МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
"Проектування комп'ютерних мереж"
для бакалаврів спеціальності 123 "Комп'ютерна інженерія",
усіх форм навчання
Розширені списки контролю доступу

2020

Методичні вказівки до виконання лабораторних робіт з дисципліни “Проектування комп’ютерних мереж” для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Розширені списки контролю доступу / Укл. Г.Г. Киричек, – Запоріжжя: НУ «Запорізька політехніка», 2020. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент: М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 1 від 21.08.2020

Затверджено
на засіданні НМК КНТ
Протокол № 1 від 28.08.2020

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА.
Іменовані та розширені списки ACL

Мета роботи: використання іменованих та розширених списків контролю доступу (ACL) для безпечної маршрутизації трафіку в комп'ютерних мережах.

1.1 Особливості іменованих та розширених ACL

Розширений ACL дозволяє фільтрувати трафік використовуючи велику кількість параметрів: адреса відправника; адреса одержувача; TCP/UDP порт відправника; TCP/UDP порт одержувача; за протоколом, дані якого в середині ip-пакету (фільтр по параметрах); типу трафіку для даного протоколу (icmp - відфільтрувати тільки icmp-reply) та ін.

Можливості розширених ACL вище за стандартні та можуть розширюватися додатковими технологіями:

– dynamic ACL – спочатку деякі рядки не працюють, але коли адміністратор підключається до маршрутизатора по telnet, ці рядки включаються, тобто адміністратор може залишити для себе «дірку» в безпеці при налагодженні параметрів або при вході в мережу;

– reflexive ACL – дзеркальні списки контролю доступу, дозволяють запам'ятовувати, хто звертався із зовнішньої мережі (з яких адрес і портів, на які адреси і порти) і автоматично формувати дзеркальний ACL, який пропускатиме зворотний трафік ззовні всередину тільки, якщо з мережі є звернення до даного ресурсу;

– timeBased ACL – деякі рядки спрацьовують тільки в конкретний час. Наприклад, легко налаштувати доступ в інтернет з офісу тільки в робочі години.

Загальна форма команди для формування рядка списку розширеного доступу:

access-list access-list-number {permit | deny} protocol source source-wildcard [operator source-port] destination destination-wildcard [operator destination-port] [precedence precedence-number] [tos tos] [established] [log | log-input], де access-list-number -100-199 | 2000-2699, protocol - ip, icmp, tcp, gre, udp, igrp, eigrp, igmp, ipinip, nos і ospf.

Для порту source-port або destination-port можна використовувати номер порту або його позначення bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois і www. Operator це eq (так само), neq (не дорівнює), gt (більше ніж), lt (менше ніж), range (вказується два порти для визначення діапазону).

Усі ACL, як стандартні так і розширені, можна задавати іменованим або нумерованим способом. Перший дозволяє редагувати ACL, а при використанні другого, список контролю доступу можна видалити тільки цілком і створити заново, або дописати рядок в кінець.

Примітка. Ім'я іменованого списку відчутно до регістру. Прив'язка іменованих ACL до інтерфейсу здійснюється командою:

Router (config) # interface type [slot_№] port_№

Router (config-if) # ip access-group ACL_name in | out

Якщо ACL іменований, то у нього є ім'я, яке ми і вкажемо на інтерфейсі. Для виконання налаштування заходимо на інтерфейс і пишемо команду ip access-group, наприклад, так:

R1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**interface FastEthernet0/0**

R1(config-if)#**ip access-group NAME in**

У цьому прикладі ми застосували ACL з ім'ям NAME на інтерфейсе Fa0/0 на весь вхідний трафік (in), якби ми вказали out - фільтрувався б вихідний трафік.

Взагалі, на один інтерфейс можна налаштувати декілька ACL, але за умови, якщо у них відрізняється напрямок або протокол (IPX ACL, AppleTalk ACL).

Розглянемо приклад використання ACL: є топологія з п’яти мереж: комп’ютер, який підключено до маршрутизатора R1, далі R2, R3 та R4 до якого підключено ноутбук. Треба заборонити доступ з комп'ютера в мережу ноутбука двома способами по черзі (спочатку за допомогою стандартного, потім за допомогою розширеного ACL). Стандартний ACL доводиться розміщувати максимально близько до одержувача трафіку (за допомогою стандартного ACL ми можемо визначити адресу відправника але можемо не знати маршрут трафіку). Тому, якщо ми забороняємо доступ з IP адреси комп'ютера на вхід Fa0/0 маршрутизатора R1, то ми зможемо заборонити або дозволити тільки весь трафік з комп'ютера відразу, тобто в усі мережі, а не тільки в

мережу ноутбука. Тому, доведеться ставити ACL максимально близько до одержувача трафіку, а саме, на R4 на вихід з інтерфейсу Fa0/1. Якщо пакет дійшов на R4 і хоче вийти через Fa0/1, значить він точно слідує в мережу ноутбука. За допомогою стандартного ACL можна заборонити трафік, що йде від комп'ютера.

Наведемо приклади команд access-list розширеного списку контролю доступу та пояснення до них.

access-list 101 deny ip any host 10.1.1.1 – будь-який ip-пакет, будь-яка ip-адреса відправника, з ip-адресою отримувача 10.1.1.1.

access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23 – пакети із заголовком TCP, з будь-якою ip-адресою відправника, з номером порту відправника, який більше (gt) 1023, з ip-адресою отримувача, яка точно співпадає з 10.1.1.1 та номером порту отримувача, що дорівнює (eq) 23.

