



Міністерство освіти та науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки

Кафедра інформатики та програмної інженерії

ЗВІТ

з дисципліни «Основи комп'ютерних систем та мереж»
лабораторна робота №6
Списки доступу ACL.

Виконав:

Студент I курсу
групи ІІІ-45
Янов Б.Є.

Перевірила:

к.т.н., доц. Зенів І.О.

Мета: Навчитись працювати з ACL.

Списки доступу (access-lists) використовуються в цілому ряді випадків і є механізмом завдання умов, які роутер перевіряє перед виконанням будь-яких дій. Маршрутизатор перевіряє кожен пакет і на підставі перерахованих вище критеріїв, зазначених в ACL визначає, що потрібно зробити з пакетом, пропустити або відкинути. Типовими критеріями є адреси відправника і одержувача пакету, тип протоколу. Кожен критерій в списку доступу записується окремим рядком. Список доступу в цілому являє собою набір рядків з критеріями, що мають один і той же номер (або ім'я). Порядок завдання критеріїв в списку істотний. Перевірка пакету на відповідність списку проводиться послідовним застосуванням критеріїв з даного списку (в тому порядку, в якому вони були введені). Пакет, який не відповідає жодному з введених критеріїв буде відкинутий. Для кожного протоколу на інтерфейс може бути назначено тільки один список доступу. Як наприклад нижче приведена таблиця списку управління доступом за замовчуванням:

№ правила	Підмережа	Кінцева точка	Дозволити або заборонити
100	0.0.0.0/0	3389	Заборонити

Без ACL - за замовчуванням при створенні кінцевої точки їй все дозволено.

Дозволити - при додаванні одного або декількох діапазонів "дозволу" всі інші діапазони за замовчуванням забороняються. Тільки пакети з дозволеного діапазону IP-адрес зможуть досягти кінцевої точки віртуальної машини.

Заборонити - при додаванні одного або декількох діапазонів "заборонити" всі інші діапазони трафіку за замовчуванням дозволяються.

Поєднання дозволу і заборони - можна використовувати поєднання (комбінацію) правил "дозволити" і "заборонити", щоб вказати вкладений дозволений або заборонений діапазон IP-адрес.

Розглянемо два приклади стандартних списків:

access-list 1 permithost 10.0.0.10 - дозволяємо проходження трафіку від вузла 10.0.0.10.

access-list 2 deny 10.0.1.0 0.0.0.255 - забороняємо проходження пакетів із підмережі 10.0.1.0/24.

Практичне завдання 6-1.

Створення стандартного списку доступу.

Списки доступу бувають декількох видів: стандартні, розширені, динамічні та інші. У стандартних ACL є можливість задати лише IP адресу джерела пакетів для їх заборони або дозволів.

Створив мережу з 2 ПК, комутатора, роутера та сервера (Рис. 6.1). Зелені трикутники вказують на успішність з'єднання.

