

## Комп'ютерний практикум № 7.

### Списки доступу ACL

Списки доступу (access-lists) використовуються в цілому ряді випадків і є механізмом задання 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 (у тому порядку, у якому вони були введені). Пакет, який не відповідає жодному з введених критеріїв буде відкинутий. Для кожного протоколу на інтерфейс може бути призначений тільки один список доступу. Як приклад нижче наведена таблиця списку управління доступом за замовчуванням:

#### № правила Підмережа Кінцева точка Дозволити чи заборонити

100	0.0.0.0/0	3389	Дозволити
-----	-----------	------	-----------

**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 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 з підмережі 10.0.1.0/24.

**Хід роботи**  
**Завдання №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 заборон або дозволів.

На рис. 7.1 показані дві підмережі: 192.168.0.0 і 10.0.0.0.

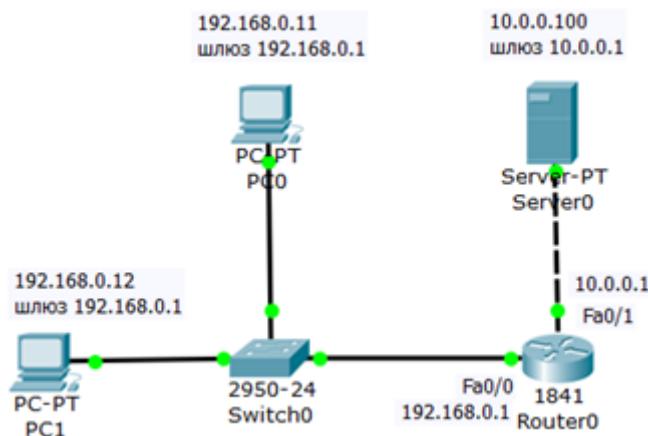


Рис. 7.1. Схема мережі

**Постановка задачі**

Потрібно дозволити доступ на сервер PC1 з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 - заборонити (рис. 7.2).

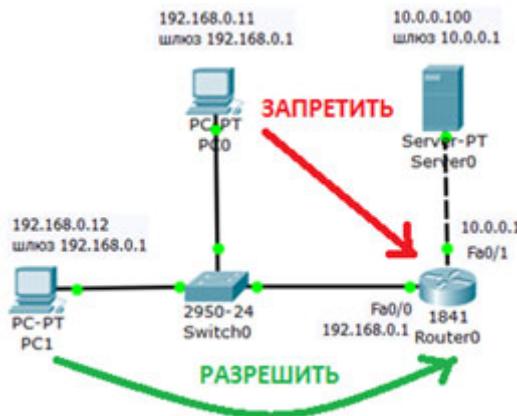


Рис. 7.2. Постановка задачі

Зберемо дану схему і налаштуємо її. Налаштування PC0 і PC1 виконайте самостійно.

### Налаштування R0

Інтерфейс 0/0 маршрутизатора 1841 налаштуємо на адресу 192.168.0.1 і включимо наступними командами:

```
Router>en
```

```
Router#conf t
```

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

```
Router (config-if)#ip addr 192.168.0.1 255.255.255.0
```

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

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

Другий інтерфейс маршрутизатора (порт 0/1) налаштуємо на адресу 10.0.0.1 і так само включимо:

```
Router (config)#intfa0/1
```

```
Router (config-if)#ip addr 10.0.0.1 255.255.255.0
```

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

### Налаштування серверу

Налаштування серверу приведені на рис.7.3 .

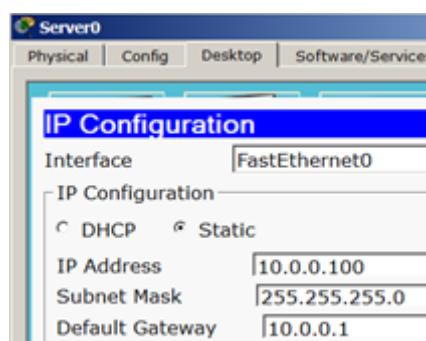


Рис. 7.3. Конфігурування S0

### Діагностика мережі

Перевіряємо зв'язок ПК з різних мереж (рис. 7.4).

```

Packet Tracer PC Command Line 1.0
PC>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=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127

```

**Рис. 7.4.** ПК з різних мереж можуть спілкуватися

### Починаємо вирішення задачі

Правило заборони і 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 "Усе, що не дозволено, то заборонено". Тому немає необхідності щось забороняти (**deny**) - вказуємо що дозволено, а "іншим - заборонити" мається на увазі автоматично. За умовами завдання потрібно на R0 пропустити пакети з вузла 192.168.0.12 на сервер рис. 7.5).

```

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit host 192.168.0.12
Router(config)#exit

```

**Рис. 7.5.** Створюємо на R0 ACL, що дозволяєм доступ

Застосовується дане правило на інтерфейс в залежності від напрямку (PC1 розташований з боку порту Fa0/0) - рис. 6.6. Ця установка означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0/0 на вхідному (in) від PC1 напрямку.

```

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