Якщо використовується розширений ACL, то його можна поставити де завгодно, але краще ставити максимально близько до відправника трафіку, тобто на R1 на вхід Fa0/0. Тому, якщо ми бачимо в розширеному ACL адресу одержувача і якщо пакет йде з комп'ютера в мережу ноутбука, то видалимо його на вході в Fa0/0, щоб далі не навантажувати мережу передачею цього пакета.

Таким чином є правило, яке все спрощує: «Стандартний ACL ставиться максимально близько до одержувача трафіку, розширений - максимально близько до джерела трафіку». Правило не завжди ефективно але для початку воно непогано працює. Тому рекомендуємо вибирати налаштування спочатку за цим правилом, а потім визначати маршрут трафіку і як можна поліпшити розміщення ACL.

1.2 Розширені списки доступу

Розглянемо використання розширених списків контролю доступу у розподілених або корпоративних мережах. Побудуємо та налаштуємо мережу із заданою топологією (рис.1.1).

З панелі приладів в робочу область перенесіть 3 маршрутизатора 1841 (для зручності можна їх перейменувати відповідно R1, R2, R3), 6 комутаторів 2950-24, 2 сервери, 2 ноутбуки і 4 комп'ютери. Для зручності скоротить назви комутаторів до Sw, а ноутбуків до Lap.

Виконайте налаштування мережі. Для цього використовуйте конфігураційні параметри, що наведені у таблиці 1.1.

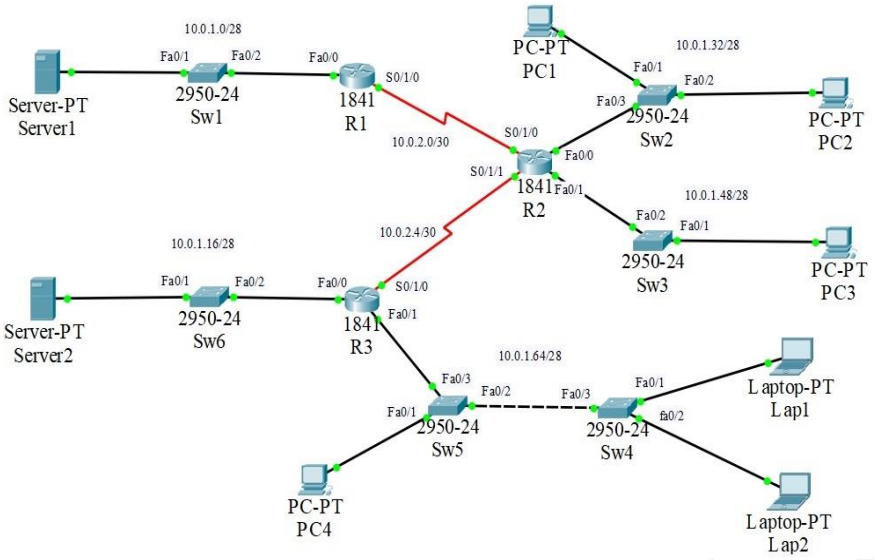

Рисунок 1.1 – Модель мережі

Таблиця 1.1 – Налаштування

Пристрій	Інтер-фейс	IP-адреса	Маска	Default Gateway
R1	Fa0/0	10.0.1.1	255.255.255.240	***
	S0/1/0	10.0.2.1	255.255.255.252	***
R2	Fa0/0	10.0.1.33	255.255.255.240	***
	Fa0/1	10.0.1.49	255.255.255.240	***
	S0/1/0	10.0.2.2	255.255.255.252	***
	S0/1/1	10.0.2.5	255.255.255.252	***
R3	Fa0/0	10.0.1.17	255.255.255.240	***
	Fa0/1	10.0.1.65	255.255.255.240	***
	S0/1/0	10.0.2.6	255.255.255.252	***
Server1	Fa0	10.0.1.2	255.255.255.240	10.0.1.1 /28
Server2	Fa0	10.0.1.18	255.255.255.240	10.0.1.16 /28
PC1	Fa0	10.0.1.34	255.255.255.240	10.0.1.33 /28
PC2	Fa0	10.0.1.35	255.255.255.240	10.0.1.33 /28
PC3	Fa0	10.0.1.50	255.255.255.240	10.0.1.49 /28
PC4	Fa0	10.0.1.66	255.255.255.240	10.0.1.65 /28
Lap1	Fa0	10.0.1.67	255.255.255.240	10.0.1.65 /28
Lap2	Fa0	10.0.1.68	255.255.255.240	10.0.1.65 /28

Здійснимо конфігурацію RIP маршрутизації на всіх маршрутизаторах, за допомогою налаштування у вкладці CLI або Config RIP.

Примітка. Маршрутизацію можна налаштувати будь-яким способом, який дя Вас є зручним.

Для R1
Router1(config)#**router rip**
Router1(config- router)#**version 2**
Router1(config- router)#**network 10.0.0.0**
Для R2
Router2(config)#**router rip**
Router2(config- router)#**version 2**
Router2(config- router)#**network 10.0.0.0**
для R3
Router3(config)#**router rip**
Router3(config- router)#**version 2**
Router3(config- router)#**network 10.0.0.0**

Перевіримо дієздатність мережі за допомогою команди ping. Інтерфейси всіх пристроїв повинні пінгуватися з усіх пристроїв.

