МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
"Комп'ютерні мережі"
для бакалаврів спеціальності 123 "Комп'ютерна інженерія",
усіх форм навчання

Динамічна конфігурація DHCP та стандартні ACL

2018

Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп’ютерні мережі" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Динамічна конфігурація DHCP та стандартні ACL / Укл. Г.Г.Киричек, С.Ю.Скрупський. – Запоріжжя: ЗНТУ, 2018. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.
С.Ю.Скрупський, 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 № 3 від 24.09.2018

Затверджено
на засіданні НМК КНТ
Протокол № 2 від 28.09.2018

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА.
Динамічна конфігурація пристроїв

Мета роботи: навчитися планувати та використовувати мережний протокол DHCP при налаштуванні динамічної конфігурації в комп'ютерних мережах.

1.1 Загальні поняття та особливості використання DHCP

Для нормальної роботи мережі кожному мережному інтерфейсу потрібні конфігураційні параметри.

Сама процедура присвоєння (в ході конфігурації комп'ютерів і маршрутизаторів), крім IP-адрес мережних інтерфейсів пристрою (і масок мережі), включає присвоєння та налаштування інших конфігураційних параметрів.

Адміністратор призначає не тільки IP-адресу вузла, але і інші параметри: маску і IP-адресу маршрутизатора за замовчуванням, IP-адресу DNS сервера, доменне ім'я комп'ютера і т.ін.

DHCP - протокол динамічної конфігурації хостів (Dynamic Host Configuration Protocol). Він автоматизує процес конфігурації мережевих інтерфейсів, гарантуючи від дублювання адрес за рахунок централізованого управління їх розподілом. Робота DHCP описана в RFC -2131, -2132, -2485, -2563, -2610, -2855, -2937, -2939, -3004, -3011, -3046, -3942, -4030, -4039. Протокол DHCP працює відповідно до моделі клієнт-сервер.

Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на отримання IP-адреси. DHCP-сервер посилає повідомлення-відповідь, яка містить IP-адресу та інші конфігураційні параметри.

Сервер DHCP може працювати в різних режимах.

Режими DHCP:

– ручне призначення статичних адрес - адміністратор, з пулом доступних адрес, надає DHCP-серверу інформацію про жорстку відповідність IP-адрес пристроїв мережі фізичним адресам або іншим ідентифікаторам вузлів. DHCP-сервер - завжди видає DHCP-клієнту одну й ту призначену адміністратором IP-адресу (набір конфігураційних параметрів);

– автоматичне призначення статичних адрес - DHCP-сервер самостійно без адміністратора довільно вибирає клієнтові IP-адресу з пулу IP-адрес і видає її клієнтові в постійне користування - між ідентифікатором клієнта і його IP-адресою, існує постійна відповідність, яка встановлюється при першому призначенні DHCP-сервером IP-адреси клієнта. При наступних запитах сервер повертає клієнтові таку ж IP-адресу;

– автоматичний розподіл динамічних адрес - DHCP-сервер видає конфігураційні параметри клієнту на обмежений час (термін оренди). Коли DHCP-клієнт видаляється з мережі, IP-адреса автоматично звільняється. При підключенні до іншої мережі - клієнт автоматично отримає нові конфігураційні параметри. Ні користувач, ні мережний адміністратор не втручаються у процес налаштування. Це надає можливість повторно використовувати IP-адресу для іншого комп'ютера.

Модель DHCP пам'яті характеризується записами ключ - значення для кожного клієнта, де ключ є деяким унікальним ідентифікатором (в межах мережі), а значення - набір конфігураційних параметрів клієнта. Ключ може являти собою пару: адреса IP-мережі, апаратна (MAC) адреса.