```

**Рис. 7.6.** Застосовуємо правило до порту Fa0/0

**Примітка:** вхідний трафік (in) - цей той, що приходить на інтерфейс із зовні. Вихідний (out) - той, який відправляється з інтерфейсу зовні. Список доступу можна 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. 7.7 і рис.7.8).

```

PC>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127

```

**Рис. 7.7.** Для PC1 сервер доступний

```

PC>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
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),

```

**Рис. 7.8.** Для PC0 сервер не доступний

Давайте переглянемо ACL (рис. 7.9).

```

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

```

**Рис. 7.9.** Вузол 192.168.0.12 дозволено

Робоча мережа даного прикладу представлена

**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 адреси 192.168.0.12 і 192.168.0.13 можуть спілкуватися з сервером, у 192.168.0.11 - немає. А для скасування 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 скасований і знову все ПК можуть пінгувати сервер.

### Розширені списки доступу ACL

Стандартні права не так гнучкі, як хотілося б. На відміну від стандартних списків, розширені списки фільтрують трафік більш "тонко". При створенні розширеніх списків в правилах доступу можна включати фільтрацію трафіку по протоколах і портах. Для зазначення портів у правилі доступу вказуються такі позначення (табл. 7.1):

Таблиця 7.1. Позначення портів у ACL

Позначення	Дія
lt n	Всі номери портів, менші n.
gt n	Всі номери портів, більші n.
eq n	Порт n
neq n	Все порти, за виключенням n.
range n m	Все порти від n до m включно.

### Завдання №2

#### Розширені списки доступу ACL

Зберіть схему мережі, показану на рис. 7.10.

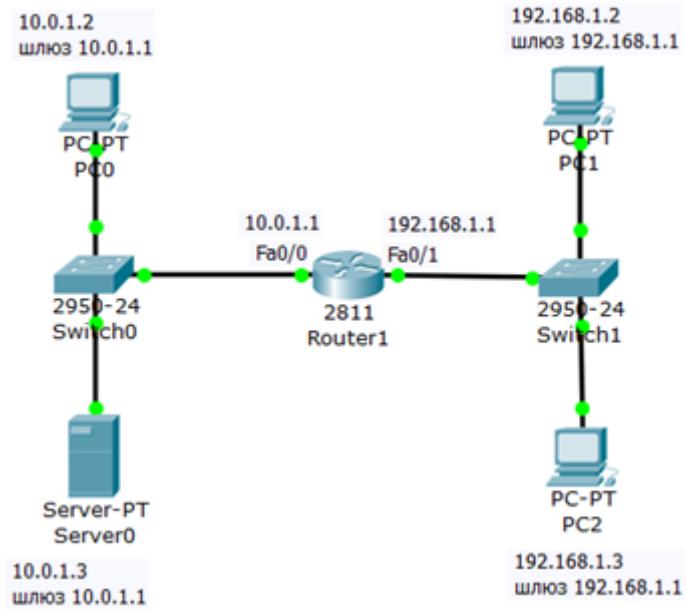


Рис. 7.10. Схема мережі

Задача: дозволити доступ до FTP сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

### Створюємо розширені списки доступу і забороняємо FTP трафік

Постановка задачі графічно зображена на рис.7.11.

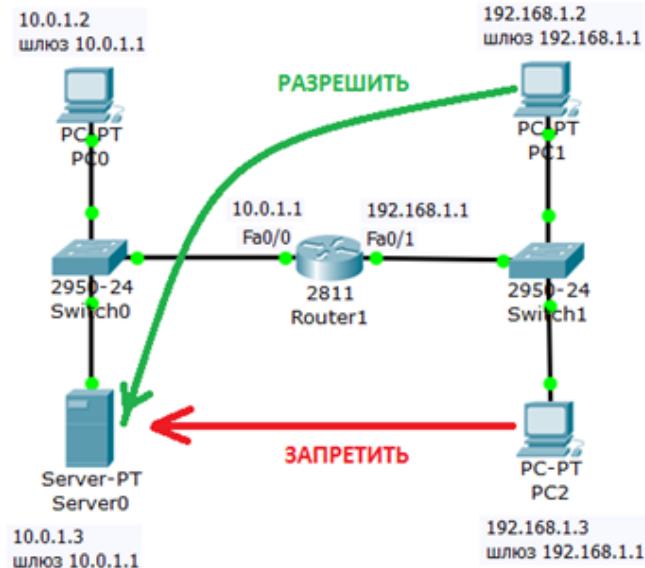


Рис. 7.11. Стрілками показана мета нашої роботи

Спочатку на сервері 10.0.1.3 FTP сервіс піднятий 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 (рис. 7.12). Виконуємо будь-які команди, наприклад, DIR - читання директорії.