1.2.1 Список доступу мережа-мережа

Створимо 2 списки доступу, які заборонять трафік:

– **перший** - від локальної мережі комп'ютерів PC1 і PC2 – адреса мережі 10.0.1.32/28, в локальну мережу ноутбуків Lap1 і Lap2 – адреса мережі 10.0.1.64/28. Так як трафік приходить від R2, а список розширений, то слід помістити список доступу на інтерфейс Fa0/0 R2 для вхідного трафіку.

Router2(conf)#**access-list 101 deny ip 10.0.1.32 0.0.0.15 10.0.1.64 0.0.0.15**

Router2(conf)#**access-list 101 permit ip any any**

Перша команда безпосередньо вирішує поставлене завдання, а друга дозволяє весь інший трафік, перевіримо створення списку 101.

Router2 # **show access-list**

Отримали наступі строки.

Extended IP access list 101
10 deny ip 10.0.1.32 0.0.0.15 10.0.1.64 0.0.0.15
20 permit ip any any

Застосуємо список доступу до інтерфейсу.

Router2 (conf) #**interface Fa0/0**

Router2 (conf-if) #**ip access-group 101 in**

Для тестування першого списку доступу, спробуйте пропінгувати від PC1 та PC2 – PC4, Lap1 і Lap2.

PC #**ping 10.0.1.67**

Для PC4, Lap1 і Lap2 пінги не йдуть. Список доступу працює;

– **другий** - від мережі комп'ютера PC3 – адреса 10.0.1.48/28, в мережу сервера Server1 – 10.0.1.0/28. Список слід помістити на інтерфейс Fa0/1 R2 для вхідного трафіку.

Router2(conf)#**access-list 102 deny ip 10.0.1.48 0.0.0.15 10.0.1.0 0.0.0.15**

Router2(conf)#**access-list 102 permit ip any any**

Застосуємо список доступу до інтерфейсу.

Router2 (conf) #**interface Fa0/1**

Router2 (conf-if) #**ip access-group 101 in**

Далі можна ввести команду **show access-list** і вона повинна вивести вміст обох списків доступу 101 та 102

Для тестування другого списку доступу, спробуйте пропінгувати від PC3 - Server1.

PC3 #**ping 10.0.1.2**

Для Server1 пінги не йдуть. Список доступу працює.

1.2.2 Список доступу хост-хост

Створимо на R3 список доступу, який блокує доступ до Server1 тільки з Lap1.

Router3(conf) #**access-list 103 deny ip 10.0.1.67 0.0.0.0 10.0.1.2 0.0.0.0**

Router3 (conf) # **access-list 103 permit ip any any**

перевіримо створення

Router3 # **show access-list**

Extended IP access list 103

10 deny ip host 10.0.1.67 host 10.0.1.2

20 permit ip any any

Застосуємо список доступу до Fa0/1 інтерфейсу R3

Router3 (conf) #**interface FastEthernet0/1**

Router3 (conf-if) #**ip access-group 103 in**

Перевірте, що ви не можете пінгувати Server1 з Lap1.

Lap1 # **ping 10.0.1.2**

Перевірте, що ви можете пінгувати Server1 з Lap2 та PC4.

Lap2 # **ping 10.0.1.2** PC4# **ping 10.0.1.2**

1.2.3 Список доступу мережа-хост

Видалить попередні списки доступу з інтерфейсів R2 і R3.

Router2 (conf) #**interface Fa0/0**

Router2 (conf-if) #**no ip access-group 101 in**

Router2 (conf) #**interface Fa0/1**

Router2 (conf-if) #**no ip access-group 102 in**

Router3 (conf) #**interface Fa0/1**

Router3 (conf-if) #**no ip access-group 103 in**

Створить розширений список доступу, який блокує весь трафік до PC1 з локальної мережі комп'ютерів PC4, Lap1 і Lap2. Так як ми блокуємо весь трафік, то будемо використовувати IP протокол та список контролю доступу на R3.

Router3 (conf) #**access-list 100 deny ip 10.0.1.64 0.0.0.15 10.0.1.34 0.0.0.0**

Router3 (conf) # **access-list 100 permit ip any any**

Застосуємо список до вихідного трафіку на інтерфейсі Serial0/1/0 маршрутизатора R3.

Router3 (conf) #**interface Serial0/1/0**

Router3 (conf-if) #**ip access-group 100 out**

Router3#**show access-list**

Extended IP access list 100

10 deny ip 10.0.1.64 0.0.0.15 host 10.0.1.34

20 permit ip any any

Для перевірки списку спробуйте пропінгувати PC1 (10.0.1.34) з PC4, Lap1 і Lap2. Пінги не пройдуть. У всіх інших з'єднаннях пристрої пінгуються. Список працює.

1.3 Іменовані ACL

Важлива перевага іменованих списків в тому, що вони дозволяють видаляти з них окремі строки, шляхом додавання потрібних команд. В завданні розглянемо переваги застосування іменованих списків з метою подальшого їх застосування як у стандартних так і у розширених ACL.

При налаштуванні моделі мережі використовуємо топологію і конфігурацію з рисунку 1.2.

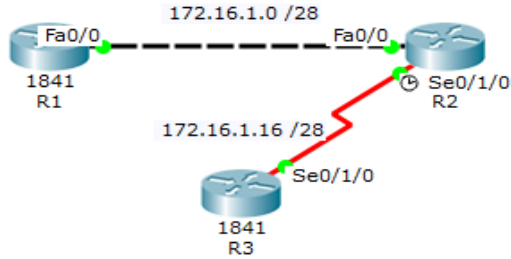

Рисунок 1.2 – Модель мережі

До R2 та R3 маршрутизатора (модель 1841) додаємо додаткові плати з Serial портами (WIC-2T).