Клієнт DHCP, який потребує конфігураційні параметри, посилає широкомовний пакет DHCPDISCOVER в пошуках сервера DHCP. Пакет містить апаратну адресу клієнта. На запит DHCPDISCOVER можуть відповісти декілька серверів DHCP, вони розглядають запит і відправляють у відповідь пакет DHCPOFFER, із запропонованою IP-адресою та іншими параметрами. Клієнт повинен вибрати одну з пропозицій DHCPOFFER і послати у відповідь пакет DHCPREQUEST з ідентифікатором обраного сервера. Інші сервери переглядають пакет DHCPREQUEST і, на основі ідентифікатора сервера, визначають, що їх пропозиція відкинута - запропоновані ними IP-адреси вільні для призначення іншим клієнтам.

Обраний сервер посилає підтвердження (DHCPACK) - процес узгодження завершується. Пакет DHCPACK містить конфігураційні параметри і час оренди. У разі якщо сервер не може прийняти конфігурацію, він посилає пакет DHCPNAK (відмова в підтвердженні), що змушує клієнта почати процес узгодження заново.

1.2 Налаштування мережі
1.2.1 Модель мережі (схема)

Виконайте наступні дії:

– запустіть ярлик на робочому столі Packet Tracer;

– побудуйте модель мережі за схемою, представленою на рисунку 1.1, використовуючи основні параметри комутаційного обладнання та інтерфейсів (табл.1.1).

Далі наведено етапи моделювання та налаштування мережі.

З панелі приладів в робочу область перенесіть 3 маршрутизатора 2620XM (для зручності можна їх перейменувати відповідно R1, R2, R3), 2 комутатори 2950-24 і 6 комп'ютерів. Для цього на панелі приладів необхідно вибрати перший елемент - **Routers** (рис.1.2). Елемент 2620XM перетягуємо в робочу область. Комутатори знаходяться на панелі приладів в розділі Switches. Комп'ютери знаходяться в розділі End Devices.

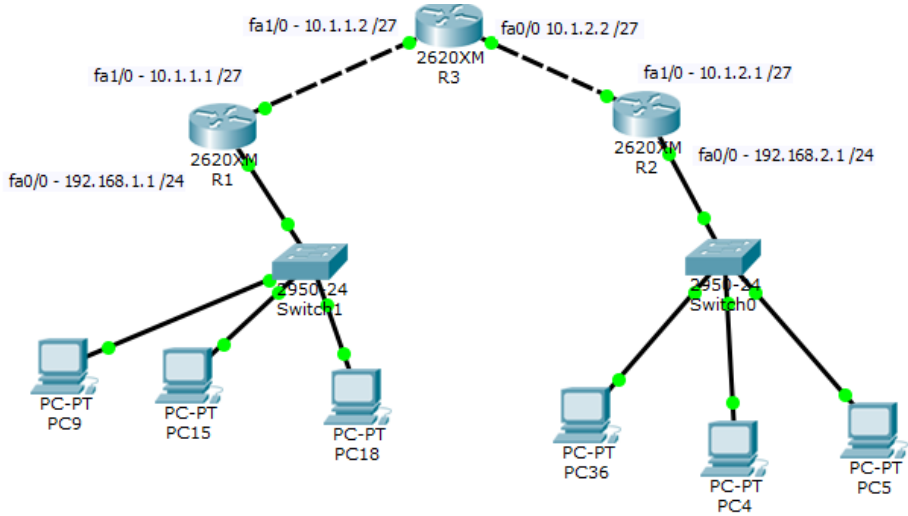

Рисунок 1.1 – Модель мережі

В таблиці 1.1 наведені загальні параметри для налаштування інтерфейсів мережних пристроїв.

Таблиця 1.1 – Параметри інтерфейсів

Пристрій	Інтерфейс	IP-адреса	Маска	Default Gateway	DNS
R1	Fa1/0	10.1.1.1	255.255.255.224	***	***
	Fa0/0	192.168.1.1	255.255.255.0	***	***
R2	Fa1/0	10.1.2.1	255.255.255.224	***	***
	Fa0/0	192.168.2.1	255.255.255.0	***	***
R3	Fa1/0	10.1.1.2	255.255.255.224	***	***
	Fa0/0	10.1.2.2	255.255.255.224	***	***

Примітка. Для перейменування будь-якого елементу моделі мережі, необхідно клацнути лівою кнопкою миші по назві пристрою і ввести необхідне ім'я згідно рисунку 1.1. На вашій схемі номера портів можуть мати іншу нумерацію, тому треба орієнтуватись на свою схему, номери (назву) маршрутизаторів та адреси мереж.

