
29	180	181	182	183	240	241	242	243
30	185	186	187	188	245	246	247	248

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Яке призначення списків контролю доступу?
2. Відмінність стандартних та розширених списків контролю доступу.
3. Які протоколи дозволяють фільтрувати розширені списки контролю доступу?
4. Який вигляд буде мати інвертна маска у списках контролю доступу у разі блокування доступу до конкретного вузла мережі та у разі блокування доступу до мережі загалом.
5. Які переваги динамічної маршрутизації порівняно зі статичною?
6. Назвіть переваги та недоліки протоколу динамічної маршрутизації RIP.
7. Назвіть переваги та недоліки протоколу динамічної маршрутизації EIGRP.
8. Яке значення буде мати метрика маршруту для протоколу EIGRP під час передавання даних через мережу довжиною у два хопа та швидкістю ліній зв’язку 1Gb/s.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Tanenbaum A. S., Feamster N., Wetherall D. J. Computer Networks. 6th Global Edition. – Pearson Education Limited, 2021. – 945 p.
2. Великодний Д. В. Курс «Мережі операторів та системи мобільного зв'язку» на платформі MIX СумДУ. Режим доступу: https://mix.sumdu.edu.ua/info/nmk/b04f041e-9453-4fda-b478-17e532ad0005.
3. Методичні вказівки до лабораторних робіт із дисциплін «Інформаційні та телекомунікаційні технології» та «Програмування в комп'ютерних мережах» [Електронний ресурс]: у 3 ч. Ч. 1: Основи Packet Tracer / укладач Д. В. Великодний. – Суми : СумДУ, 2022. – 44 с.
4. CCNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks. Anthony Bruno, Steve Jordan. Cisco Press, 2020. – 1100 p.
5. Жураковський Б. Ю. Комп'ютерні мережі [Електронний ресурс] : навч. посіб. / Б. Ю. Жураковський, І. О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – Ч. 2. – 372 с.
6. Коробейнікова Т. І. Комп'ютерні мережі : навч. посіб. / Т. І. Коробейнікова, С. М. Загарченко. – Львів : Львівська політехніка, 2022. – 228 с.

Електронне навчальне видання

Методичні вказівки
до лабораторних робіт
на тему **«Списки контролю доступу та динамічна маршрутизація»**
з дисципліни **«Мережі операторів та системи мобільного зв'язку»**
для здобувачів спеціальності 122 *«Комп'ютерні науки»*
освітнього ступеня «бакалавр»
усіх форм здобуття вищої освіти

Відповідальна за випуск О. А. Шовкопляс
Редакторка Т. Г. Чернишова
Комп'ютерне верстання Д. В. Великодного

Формат 60x84/16. Ум. друк. арк. 1,74. Обл.-вид. арк. 1,10.

Видавець і виготовлювач
Сумський державний університет,
вул. Харківська, 116, м. Суми, 40007
Свідоцтво про внесення суб'єкта господарювання до Державного реєстру видавців, виготовлювачів та розповсюджувачів видавничої продукції ДК № 8193 від 15.10.2024.