Примітка. Обов'язково виключаємо маршрутизатори при встановленні нових плат.

Далі призначимо адреси інтерфейсів згідно таблиці 1.2. При налаштуванні Serial портів не забувайте задати значення синхронізації (наприклад 64000).

Таблиця 1.2 – Налаштування

	R1	R2	R3
Ethernet порти	172.16.1.2 /28	172.16.1.1 /28	
Serial порти		172.16.1.17 /28	172.16.1.18 /28

Здійснимо конфігурацію RIP маршрутизації (або залишимо вже існуючу) на всіх маршрутизаторах, за допомогою налаштування у вкладці CLI або Config RIP.

Для Router1

Router1(config)#**router rip**

Router1(config- router)#**version 2**

Router1(config- router)#**network 172.16.0.0**

Для Router2

Router2(config)#**router rip**

Router2(config- router)#**version 2**

Router2(config- router)#**network 172.16.0.0**

Для Router3

Router3(config)#**router rip**

Router3(config- router)#**version 2**

Router3(config- router)#**network 172.16.0.0**

Перевіримо дієздатність мережі за допомогою команди ping (можливість пінгувати інтерфейс Ethernet0/0 (172.16.1.2) R1 з R3).

Router3#**ping 172.16.1.2**

Далі налаштуємо списки контролю доступу.

Поставимо задачу заборонити по всій мережі лише пінг від R3 на R1. Список доступу розширений тому буде розташований ближче до джерела (для скорочення трафіку).

В цьому прикладі розташуємо іменований список з ім'ям deny_ping на R1.

Router1 (config) #**ip access-list extended deny_ping**

Router1 (config-ext-nacl) #**deny icmp 172.16.1.18 0.0.0.0 172.16.1.2 0.0.0.0**

Router1 (config- ext-nacl) #**permit ip any any**

Перша команда вказує, що ми створюємо іменований розширений список доступу з ім'ям deny_ping. Друга команда вказує на заборону ICMP трафіку з адресою джерела **172.16.1.18** і адресою приймача **172.16.1.2**. Третя команда дозволяє решту IP трафіку. Перевіримо створення списку.

Router1 #**show access-list**

Extended IP access list deny_ping

10 deny icmp host **172.16.1.18** host **172.16.1.2**

20 permit ip any any

Все правильно, ми бачимо в першому рядку просто іншу форму подання команди deny icmp **172.16.1.18** 0.0.0.0 **172.16.1.2** 0.0.0.0. Застосуємо список для вхідного трафіку інтерфейсу Fa0/0 на R1.

Router1 (conf) #**interface Fa0/0**

Router1 (conf-if) #**ip access-group deny_ping in**

Приєднаємося до R3 і пропінгуем R1

Router3 # **ping 172.16.1.2**

Невдача. Приєднаємося до R2 і пропінгуем R1

Router2 # **ping 172.16.1.2**

Пінг пройшов успішно. Зробимо висновок, що список контролю доступу працює.

Видалить команду (20 permit ip any any), яка дозволяє передачу пакетів з будь-яких інших пристроїв.

Іменовані списки дозволяють видаляти окремі команди.

Router1 (config) #**ip access-list extended deny_ping**

Router1 (config- ext-nacl) #**no permit ip any any**

Router1 (config- ext-nacl) #^**z**

Перевіримо зміни у списку.

Router1 #**show access-list**

Отримали наступне.

Extended IP access list deny_ping

10 deny icmp host **172.16.1.18** host **172.16.1.2**

Тепер пінг не пройде ні з R3 ні з R2.

Використовуючи іменовані списки як стандартні так і розширені ви маєте більші можливості при редагуванні окремих команд у списку.

1.4 Використання протоколів в ACL

Розглянемо випадок коли є можливість підключення за протоколом віддаленого доступу до кожного маршрутизатора мережі тільки пристроям з мережі 172.16.1.16/28. У такому випадку на кожному маршрутизаторі можна використовувати конфігурацію, яка розглянута та наведена у цьому розділі при налаштуванні списків ACL.

При налаштуванні використовуємо топологію і конфігурацію з рисунку 1.3.

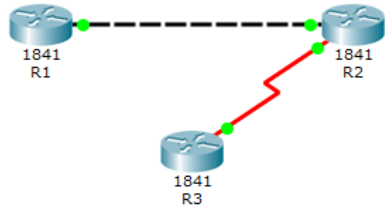

Рисунок 1.3 – Модель мережі

До R2 та R3 маршрутизатора (1841) додаємо додаткові плати з Serial портами (WIC-2T).

Примітка. Обов’язково виключаємо маршрутизатори при встановленні нових плат.

Далі призначимо адреси інтерфейсів згідно таблиці 1.3. При налаштуванні Serial портів не забувайте задати значення синхронізації (наприклад 64000).

Таблиця 1.3 – Налаштування

	R1	R2	R3
Ethernet порти	172.16.1.2 /28	172.16.1.1 /28	
Serial порти		172.16.1.17 /28	172.16.1.18 /28

Здійснимо конфігурацію RIP маршрутизації на всіх маршрутизаторах, за допомогою налаштування у вкладці CLI або Config RIP.

Для R1, R2 та R3 виконаємо налаштування RIP.