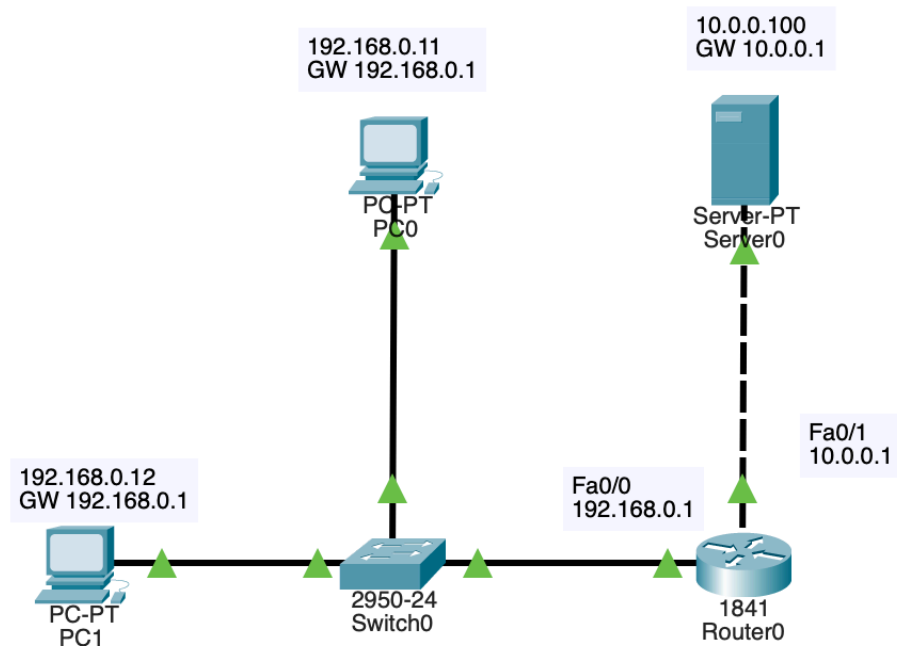


Рис. 6.1. Мережа мережі для завдання.

Потрібно дозволити доступ на сервер PC1 з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 - заборонити

Інтерфейс 0/0 маршрутизатора 1841 налаштував на адресу 192.168.0.1, 0/1 на 10.0.0.1 (Рис. 6.2).

```
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip addr 192.168.0.1 255.255.255.0
Router(config-if)#int fa0/1
Router(config-if)#ip addr 10.0.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
```

Рис. 6.2. Налаштування роутера.

Перевірив зв'язок ПК з різних мереж (Рис. 6.3).

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Рис. 6.3. ПК з різних мереж можуть спілкуватися.

Правило заборони та дозволу доступу будемо складати з використанням стандартних списків доступу (ACL). Поки не заданий список доступу на інтерфейсі все дозволено (permit). Але, варто створити список, відразу діє механізм "Все, що не дозволено, то заборонено". Тому нема потреби щось забороняти (deny) - вказуємо що дозволено. За умовами завдання нам потрібно на R0 пропустити пакети з вузла 192.168.0.12 на сервер (Рис. 6.4).

Застосовується дане правило на інтерфейс залежно від напрямку (PC1 розташований з боку порту Fa0/0). Ця установка означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0/0 на вхідному (in) від PC1 напрямку.

```

Router(config)#access-list 1 permit host 192.168.0.12
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#

```

Рис. 6.4. Створюємо на R0 дозволяє ACL.

Примітка: Вхідний трафік (in) - цей той, який приходить на інтерфейс ззовні. Вихідний (out) - той, який відправляється з інтерфейсу зовні. Список доступу ви можете застосувати або на вхідний трафік, тоді небажані пакети не будуть навіть потрапляти на маршрутизатор і відповідно, далі в мережу, або на вихідний, тоді пакети приходять на маршрутизатор, обробляються ним, доходять до цільового інтерфейсу і тільки на ньому обробляються. Як правило, списки застосовують на вхідний трафік (in).

Перевіряємо зв'язок ПК з сервером (Рис. 6.5 та 6.6).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Reply from 10.0.0.100: bytes=32 time=2ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

Рис. 6.5. Для PC1 сервер доступний.

```
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 6.6. Для PC2 сервер недоступний.

Якщо подивитись ACL, можна побачити такий результат (Рис. 6.7).

