МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМ. ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОІНЖЕНЕРІЇ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

Микитишин А.Г., Стухляк Д.П., Королюк Р.І.

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМПЛЕКСНА БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖЕВИХ СИСТЕМ

Частина 2

(лабораторні роботи №6-№9)

для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»

Тернопіль
2022

Методичні вказівки до лабораторних робіт з курсу «Комплексна безпека інформаційних мережевих систем». Частина 2 (лабораторні роботи №6-№9). Для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / укл.: А.Г. Микитишин, Д.П. Стухляк, Р.І. Королюк. – Тернопіль: ТНТУ імені Івана Пулюя, 2022. – 20 с.

Рецензент: д.т.н., професор Лупенко С.А.

Відповідальний за випуск: к.т.н., доцент Микитишин А.Г.

Методичні вказівки розглянуто і схвалено на засіданні кафедри комп'ютерно-інтегрованих технологій (протокол №2 від 06.09.2022 р.)

Схвалено та рекомендовано до друку науково-методичною комісією факультету прикладних інформаційних технологій та електроінженерії (протокол №2 від 04.10.2022 р.)

Методичні вказівки призначені для проведення лабораторних робіт дисципліни «Комплексна безпека інформаційних мережевих систем» для студентів, які навчаються за спеціальністю 151 – «Автоматизація та комп'ютерно-інтегровані технології». Викладені матеріали приведені з урахуванням модульної системи навчання, рекомендацій до самостійної роботи і індивідуальних завдань, тем лабораторних занять, тестів, екзаменаційних питань, типової форми та вимог для комплексної перевірки знань з дисципліни.

ЗМІСТ

Лабораторна робота №6

Створення комутованої мережі з резервними каналами

Мета роботи:

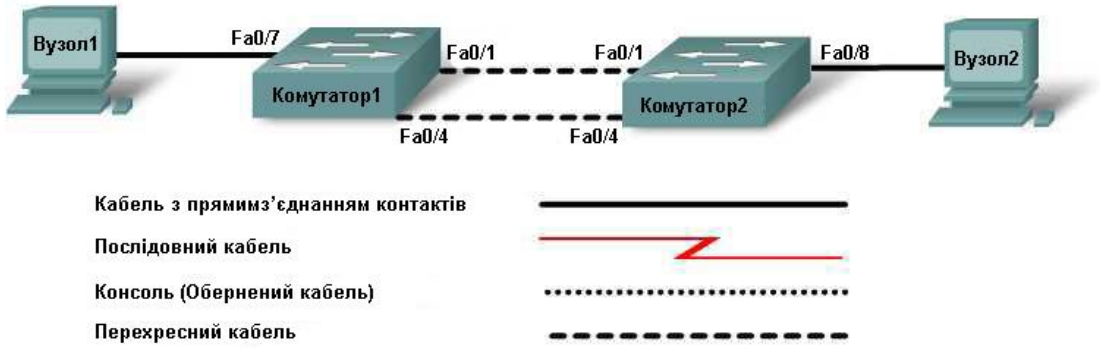
- Створити комутовану мережу з резервними каналами.
- Визначити, який комутатор обраний в якості кореневого моста з заводськими налаштуваннями за замовчуванням.
- Виконати налаштування ідентифікатора BID на комутаторі для контролю вибору кореневого моста.

Вихідні дані.

У даній лабораторній роботі досліджується вплив вибору кореневого моста на організацію з'єднань в комутованої мережі з резервними каналами. Спочатку виконується конфігурування мережі із заводськими налаштуваннями, а потім переназначається кореневий міст, змінивши значення пріоритетності мосту.