The image shows two windows from the Cisco Packet Tracer software. The top window is titled 'Command Prompt' and displays the following text:

```

Packet Tracer PC Command Line 1.0
PC>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>

```

The bottom window is also titled 'Command Prompt' and displays the following text:

```

Password:
230- Logged in
(passive mode On)
ftp>dir
Listing /ftp directory from 10.0.1.3:
0 : c1841-adviservicesk9-mz.124-15.T1.bin      33591768
1 : c1841-ipbase-mz.123-14.T7.bin              13832032
2 : c1841-ipbasek9-mz.124-12.bin               16599160
3 : c2600-adviservicesk9-mz.124-15.T1.bin      33591768
4 : c2600-i-mz.122-28.bin                      5571584
5 : c2600-ipbasek9-mz.124-8.bin                13169700
6 : c2800nm-adviservicesk9-mz.124-15.T1.bin    50938004
7 : c2800nm-adviservicesk9-mz.151-4.M4.bin     33591768
8 : c2800nm-ipbase-mz.123-14.T7.bin            5571584
9 : c2800nm-ipbasek9-mz.124-8.bin              15522644
10 : c2950-i6q412-mz.121-22.EA4.bin            3058048
11 : c2950-i6q412-mz.121-22.EA8.bin            3117390
12 : c2960-lanbase-mz.122-25.FX.bin            4414921
13 : c2960-lanbase-mz.122-25.SEE1.bin          4670455
14 : c3560-adviservicesk9-mz.122-37.SE1.bin    8662192
15 : pt1000-i-mz.122-28.bin                   5571584
16 : pt3000-i6q412-mz.121-22.EA4.bin          3117390
ftp>quit
Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>
```

**Рис. 7.12.** FTP сервер доступний

**Примітка:** при наборі пароля на екрані нічого не відображається.

Тепер створимо список правил з номером 101, у якому вказуємо 2 дозволених і 2 заборонених правила для портів сервера 21 і 20 (ці порти служать для FTP - передачі команд і даних) – рис. 7.13.

```

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 21
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. 7.13.** Складаємо розширені списки доступу

*Порада:* набирайте команди акуратно і уважно: навіть один зайвий пробіл може привести до помилки при виконанні команди.

Застосовуємо список з номером 101 на вхід (in) Fa0/1 тому, що трафік входить на цей порт роутера з боку мережі 192.168.1.0 (рис. 7.14).

```

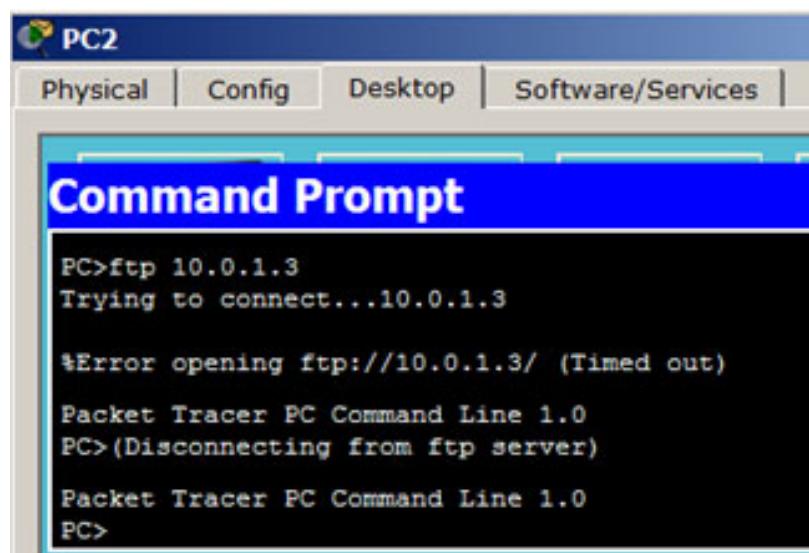
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#

```

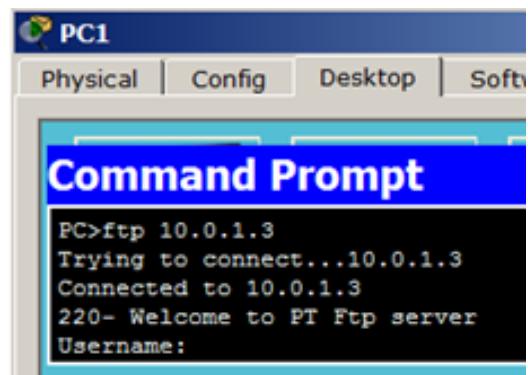
**Рис. 7.14.** Застосовуємо правило з номером 101 до порту 0/1 роутера

Перевіряємо зв'язок сервера з PC2 (рис. 7.15).



**Рис. 7.15.** Для PC2 FTP сервер не доступний

Перевіряємо зв'язок сервера з PC1(рис. 7.16).



**Рис. 7.16.** Для PC1 FTP сервер доступний  
Робоча мережа даного прикладу представлена