```
Router#sh access-list
Standard IP access list 1
  10 permit host 192.168.0.12 (4 match(es))
```

Рис. 6.7. Вузол 192.168.0.12 дозволено.

Примітка: Тепер, припустимо, потрібно додати новий вузол, наприклад, PC2 з адресою 192.168.0.13 в розділ "дозволених". Пишемо команду **Router (config)#access-list 1 permit host 192.168.0.13**. Тепер адреса 192.168.0.12 і 192.168.0.13 можуть спілкуватися з сервером, а 192.168.0.11 – ні. А для скасовувати будь-якого правила – повторюємо його з приставкою "no". Тоді це правило виключається з конфігурації. Наприклад, якщо виконати команду

Router (config-if)#no ip access-group 1 in, то ACL буде відмінено і знову всі ПК можуть пінгувати сервер.

Стандартні права не так гнучкі, як хотілося б. На відміну від стандартних списків, розширені списки фільтрують трафік більш "тонко". При створенні розширених списків в правилах доступу можна включати фільтрацію трафіку по протоколах і портам. Для вказівки портів в правилі доступу вказуються такі позначення:

lt n - всі номери портів, менші n

gt n - всі номери портів, більші n

eq n - порт n

neq n - всі порти, крім n

range n m - всі порти від n до m включно

Висновок до практичного завдання: Було створено та налаштовано прості списки доступу (ACL). В результаті виконання завдання сервер був доступний для PC1, але не для PC2. Після відміни ACL сервер став доступним для всіх ПК.

Практичне завдання 6-2. Розширені списки доступу ACL.

Створив мережу з 3 ПК, 2 комутаторів, маршрутизатора та сервера (Рис. 6.7).

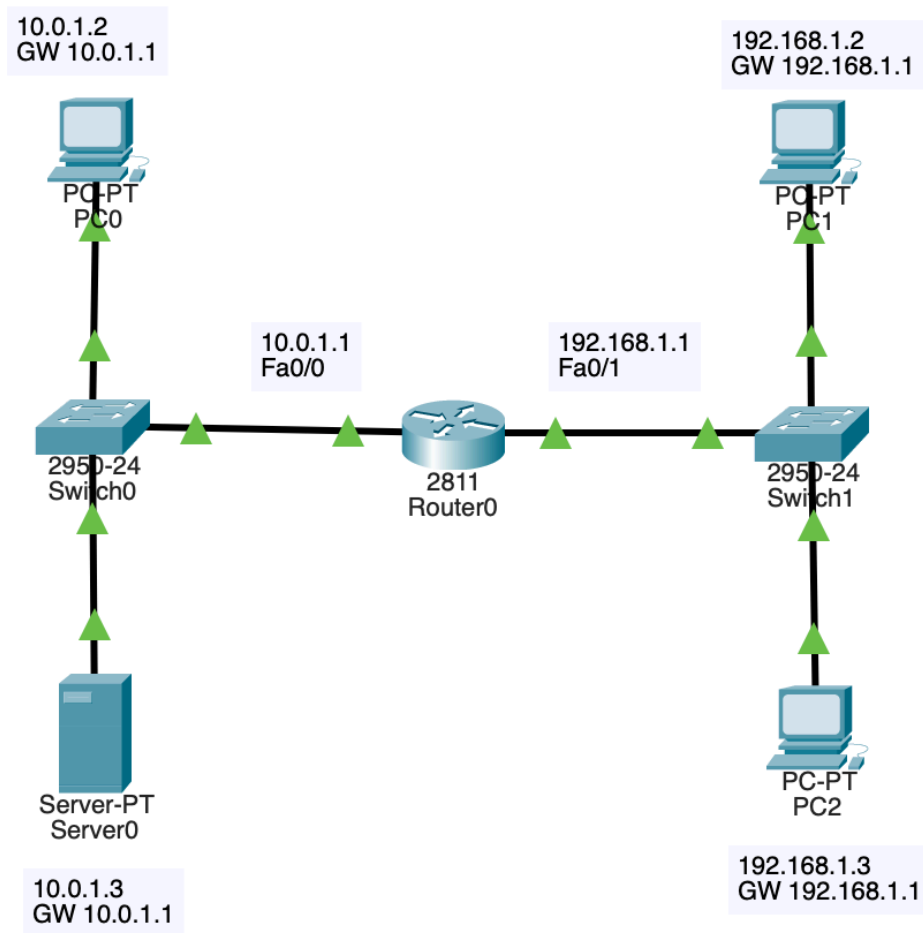


Рис. 6.7. Схема мережі для завдання.

Потрібно дозволити доступ до FTP-сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

Спочатку на сервері FTP сервіс піднято за замовчуванням зі значеннями ім'я користувача **cisco**, пароль **cisco**. Переконаємося, що вузол S0 доступний і FTP працює, для цього заходимо на PC1 і зв'язуємося з сервером. Виконуємо будь-які команди, наприклад, DIR - читання директорії (Рис. 6.8).

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.0.1.3
Trying to connect...10.0.1.3
Connected to 10.0.1.3
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.0.1.3:
0   : asa842-k8.bin                    5571584
1   : asa923-k8.bin                    30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3   : c1841-ipbase-mz.123-14.T7.bin    13832032
4   : c1841-ipbasek9-mz.124-12.bin     16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7   : c2600-i-mz.122-28.bin            5571584
8   : c2600-ipbasek9-mz.124-8.bin      13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11  : c2800nm-ipbase-mz.123-14.T7.bin   5571584
12  : c2800nm-ipbasek9-mz.124-8.bin     15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14  : c2950-i6q4l2-mz.121-22.EA4.bin   3058048
15  : c2950-i6q4l2-mz.121-22.EA8.bin   3117390
16  : c2960-lanbase-mz.122-25.FX.bin    4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin  4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin  4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25  : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26  : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27  : ir800-universalk9-mz.SPA.155-3.M 61750062
28  : ir800-universalk9-mz.SPA.156-3.M 63753767
29  : ir800_yocto-1.7.2.tar            2877440
30  : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31  : pt1000-i-mz.122-28.bin            5571584
32  : pt3000-i6q4l2-mz.121-22.EA4.bin   3117390
ftp>