Необхідно використовувати такі ресурси:

- два комутатора Cisco 2960 або аналога;
- два комп'ютери: один в якості клієнта, інший - сервера;



Топологія мережі

Номер коммутатора	Пароль з шифруванням привілейованого доступу	Пароль консолі, каналу vty і пароль з шифруванням	IP-адрес	Маска підмережі
Комутатор 1	class	cisco	192.168.1.2	255.255.255.0
Комутатор 2	class	cisco	192.168.1.3	255.255.255.0

Крок 1. Підключення вузлів мережі

1. Підключіть вузол 1 до порту Fa0/7 комутатора 1 за допомогою прямого кабелю Ethernet.
2. Підключіть вузол 2 до порту Fa0/8 комутатора 2 за допомогою прямого кабелю Ethernet.
3. Підключіть порт Fa0/1 комутатора 1 до порту Fa0/1 комутатора 2 за допомогою перехресного кабелю Ethernet.
4. Створіть резервний канал між комутаторами, приєднавши порт Fa0/4 комутатора 1 до порту Fa0/4 комутатора 2 за допомогою перехресного кабелю Ethernet.

Який, як правило, небажаний тип з'єднання ви створили, з'єднавши два комутатора за допомогою перехресного кабелю?

Припустіть, яким чином комутатори можуть протидіяти виникненню цієї проблеми?

Крок 2. Налаштування комутаторів

1. Задайте в конфігурації комутатора 1 назву вузла, паролі, IP-адрес інтерфейсу VLAN 1 і маску підмережі.
2. Збережіть конфігурацію.
3. Задайте в конфігурації комутатора 2 назву вузла, паролі, IP-адрес інтерфейсу VLAN 1 і маску підмереж.
4. Збережіть конфігурацію.

Крок 3. Налаштування вузлів

1. Задайте кожному вузлу IP-адрес та маску підмережі з тієї ж мережі, що і комутатор.

Чому для даної мережі не вказаний шлюз за замовчуванням?

Крок 4. Перевірка підключення

1. Для перевірки з'єднання виконайте тестування з використанням ехо-запитів з вузла 1 на вузол 2.

Якщо ехо-запит виконати не вдалося, який засіб можна використовувати для визначення в якому місці мережі стався збій?

Крок 5. Вивчення інформації інтерфейсу VLAN 1

1. З привілейованого режиму EXEC введіть команду:

SwitchA#**show interface vlan1 ?**

Перерахуйте деякі з доступних параметрів.

2. З привілейованого режиму EXEC на комутаторі SwitchA введіть команду:

SwitchA#**show interface vlan1**

Яка MAC-адреса у комутатора?

3. З привілейованого режиму EXEC на комутаторі SwitchB введіть команду **show interface vlan1.**

Яка MAC-адреса у комутатора?

Який комутатор повинен бути кореневим комутатором STP дерева для даної мережі?

Крок 6. Вивчення таблиць STP дерева на кожному комутаторі

1. З привілейованого режиму EXEC на комутаторі SwitchA введіть команду **show spanning-tree**.
2. З привілейованого режиму EXEC на комутаторі SwitchB введіть команду **show spanning-tree**.
3. Вивчіть вихідні дані і дайте відповідь на наступні питання:

Який комутатор є кореневим?

Який пріоритет має кореневий міст?

Який ідентифікатор BID має кореневої міст?

Які порти кореневого моста є передаючими?

Які порти кореневого моста є блокуючими?

Який пріоритет має некореневий міст?

Який ідентифікатор BID має некореневий міст?

Які порти некореневого мосту є передаючі?

Які порти некореневого мосту є блокуючими?

4. Вивчіть індикатори зв'язку на обох комутаторах.

Чи можна визначити, який з портів знаходиться в блокуючому стані?

Чому стан індикаторів зв'язку не змінився?

Крок 7. Перепризначення кореневого моста

Що потрібно зробити, щоб змінити в даній мережі кореневий міст

Чому виникає необхідність це зробити?

Припустимо, що комутатор, який є в даний момент кореневим мостом (комутатор A), є небажаним.

Щоб призначити комутатор B новим кореневим мостом, необхідно задати для нього в налаштуваннях конфігурації новий пріоритет.