Router1(config)#**router rip**

Router1(config- router)#**version 2**

Router1(config- router)#**network 172.16.0.0**

Перевіримо дієздатність мережі за допомогою команди ping (можливість пінгувати інтерфейс Ethernet0/0 (172.16.1.2) Router1 з Router3).

Router3#**ping 172.16.1.2**

Налаштуємо конфігурацію списку контролю доступу.

Дозволимо заходити на R2 телнетом на два інтерфейси з паролем router2

Router2 (config) #**line vty 0 4**

Router2 (config-line) #**login**

Router2 (config-line) #**password router2**

В даній роботі ACL виконують два різних завдання. Перше дозволяє тільки телнет з мережі послідовного з'єднання (інтерфейс Serial0/1/0) 172.16.1.16/240 для входу на R2.

Router2 (conf) #**access-list 101 permit tcp 172.16.1.16 0.0.0.15 any eq telnet**

Друге дозволяє на маршрутизаторі R2 весь трафік з Ethernet0/0 мережі 172.16.1.0 /240.

Router2 (conf) # **access-list 102 permit ip 172.16.1.0 0.0.0.15 any**

Перевіримо установку списків.

router1#**show access-list**

В результаті отримали наступні рядки.

Extended IP access list 101
10 permit tcp 172.16.1.16 0.0.0.15 any eq telnet
Extended IP access list 102
10 permit tcp 172.16.1.0 0.0.0.15 any

Тепер застосуємо списки до інтерфейсів для вхідних пакетів

Router2(conf)#**interface Serial0/1/0**
Router2(conf-if)#**ip access-group 101 in**
Router2(conf-if)#**interface fa0/0**
Router2(conf-if)#**ip access-group 102 in**

Для перевірки, що ACL присутні на інтерфейсах, використовуйте команду:

Router2 #**show running-config**

або

Router2 #**show ip interface**

Перевіримо функціонування ACL. Приєднаємося до R3 і спробуємо безуспішно пропінгувати інтерфейс Serial0/1/0 на R2.

Router3 #**ping 172.16.1.17**

ACL номер 101 заблокував ping. Але повинен дозволити telnet

Router3 #**telnet 172.16.1.17**

Успішно. Введемо пароль “router2”. Запрошення Router3# змінилося на Router2>. З R2 можна пропінгувати R3 чи R1, для цього треба виконати команду **ping 172.16.1.18 або ping 172.16.1.2.** У даному випадку команда **ping 172.16.1.18** не спрацює. Для повернення на R3 треба ввести одночасно **ctrl-shift-6**, а потім **x**, повернемося до запрошення Router3#.

Подивимося номер сесії і видалимо телнет з'єднання.

Router3 #**show sess**

Router3 #**disconnect 1**

Приєднаємося до R1 і подивимося, чи можна пропінгувати інтерфейс Serial на R3.

Router1 #**ping 172.16.1.18**

Невдало. Пакет стартує в R1, йде через R2 і приходить на R3. На R3 він переформується і відсилається назад до R1. Коли R3 переформатовує пакет, адреса джерела стає адресою приймача, а адреса приймача стає адресою джерела. Коли пакет приходить на інтерфейс Serial0/1/0 на R2 він відкидається, так як адреса джерела дорівнює IP адресі інтерфейсу Serial0/1/0 на R2 **172.16.1.17,** а тут дозволений лише

tcp. Приєднаємося до R1 і подивимося, чи можемо ми пропінгувати інтерфейс Ethernet0 на R2.

Router1 # **ping 172.16.1.1**

Успішно. Аналогічно і для телнет

Router1 # **telnet 172.16.1.1**

Введемо пароль “router2” (для повернення **ctrl-shift-6**, а потім **x**). ACL працюють успішно.

1.5 Самостійне завдання

Використовуючи наступну модель мережі (рис.1.4), але змінивши її кожен під свій варіант, виконайте наведені нижче завдання. Усі налаштування можна використати у курсовому проекті.

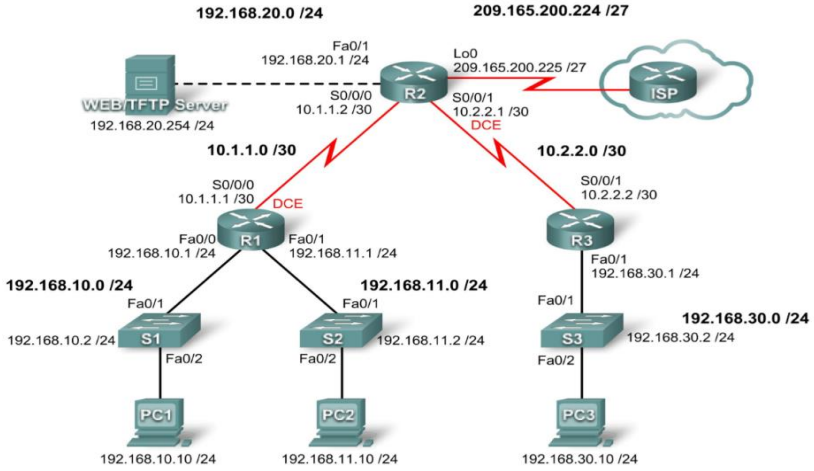

Рисунок 1.4 – Модель мережі

Для налаштування, використовуйте таблицю 1.4 але **кожний студент повинен <u>індивідуально</u> змінити усі мережі**, які починаються **з 192.168** (у прикладі) **на власні**. Де **192** змінюється на **номер студента у списку групи, а 168** на **кількість літер у прізвищі студента**.