```

Рис. 6.8. FPT доступный.

Тепер створимо список правил з номером 101 в якому вкажемо 2 дозволяючих і по 2 забороняючих правила для портів сервера 21 і 20 (Ці порти служать для FTP - передачі команд і даних)

```
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#|
```

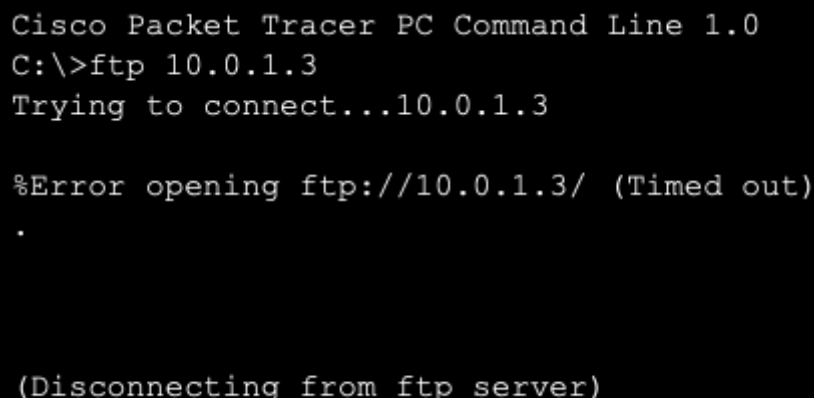
Рис. 6.9. Складаємо розширені списки доступу.

Застосовуємо наш список з номером 101 на вхід (in) Fa0/1 тому, що трафік входить на цей порт роутера з боку мережі 192.168.1.0.

```
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#
```

Рис. 6.10. Застосовуємо правило з номером 101 до порту 0/1 роутера.

Перевіряємо зв'язок сервера з ПК (Рис. 6.11, 6.12).

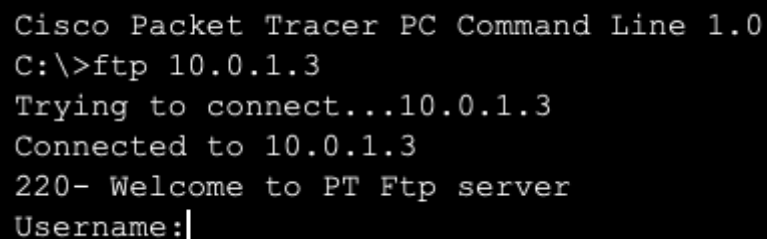


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.0.1.3
Trying to connect...10.0.1.3

%Error opening ftp://10.0.1.3/ (Timed out)
.

(Disconnecting from ftp server)
```

Рис. 6.11. Для PC2 сервер не доступний.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.0.1.3
Trying to connect...10.0.1.3
Connected to 10.0.1.3
220- Welcome to PT Ftp server
Username:|
```

Рис. 6.12. Для PC1 сервер доступний.

Висновок: створено та налаштовано розширені списки доступу ACL. Завдяки ним ПК1 було дозволено спілкуватися з сервером по 20 та 21 портам, а

для ПК - ні. В результаті для ПК1 FTP сервер був доступним, а для ПК2 - недоступним.

Висновок всієї роботи: добре засвоєна робота зі списками доступу (access-lists). Створено та протестовано декілька мереж, в тому числі і з розширеними списками доступу ACL.