Лабораторна робота №5. Застосування списків доступу на обладнанні Cisco.

Метою даної лабораторної роботи є налагодження стандартних списків доступу на маршрутизаторах Cisco і знайомство з розширеними списками доступу.

Завдання на лабораторну роботу

Отримати наступні практичні навички:
• Зіставлення інтерфейсу маршрутизатора деякої групи доступу
(Ip access-group);
• Створення списків доступу дозволяють або перешкоджають передачі даних між вузлами мережі (access-list).

Хід роботи:

1. Зібрати схему мережі з наступних елементів:
• Комутатори S1, S2, S3 (3 шт.);
• Маршрутизатори R1, R2, R3 (3 шт.);
• Персональні комп'ютери PC1, PC2, PC3 (3 шт.);
• Схема мережі представлена на рис.5.

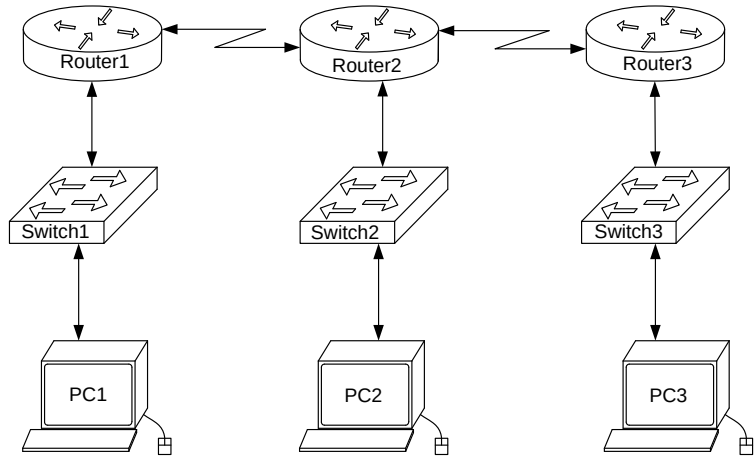

Рис.5. Схема мережі

2. Задати для всіх вузлів мережі IP адреси.

3. Налаштувати динамічну маршрутизацію між усіма вузлами мережі.

4. Виявити можливість пересилки даних по протоколу IP між будь-якими об'єктами мереж.

5. Розробити та застосувати на маршрутизаторах списки доступу.
Заборонити маршрутизаторам R0 і R2 обмінюватися ICMP-пакетами по послідовному мережному інтерфейсу.
Для маршрутизатора R3 створимо і застосуємо стандартний список доступу.

Router(config)#ip access-list standard FROM-R1

де *FROM-R1* – назва списку доступу, який створений для унеможливлення отримання ICMP-пакету від маршрутизатору R1.

Далі, пострічковими командами наповнюємо список доступу правилами. Правила виконуються по одному, зверху вниз. Тому більш деталізовані правила пишуться зверху списку, а більш загальні – знизу.

Router(config-std-nacl)#deny 10.10.12.0 0.0.0.255
Router(config-std-nacl)#permit any

де *deny* і *permit* – заборонити і дозволити відповідно.
Перше правило блокує всі IP-пакети в яких в джерелом виступає хост з мережі 10.10.12.0 255.255.255.0 (в правилі вказується дзеркальна або “wildcard”- маска 0.0.0.255). Друге правило відміняє неявне правило за замовчуванням, яке автоматично створюється останнім і звучить як *deny any (заборонити будь-який)*. Тому передостаннім (другим) правилом, в даному випадку, виступає дозвільне *permit any (дозволити будь-який),* що дозволяє проходженню через інтерфейс маршрутизатора всіх IP-пакетів окрім тих, які вказані в першому правилі.

Наступна дія – застосувати список доступу до відповідного інтерфейсу.

Router(config)#int se2/0
Router(config-if)#ip access-group FROM-R1 in

де *se2/0* –інтерфейс до якого застосовують список доступу, *ip access-group FROM-R1* –команда для застосування відповідного списку доступу до інтерфейсу, *in* –вказівник який показує, що правила застосовуються лишу для вхідного трафіку (можливі варіанти: in – для вхідного, out – для вихідного).

6. Для маршрутизатора R1 створимо і застосуємо розширений список доступу. Розширені списки доступу мають значно більше можливостей ніж стандартні і дозволяють блокувати не тільки IP-пакети, а й окремі протоколи і порти.

Router(config)#ip access-list extended FROM-R3

де *FROM-R3* – назва списку доступу, який створений для унеможливлення отримання ICMP-пакету від маршрутизатору R3.

Далі, пострічковими командами наповнюємо список доступу правилами.

Router(config-std-nacl)#deny icmp host 10.10.23.2 host 10.10.12.1
Router(config-std-nacl)#permit ip any any

де *deny* і *permit* – заборонити і дозволити відповідно.
Перше правило блокує всі ICMP-пакети в яких в джерелом виступає хост з мережі 10.10.23.2 а пунктом призначення хост 10..10.12.1. Друге правило відміняє неявне правило за замовчуванням, яке автоматично створюється останнім і звучить як *deny any*. Тому передостаннім (другим) правилом, в даному випадку, виступає дозвільне *permit ip any any*, що дозволяє проходженню через інтерфейс маршрутизатора всіх IP-пакетів окрім тих, які вказані в першому правилі. Зверніть увагу, що на відміну від попереднього списку доступу в розширеному передостаннє правило містить вказівку на протокол *IP* і два слова *any* (дозволити будь-які ip-пакети від будь-якого джерела до будь-якого пункту призначення).

Наступна дія – застосувати список доступу до відповідного інтерфейсу.

Router(config)#int se2/0
Router(config-if)#ip access-group FROM-R3 in

7. Заборонити комп'ютерам PC1 і PC3 обмінюватися ICMP-пакетами по інтерфейсу Ethernet.

По аналогії з попереднім пунктом застосуємо розширені списки доступу для маршрутизаторів R1 I R2.

Для R1:
Router(config)#ip access-list extended NO-PING-PC1
Router(config-std-nacl)#deny icmp host 192.168.10.10 host 192.168.20.10
Router(config-std-nacl)#permit ip any any

Router(config)#int fa0/0
Router(config-if)#ip access-group NO-PING-PC1 in

Для R2:
Router(config)#ip access-list extended NO-PING-PC2
Router(config-std-nacl)#deny icmp host 192.168.20.10 host 192.168.10.10
Router(config-std-nacl)#permit ip any any
Router(config)#int fa0/0
Router(config-if)#ip access-group NO-PING-PC2 in

8. Переключившись в «Режим симуляції» розглянути і пояснити процес обміну даними по протоколу RIP (в разі динамічної маршрутизації) між пристроями (виконавши команду Ping з одного комп'ютера на інший). Детальне пояснення включити в звіт.

Структура звіту по роботі:
• Титульна сторінка;
• Завдання;
• Топологічна схема мережі:
Вказати на схемі найменування вузлів мережі, адреси та типи мережевих інтерфейсів.
• Хід роботи:
Даний розділ складається з послідовного опису значущих виконуваних кроків (із зазначенням їх суті) і копій екранів (повинна бути видна набрана команда і реакція системи, якщо вона є).
• Зміни обладнання;
Привести значущі фрагменти конфігураційних файлів (startup-config) для комутаторів і маршрутизаторів Cisco, пояснити значення команд.
• Висновки.