Приклад. Федоренко (№ за списком 18) – усі табличні данні повинен змінити з 192.168.x.x на 18.9.x.x і у подальших налаштуваннях використовувати тільки їх.

Таблиця 1.4 – Приклад налаштування

Елемент мережі	Інтерфейс	Ір-адреса	Маска мережі	Шлюз за замовченням
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Примітка. Якщо виникають труднощі, то зверніть увагу на те, що загальні налаштування маршрутизаторів наведені далі, у пункті 1.5.6.

1.5.1 Розробка схеми та налаштування мережі

Спочатку треба зібрати мережу, згідно топології рисунку 1.4.

Ви можете використовувати будь-який маршрутизатор у вашій роботі, якщо він має необхідні інтерфейси, які наведено на рисунку.

Примітка. Ця схема розроблена та перевірена з використанням маршрутизаторів серії 1841. Якщо ви використовуєте маршрутизатори іншої серії, порти маршрутизатора та опис інтерфейсів можуть бути іншими. На старих маршрутизаторах деякі команди не існують зовсім.

Видалить будь-які існуючі конфігурації на маршрутизаторах, якщо ви скористались робочою схемою мережі.

Налаштуйте конфігурацію маршрутизаторів R1, R2, R3, комутаторів S1, S2, S3 комп'ютерів та серверу, відповідно до наступних правил:

– налаштуйте імена пристроїв так, щоб вони відповідали схемі на рисунку;

– вимкніть пошук DNS (команда no ip domain-lookup);
– налаштуйте пароль режиму EXEC класу;
– налаштуйте пароль cisco для консольних з'єднань;
– налаштуйте пароль для віддалених підключень VTY;
– налаштуйте IP-адреси та маски на усіх пристроях;
– увімкніть область OSPF з ідентифікатором процесу 1 для всіх маршрутизаторів і мереж;

налаштуйте інтерфейс зворотного зв'язку на R2 для моделювання ISP (команда interface loopback0);

– налаштуйте IP-адреси для інтерфейсів VLAN1 на кожному комутаторі;

– налаштуйте кожен перемикач за допомогою відповідного шлюзу за замовчуванням;

– перевірте повне з'єднання через IP за допомогою команди ping.

Примітка. Далі неведені команди, які вам допоможуть при виконанні налаштування.

Включити запис історії зміни конфігурації.

(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging on
(config-archive-log-cfg)# hidekeys

Включити ведення журналу.

(config)# logging on
(config)# logging buffered
(config)# logging trap <0-7>

0 - мінімум, 7- запис усіх повідомлень

Встановити пароль на привелегірований режим.

Router(config)#enable password *пароль*
або
Router(config)#enable secret *пароль*

Встановити пароль на лінії vty.

Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password *пароль*

Пароль на консоль.

Router(config)#line console 0
Router(config-line)#password *пароль*

Router(config-line)#login
Тепер при підключенні з консолі отримали запрошення:
Press RETURN to get started.
User Access Verification
Password:
Треба ввести пароль. При введенні символи не відображаються.

1.5.2 Конфігурування стандартного ACL

Стандартні списки ACL можуть фільтрувати трафік лише на основі IP-адреси джерела. Типовою практикою є налаштування стандартного ACL як можна ближче до місця призначення. У цьому завданні ви налаштуєте стандартний ACL. ACL призначений для блокування трафіку з мережі 192.168.11.0/24 для доступу до будь-яких локальних мереж на R3.

Цей ACL застосовано до вхідного послідовного (Serial) інтерфейсу R3. Пам'ятайте, що кожен ACL має неявний "deny all", що приводить до блокування всього трафіку, який не співпадає з умовами в ACL. З цієї причини треба додати дозвіл будь-якому твердженню у кінці ACL.

Перш ніж налаштувати та застосувати цей ACL, обов'язково перевірте підключення з PC1 (або інтерфейсу Fa0/1 на R1) до PC3 (або інтерфейсу Fa0/1 на R3). Тести з'єднання повинні бути успішними перед застосуванням ACL.

Далі треба створити ACL на маршрутизаторі R3. Для цього у режимі глобальної конфігурації створіть стандартний, іменований ACL, з ім’ям STND-1.

R3(config)#ip access-list standard STND-1

У режимі конфігурації стандартного ACL додайте команду, яка заблокує всі пакети з інтерфейсу, адреса якого 192.168.11.0/24.

R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255

Дозволити увесь інший трафік.

R3(config-std-nacl)#permit any

Далі зробіть прив’язку ACL до інтерфейсу.

Визначте ACL STND-1 фільтром на вхідні пакети R3 через Serial interface 0/0/1.

R3(config)#interface serial 0/0/1

R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start

Протестуйте роботу ACL.

Перевірте роботу ACL, використовуючи пінг від PC2 до PC3. Оскільки ACL призначений для блокування трафіку з вихідними адресами з мережі 192.168.11.0/24, PC2 (192.168.11.10) не буде мати можливості для ping PC3.

Ви також можете використовувати розширений пінг від інтерфейсу Fa0/1 на R1 до інтерфейсу Fa0/1 на R3.

R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Введіть escape-послідовність для завершення.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)

Ви повинні побачити наступне повідомлення на консолі R3:

*Sep 4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0 0.0.0.0 -> 192.168.11.1, 1 packet

У привілейованому режимі EXEC на маршрутизаторі R3 введіть команду **show access-lists**. Ви бачите вивід, подібний до наступного. Кожен рядок ACL має пов'язаний з ним лічильник, який показує, скільки пакетів відповідали правилу.