1. Увійдіть в режим конфігурації на комутаторі B.
2. Визначте параметри, які можуть бути налаштовані для протоколу STP, виконавши наступну команду:

SwitchB(config)#**spanning-tree ?**

3. Перерахуйте доступні параметри:
4. Встановіть пріоритет комутатора в значення 4096.

SwitchB(config)#**spanning-tree vlan 1 priority 4096**

SwitchB(config)#**exit**

Крок 8. Вивчення таблиці сполучного дерева

1. З привілейованого режиму EXEC на комутаторі SwitchA введіть команду **show spanning-tree**.
2. З привілейованого режиму EXEC на комутаторі SwitchB введіть команд **show spanning-tree.**
3. Вивчіть вихідні дані і дайте відповідь на наступні питання:

Який комутатор є кореневим?

Який пріоритет має кореневий міст?

Який ідентифікатор BID має кореневий міст?

Які порти кореневого моста є передаючі?

Які порти кореневого моста є блокуючими?

Який пріоритет має некореневий міст?

Який ідентифікатор BID має некореневий міст?

Які порти некореневого мосту є передаючі?

Які порти некореневого мосту є блокуючими?

Крок 9. Перевірка файлу поточної конфігурації на кореневому мості

1. Після того, як комутатор став кореневим мостом, введіть у привілейованому режимі EXEC команду **show running-config**.
2. Знайдіть інформацію про пріоритет цього комутатора в STP.
3. Як можна визначити, виходячи з цієї інформації, що комутатор є кореневим мостом?

Лабораторна робота №7

Налаштування протоколів аутентифікації PAP і CHAP

Мета роботи: Налаштування аутентифікації PPP за допомогою PAP і CHAP

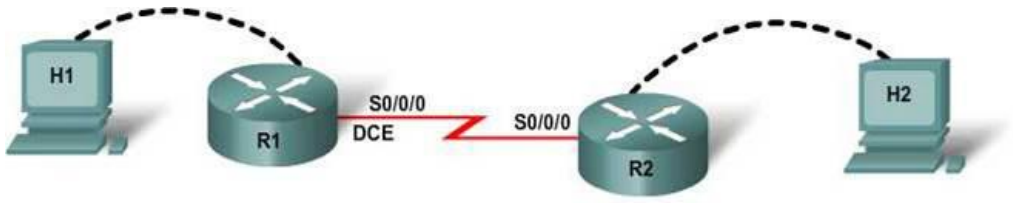
Вихідні дані.

Підключіть мережеве обладнання відповідно до топології мережі. Для даної лабораторної роботи підходить будь-який маршрутизатор з одним послідовним інтерфейсом. Можна використати маршрутизатор Cisco 1841 з модулем WIC-2T, що містить 2 послідовних інтерфейси.

Інформація, що міститься в цій лабораторній роботі, поширюється і на інші маршрутизатори, проте синтаксис командної мови може відрізнятися. Залежно від моделі маршрутизатора інтерфейси можуть визначатися по-різному. Наприклад, на деяких маршрутизаторах послідовний інтерфейс Serial 0 може бути представлений як Serial 0/0 або Serial 0/0/0, а Ethernet 0 – як FastEthernet 0/0. Інформація в цій лабораторній роботі поширюється на маршрутизатори Cisco 1841, в яких послідовний порт представляється Serial 0/0/0. Якщо використовується інший маршрутизатор, використовуйте відповідне представлення послідовного інтерфейсу.