Standard IP access list STND-1
10 deny 192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
20 permit any (25 matches)

Метою створення цього ACL є блокування хостів з мережі 192.168.11.0/24. Усім іншим хостам, наприклад з мережі 192.168.10.0/24, слід надавати доступ до мереж на R3. Проведіть ще один тест з PC1 на PC3, щоб переконатися, що цей трафік не заблоковано.

Ви також можете використовувати розширений пінг з інтерфейсу Fa0/0 на R1 до інтерфейсу Fa0/1 на R3.

R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Введіть escape-послідовність для завершення.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms.

1.5.3 Конфігурування розширеного ACL

Якщо потрібна більша деталізація, ви повинні використовувати розширені списки ACL. Розширені списки ACL можуть фільтрувати трафік за принципом більш ніж просто вихідні або вхідні адреси. Розширені списки ACL можуть фільтрувати IP-адреси протоколу,

джерела та призначення, а також номери портів джерела та призначення.

Додаткова політика для цієї мережі говорить про те, що пристрої з мережі 192.168.10.0/24 мають доступ до внутрішніх мереж. Комп'ютери в цій локальній мережі не мають доступу до Інтернету. Тому її користувачі повинні заблокувати доступ до IP-адреси 209.165.200.225. Оскільки ця вимога повинна забезпечувати дотримання умов як до джерела, так і місця призначення, потрібен розширений ACL.

У цьому завданні ви налаштуєте розширений ACL на R1, який блокує трафік, що надходить з будь-якого пристрою мережі 192.168.10.0/24 для доступу до хоста 209.165.200.255 (моделюється ISP). Цей ACL застосовано до інтерфейсу R1 Serial 0/0/0. Найкращою практикою застосування розширених ліцензійних ліній зв'язку є розміщення їх як можна ближче до джерела.

Перед тим, як почати, перевірте, що ви можете запустити ping 209.165.200.225 з PC1.

Далі у режимі глобальної конфігурації створіть іменований, розширений ACL з ім’ям EXTEND-1.

R1(config)#ip access-list extended EXTEND-1

Зверніть увагу, що пропозиція маршрутизатора змінюється, вказуючи на те, що ви зараз перебуваєте в розширеному режимі конфігурації ACL. З цього рядка додайте необхідні команди для блокування трафіку з мережі 192.168.10.0/24 на хост. Використовуйте ключове слово хосту при визначенні місця призначення. Нагадаємо, що неявний "deny all" блокує весь інший трафік без додаткового дозволу. Додайте команду про дозвіл, щоб переконатися, що інший трафік не заблоковано.

R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225

R1(config-ext-nacl)#permit ip any any

Зробіть прив’язку ACL до інтерфейсу.

Із стандартними ACL найкращим кроком є розміщення ACL як можна ближче до місця призначення. Розширені ACL, як правило, розміщуються поблизу джерела. ACL EXTEND-1 розмістимо на послідовному інтерфейсі для фільтрації вихідного трафіку.

R1(config)#interface serial 0/0/0

R1(config-if)#ip access-group EXTEND-1 out
R1(config-if)#end
R1#copy run start

Протестуйте ACL. З PC1 пропінгуйте інтерфейс loopback на маршрутизаторі R2. Ці пінги не повинні пройти, оскільки весь трафік з мережі 192.168.10.0/24 відфільтровується, коли отримувач 209.165.200.225. Якщо адресатом є інша адреса, то пінг повинен бути успішним. Підтвердіть це, перевіривши R3 з комп'ютера мережі 192.168.10.0/24.

Примітка. Розширена функція ping на R1 не може бути використана для перевірки цього ACL, оскільки трафік почнеться в межах R1 і ніколи не буде перевірятися на ACL, який застосовано до послідовного інтерфейсу R1.

R1#show ip access-list

Отримали наступне.

Extended IP access list EXTEND-1
10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
20 permit ip any any

1.5.4 Контроль доступу по vty лініям

Якщо треба або рекомендовано обмежити доступ до ліній VTY маршрутизатора при виконанні віддаленого адміністрування, то можна застосувати ACL до ліній VTY, що дозволить обмежити доступ до певних вузлів або мереж. У цьому завданні вам треба налаштувати стандартний ACL, щоб дозволити хостам з двох мереж отримати доступ до ліній VTY. Іншим пристроям у доступі буде відмовлено.

Переконайтеся, що ви можете встановити telnet з'єднання на R2 з обох маршрутизаторів R1 і R3.

Зконфігуруйте іменований стандартний ACL на маршрутизаторі R2 який дозволяє трафік з 10.2.2.0/30 та192.168.30.0/24 і забороняє весь інший трафік. Назвіть його ACL TASK-5.

R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255

Налаштуйте та виконайте прив'язку ACL до інтерфейсу.

Далі налаштуйте режим конфігурації для п’яти ліній VTY 0-4. Використовуйте команду access-class для застосування ACL до ліній vty у вхідному напрямку.

R2(config)#line vty 0 4
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start

Протестуйте роботу ACL. Для цього виконайте команду telnet на R2 з маршрутизатора R1. Зверніть увагу, що IP-адрес R1 не знаходиться у адресному діапазоні для дозволу ACL TASK-5, тому спроби підключення будуть неуспішні.

R1# telnet 10.1.1.2
Неуспішно.
Trying 10.1.1.2 …
% Connection refused by remote host

При здійсненні команди telnet від R3 до R2 вам буде потрібно ввести пароль для лінії VTY.