Необхідно використовувати наступні ресурси:

- два маршрутизатори з послідовним з'єднанням;
- два комп’ютери;
- консольні кабелі для налаштування маршрутизаторів;
- один двокомпонентний послідовний кабель (DTE/DCE);



Пристрій	IP-адрес інтерфейсу Serial 0/0/0 та маска підмережі	Тип інтер-фейсу Serial 0/0/0	Пароль з шифру-ванням для доступу в привілейований режим	Пароль консолі, каналу vty
Маршрутизатор R1	192.168.15.1/24	DCE	class	cisco
Маршрутизатор R2	192.168.15.2/24	DTE	class	cisco

Крок 1. Підключення обладнання

З'єднаєте маршрутизатори 1 і 2 послідовним кабельним з'єднанням (DTE/DCE) з інтерфейсами Serial 0/0/0, як вказано в діаграмі топології.

Крок 2. Базове конфігурування маршрутизатора R1

На маршрутизаторі R1 задайте ім'я вузла, IP-адресу і паролі згідно таблиці адресації. Збережете конфігурацію.

Крок 3. Базове конфігурування маршрутизатора R2

На маршрутизаторі R2 задайте ім'я вузла, IP-адресу і паролі згідно таблиці адресації. Збережете конфігурацію.

Крок 4. Налаштування інкапсуляції PPP на маршрутизаторах R1 і R2

Змініть тип інкапсуляції на PPP, ввівши команду **encapsulation ppp** в рядку режиму конфігурації інтерфейсу Serial0/0 на обох маршрутизаторах.

```
R1(config-if) #encapsulation ppp
R2(config-if) #encapsulation ppp
```

Крок 5. Перевірка інкапсуляції PPP на маршрутизаторах R1 і R2

Введіть команду **show interface serial 0/0/0**, аби перевірити інкапсуляцію PPP на маршрутизаторах R1 і R2.

```
R1#show interface serial 0/0/0
R2#show interface serial 0/0/0
```

Переконайтесь, чи використовують маршрутизатори R1 та R2 інкапсуляцію PPP?

Крок 6. Перевірка функціонування послідовного з'єднання

Відправте ехо-запити між маршрутизаторами R1 та R2, аби переконатися в наявності з'єднання між ними.

```
R1#ping 192.168.15.2
R2#ping 192.168.15.1
```

Переконайтесь, чи проходять ехо-запити між маршрутизаторами R1 та R2. Якщо ні, то виконаєте пошук і усунення помилок в конфігурації маршрутизаторів. Повторюйте відправку ехо-запитів до здобуття успішного результату.

Крок 7. Налаштування аутентифікації PPP на маршрутизаторі R1 за допомогою протоколу PAP

Задайте ім'я користувача і пароль на маршрутизаторі R1. Ім'я користувача має бути ідентичним імені вузла іншого маршрутизатора. І пароль, і ім'я користувача є реєстрозалежними. На маршрутизаторах Cisco пароль з шифруванням має бути однаковим для обох маршрутизаторів.

```
R1(config) #username R2 password cisco
R1(config) #interface serial 0/0/0
R1(config-if) #ppp authentication pap
```

У Cisco IOS версії 11.1 або пізніше на інтерфейсі необхідно включати PAP, оскільки він відключений за умовчанням. У рядку режиму конфігурації інтерфейсу Serial 0/0/0 включіть PAP на інтерфейсі.

```
R1(config-if) #ppp pap sent-username R1 password cisco
```

Крок 8. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки ехо-запиту послідовному інтерфейсу маршрутизатора R2.

Чи була перевірка успішною?

Крок 9. Налаштування аутентифікації PPP на маршрутизаторі R2 за допомогою протоколу PAP

Аналогічно до кроку 7, задайте ім'я користувача і пароль на маршрутизаторі R2 та включіть PAP на інтерфейсі Serial 0/0/0.

```
R2(config) #username R1 password cisco
R2(config) #interface serial 0/0/0
R2(config-if) #ppp authentication pap
R2(config-if) #ppp pap sent-username R2 password cisco
```

Крок 10. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки ехо-запиту послідовному інтерфейсу маршрутизатора R1.

Чи була перевірка успішною?

Крок 11. Видалення PAP з маршрутизаторів R1 і R2

Видаліть PAP з маршрутизаторів R1 і R2 за допомогою команди **no** напроти команд, що використовувались для конфігурації PAP.

```
R1(config) #interface serial 0/0/0
R1(config-if) #no ppp authentication pap
```

```
R1(config-if) #no ppp pap sent-username R1 password cisco
R1(config-if) #exit
R1(config) #no username R2 password cisco

R2(config) #interface serial 0/0/0
R2(config-if) #no ppp authentication pap
R2(config-if) #no ppp pap sent-username R2 password cisco
R2(config-if) #exit
R2(config) #no username R1 password cisco
```

Крок 12. Налаштування аутентифікації PPP на маршрутизаторі R1 за допомогою протоколу CHAP

Якщо включені і CHAP, і PAP під час фази узгодження зв'язку запрошується перший вказаний метод аутентифікації. Якщо одноранговий вузол передбачає використання другого методу або просто відмовляється використовувати перший метод, робиться спроба використовувати другий метод.
Збережіть конфігурацію на маршрутизаторах R1 і R2 і перезавантажте їх.

```
R1#copy running-config startup-config
R1#reload

R2#copy running-config startup-config
R2#reload
```

Задайте ім'я користувача і пароль на маршрутизаторі R1.

```
R1(config) #username R2 password cisco
R1(config) #interface serial 0/0/0
R1(config-if) #ppp authentication chap
```

Крок 13. Налаштування аутентифікації PPP на маршрутизаторі R2 за допомогою протоколу CHAP

Задайте ім'я користувача і пароль на маршрутизаторі R2.

```
R2(config) #username R1 password cisco
R2(config) #interface serial 0/0/0
R2(config-if) #ppp authentication chap
```

Крок 14. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки ехо-запиту на послідовний інтерфейс маршрутизатора R1.
Чи була перевірка успішною?

Крок 15. Перевірка інкапсуляції на маршрутизаторах R1 та R2

Введіть команду **show interface serial 0/0/0** для перегляду відомостей про інтерфейс.

R1#show interface serial 0/0/0
R2#show interface serial 0/0/0

Яким є стан інтерфейсу Serial 0/0/0?
Протокол лінії _____
Інкапсуляція _____
Чи відкритий протокол LCP? _____
Скільки протоколів NCP було встановлено? _____

Питання для повторення

1. Які переваги використання CHAP в порівнянні з PAP?
2. Який протокол PPP використовується для установки магістральної лінії?
3. Який протокол PPP використовується для конфігурації різних протоколів мережевого рівня?

Лабораторна робота №8

Налаштування та перевірка розширених ACL-списків для фільтрації трафіку по номерах портів

Мета роботи: Налаштування розширеного ACL-списку для фільтрації трафіку по номерах портів

Вихідні дані.

Служба безпеки вирішила підсилити захист серверів. Необхідно, щоб у мережі 10.10.10.0 був дозволений лише веб-трафік і DNS. Всі інші види трафіку в мережі 10.10.10.0 мають бути заборонені.

Крок 1. Перевірка поточного підключення

1. Відправте ехо-запит на сервер **DNS** (10.10.10.250) з комп'ютера **PC0**.
2. Відправте ехо-запит на **веб-сервер** (10.10.10.254) з комп'ютера **PC0**.
3. Повторіть кроки для **PC1.**

Крок 2. Створення розширеного ACL-списку

1. Виберіть маршрутизатор **ISP**.
2. Увійдіть в режим конфігурування.
3. Створіть розширений список доступу з номером 100. Введіть наступні команди:

```
access-list 100 permit tcp any host 10.10.10.254 eq 80
access-list 100 permit udp any host 10.10.10.250 eq 53
access-list 100 deny ip any any
```

4. Застосуєте цей ACL-список до інтерфейсу Fast Ethernet 0/0 в якості вихідного.