R3# telnet 10.1.1.2
Успішно. Треба увійти по паролю.
Trying 10.1.1.2 … Open
Несанкціонований доступ заборонено
User Access Verification
Password:

1.5.5 Вирішення проблем ACLs

Якщо список ACL налаштовано або застосовано до неправильного інтерфейсу чи у неправильному напрямку, мережний трафік може стати небажаним.

Виконайте вилучення ACL STND-1 з S0/0/1 маршрутизатора R3.

Так як раніш ви вже створили та застосували назву стандартного ACL на маршрутизаторі R3, то треба ввести команду **show running-config**, щоб переглянути ACL та його розташування (інтерфейс). Результатом є те, що ACL з назвою STND-1 налаштовано та застосовано на послідовному 0/0/1 (S0/0/1). Цей ACL створено для блокування

всього мережного трафіку з адресою відправника, яка знаходиться в мережі 192.168.11.0/24, при доступі до локальної мережі на R3.

Для видалення цього ACL, треба перейти до режиму конфігурації інтерфейсу для Serial 0/0/1 на R3. Використовуйте команду STND-1 без групи ip, щоб видалити ACL з інтерфейсу.

R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in

Використовуйте команду show running-config, щоб перевірити, що ACL видалено з Serial 0/0/1.

Щоб перевірити напрямок фільтрування ACL, повторно застосуйте ACN STND-1 до інтерфейсу Serial 0/0/1. Цього разу ACL фільтрує вихідний трафік, а не вхідний трафік.

R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out

Перевірте роботу ACL за допомогою виконання пінгу від PC2 до PC3. Можна використовувати розширений пінг з R1. Зверніть увагу, що цього разу пінги досягають успіху, а лічильники ACL не збільшуються. Це можна перевірити за допомогою команди show ip access-list на R3.

Відновіть ACL до початкової конфігурації. Вилучіть ACL з вихідного напрямку та повторно застосуйте його до вхідного напрямку.

R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in

Застосуйте TASK-5 до вхідного послідовного інтерфейсу S0/0/0 маршрутизатора R2.

R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in

Протестуйте роботу ACL. Спробуйте зв'язатися з будь-яким пристроєм, підключеним до R2 або R3 з R1 або до нього підключених мереж. Зверніть увагу, що всі повідомлення заблоковані; однак, лічильники ACL не збільшуються. Це пов'язано з неявним "заперечувати всіх" в кінці кожного ACL. Це заперечення дозволить закрити вхідний трафік до S0/0/0 з будь-якого джерела, виключая R3. Це призведе до вилучення маршрутів з таблиці маршрутизації R1.

Ви повинні бачити повідомлення, подібні до наведених нижче, на консолях R1 і R2 (це займе деякий час):

*Sep 4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

Як тільки ви отримаєте це повідомлення, виконайте команду **show ip route** як на R1, так і на R2, щоб побачити, які маршрути вилучені з таблиці маршрутизації. Вилучіть ACL TASK-5 з інтерфейсу та збережіть свої конфігурації.

R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start

1.5.6 Конфігурація маршрутизаторів

Далі наведена загальна конфігурація маршрутизаторів, згідно основних пунктів завдань.

Примітка. У вас є зміни у адресації, які ви повинні враховувати.

Router 1

```
hostname R1
enable secret class
!no ip domain lookup
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
no shutdown
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
ip access-group EXTEND-1 out
clockrate 64000
no shutdown
!
```

```
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 permit ip any
any
!
banner motd ^ Несанкціонований доступ заборонено.^ !

line con 0
password cisco
logging synchronous
login
!
line vty 0 4
password cisco
login
!
```

Router 2

```
hostname R2
enable secret class
no ip domain lookup

interface Loopback0
ip address 209.165.200.225 255.255.255.224
interface FastEthernet0/1
ip address 192.168.20.1 255.255.255.0
no shutdown
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
no shutdown
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
clockrate 125000
no shutdown
```

```
!
router ospf 1
no auto-cost
network 10.1.1.0 0.0.0.3 area 0
network 10.2.2.0 0.0.0.3 area 0
network 192.168.20.0 0.0.0.255 area 0
network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
permit 10.2.2.0 0.0.0.3
permit 192.168.30.0 0.0.0.255
!
banner motd ^ Несанкціонований доступ заборонено.^ !

line con 0
password cisco
logging synchronous
login
line vty 0 4
access-class TASK-5 in
password cisco
login
!
```

Router 3

```
hostname R3
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
ip address 192.168.30.1 255.255.255.0
no shutdown
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
ip access-group STND-1 in
no shutdown
!
router ospf 1
```

```
network 10.2.2.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
deny       192.168.11.0 0.0.0.255 log
permit any
!
banner motd ^ Несанкціонований доступ заборонено.^ !

line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
!
end
```

1.6 Зміст звіту

– хід роботи;

– основна працююча схема мережі за варіантом та усі схеми мережі, які відображають виконання наведених завдань;

– відповіді на контрольні питання.

1.7 Контрольні питання

1. Наведіть визначення іменованих ACL?
2. Наведіть визначення розширених ACL?
3. Приклад формування стандартного іменованого ACL.
4. Форма команди для формування розширеного списку.
5. Принцип створення та налаштування розширеного ACL. Наведіть приклад.
6. Загальне правило розташування та налаштування ACL. До чого приводить його невиконання?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.

2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.

3. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

4. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.

5. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.