Крок 3. Перевірка списку доступу

1. Відправте ехо-запит на сервер **DNS** (10.10.10.250) з комп'ютера **PC0**.
2. Відправте ехо-запит на **веб-сервер** (10.10.10.254) з комп'ютера **PC0**.
3. Перейдіть на сайт **www.cisco.com** з **PC0**.
4. Повторіть дані кроки для **PC1.**

Ехо-запити мають бути невдалими. Якщо ви можете перейти на **www.cisco.com**, то ACL-список налагоджений правильно, тобто дозволений лише трафік HTTP і DNS.

5. Виберіть **Check Results**.

Питання для повторення

1. Які найбільш поширені скорочення використовуються для позначення стану порту?
2. Закінчіть наступний ACL-список, дозволяючий TCP-порти в діапазоні 20 — 80.

ip access-list 100 permit tcp any 192.168.1.0 0.0.0.255

3. Яка інструкція, що мається на увазі, стоїть в кінці будь-якого списку доступу?

Лабораторна робота №9

Створення стандартних, розширених та іменованих ACL-списків

Мета роботи: Створення стандартних, розширених та іменованих ACL-списків для підвищення безпеки мережі

Вихідні дані.

Підрозділу обслуговування мережі потрібен доступ до маршрутизатора, що встановлений у Лондоні. Необхідно налаштувати ACL-список для надання співробітникам відділу техобслуговування доступ до маршрутизатора по протоколу telnet, і одночасно, заборонити доступ до вказаного маршрутизатора усім іншим користувачам. Для задоволення цих вимог необхідно створити додаткові ACL-списки на маршрутизаторах London і DC.

- Дозвольте доступ до сервера і ресурсів London всім клієнтам London і обмежте доступ усім іншим користувачам.
- Дозвольте доступ до сервера і ресурсів DC всім клієнтам DC і обмежте доступ усім іншим користувачам.

Пароль привілейованого режиму: **admin.**

Крок 1. Створення стандартного списку доступу для обмеження VTY-доступу

1. Виберіть маршрутизатор **London**.
2. Налаштуйте канали **vty 0–4** для входу. Встановіть пароль **cisco123**.
3. Створіть стандартний список доступу, який дозволить віддалений доступ для всіх клієнтів з підмережі техобслуговування.
   - Дайте списку доступу номер 10.
   - Підмережа техобслуговування: 172.16.50.0 255.255.255.0.
4. Застосуйте список доступу до каналів vty 0-4.

   Увійдіть в режим конфігурування та введіть команди:

   line vty 0 4

   access-class 10 in
5. Збережіть конфігурації.

Крок 2. Створення розширеного списку доступу на маршрутизаторі DC

1. Сплануйте і створіть на маршрутизаторі DC нумеровані списки доступу, які задовольняли б наступним вимогам.
   1) Створити один вихідний список доступу з номером 150 і застосувати його до інтерфейсу Fast Ethernet 0/1.1
   2) Створити один вихідний список доступу з номером 160 і застосувати його до інтерфейсу Fast Ethernet 0/1.2

Клієнти	Відправник	Ресурси	Отримувач	Дозволити	Заборонити	Протокол
Клієнти London	172.16.100.0 255.255.255.0	Ресурси London	172.16.20.0 255.255.255.0	X		Всі
Клієнти DC	172.16.10.0 255.255.255.0	Сервер London	172.16.20.100 255.255.255.0	X		Тільки HTTP
Клієнти DC	172.16.10.0 255.255.255.0	Ресурси London	172.16.100.0 255.255.255.0		X	ICMP
Клієнти DC	172.16.10.0 255.255.255.0	Ресурси DC	172.16.30.0 255.255.255.0	X		Всі
Клієнти London	172.16.100.0 255.255.255.0	Сервер DC	172.16.30.100 255.255.255.0	X		Тільки HTTP
Клієнти London	172.16.100.0 255.255.255.0	Ресурси DC	172.16.10.0 255.255.255.0		X	ICMP

2. Збережіть конфігурації.

Крок 3. Створення іменованого списку доступу на маршрутизаторі London

1. Сплануйте і створіть на маршрутизаторі **London** іменований список доступу, що задовольняє таким вимогам. Назвіть цей список доступу **ICMP**.

Клієнти	Відправник	Ресурси	Отримувач	Дозволити	Заборонити	Протокол
Клієнти DC	172.16.10.0 255.255.255.0	Клієнти London	172.16.100.0 255.255.255.0	X		ICMP
Клієнти DC	172.16.10.0 255.255.255.0	Клієнти London	172.16.100.0 255.255.255.0		X	Всі

2. Застосуйте цей список доступу до послідовного інтерфейсу в якості вхідного ACL-списку.
3. Збережіть конфігурацію.

Крок 4. Перевірка налаштованого списку доступу

1. Перевірте обмеження vty, що використовуються на маршрутизаторі London:

1) Виберіть комп'ютер **Maint** і встановіть сеанс telnet з маршрутизатором **London**.
2) Виберіть **PC2** і встановіть сеанс telnet з маршрутизатором **London**.

Сеанс telnet з комп'ютера **Maint** повинен бути створений успішно, а сеанс з **PC2** повинен бути заборонений.

2. Перевірте розширений ACL-список на маршрутизаторі **DC**.

1) Виберіть **PC2** і перейдіть на сервер **DC** (172.16.30.100).
2) Виконайте ехо-тестування сервера **DC** (172.16.30.100).
3) Перейдіть на сервер **London** (172.16.20.100).
4) Виконайте ехо-тестування сервера **London** (172.16.20.100).
5) Виберіть **PC1** і перейдіть на сервер **London** (172.16.20.100).
6) Виконайте ехо-тестування сервера **London** (172.16.20.100).
7) Перейдіть на сервер **DC** (172.16.30.100).
8) Виконайте ехо-тестування сервера **DC** (172.16.30.100).

Перехід повинен пройти успішно, а ехо-запити від **PC2** до сервера **London** та від **PC1** до сервера **DC** повинні бути невдалими.

3. Перевірте іменований список доступу на маршрутизаторі **London**.

1) Виберіть **PC2** і відправте ехо-запит на **PC1**.
2) З **PC2** викличте сервер **Server0** (172.16.100.250).

Ехо-запит має бути успішним, а виклик повинен привести до помилки по перевищенні часу очікування.

4. Виберіть **Check Results**.

Питання для повторення

1. Яке значення має слово "**out**" в кінці рядка ip access-group?
2. Чим відрізняються команди додавання ACL-списку до конкретного інтерфейсу і VTY?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, «Магнолія 2006», 2013. – 256 с.
2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, «Магнолія 2006», 2014. – 312 с.
3. Микитишин А.Г., Митник, П.Д. Стухляк. Телекомунікаційні системи та мережі – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
4. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. Вид. Львів: Бак, 2003. – 584 с.
5. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
6. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. —С-Пт. : Питер, 2013. — 960 с.
7. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологи, протоколы: Ученик для вузов. 5-е узд.– СПб.: Питер, 2016. – 992 с.
8. Амато, Вито. Основы организации сетей Cisco, том 1.: Пер. с англ. - М.: Издательский дом "Вильяме",2002.
9. Амато, Вито. Основы организации сетей Cisco, том 2.: Пер. с англ. - М.: Издательский дом "Вильяме", 2002.
10. Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. / Царьов Р.Ю., Нікітюк Л. А., Резніченко П. І. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 260 с.: іл.
11. Крук Б.И, Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2003. – 647 с.
12. Катунин Г.П., Мамчев Г.В., Попантонопуло Б.И, Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2004. – 672 с.
13. Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 3 – Мультисервисные сети/; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2005. – 592 с.
14. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавничій Центр, 2002. – 520 с.