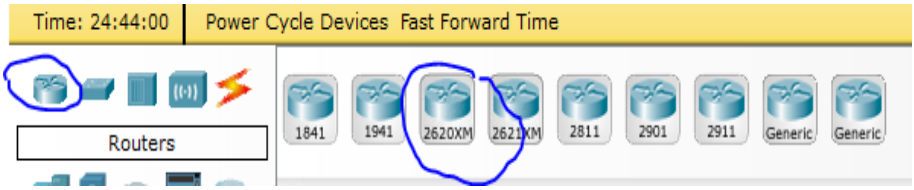

Рисунок 1.2 – Панель обладнання

Далі вибираємо елемент R1 - одне натискання лівої кнопки миші. На вкладці **Physical,** у вікні **Physical Device View** відключаємо живлення (тумблер на 0). З лівого боку екрану вибираємо плату NM-1FE2W (коли треба, дозволяє підключати концентратори з підтримкою стандарту 10Base-T), перед нами з'являється її опис, а зовнішній вигляд - в правому нижньому кутку цього вікна. Тепер можна додати плату, перетягнувши її зображення, до маршрутизатора, згідно рисунку 1.3.

Примітка. Важливо відключати живлення перед установкою плати і не забувати включити після.

Аналогічно додаємо плати до маршрутизаторів R2 та R3.

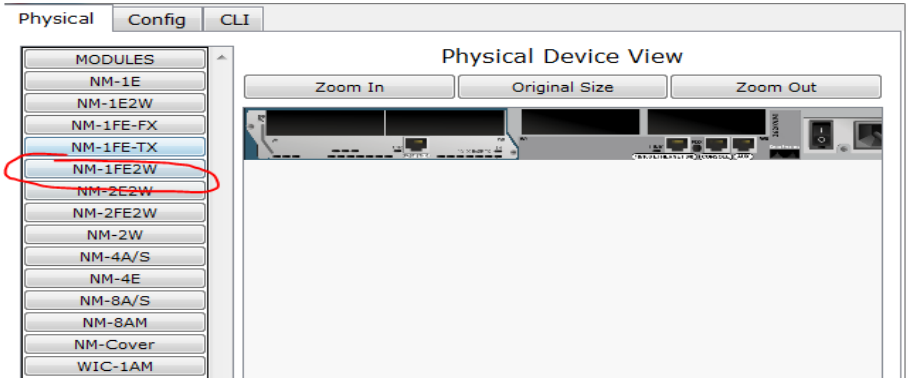

Рисунок 1.3 – Вибір плати NM-1FE2W

З'єднуємо пристрої необхідними кабелями. На панелі інструментів заходимо в розділ **Connections** (рис.1.4) елемент 1. Для вибору перехресної або прямої витої пари необхідно вибрати елементи 2 або 3 (рис.1.4), відповідно.

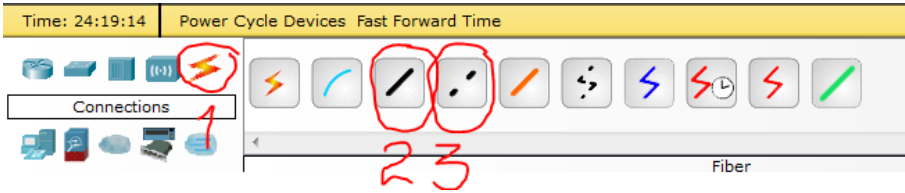

Рисунок 1.4 – Вибір типу кабеля

Для того, щоб з'єднати 2 інтерфейси різних пристроїв кабелем:

– виберіть відповідний кабель, після чого покажчик миші зміниться;

– далі натисніть лівою кнопкою по першому пристрою, який ви хочете підключити;

– у спливаючому меню виберіть порт, до якого буде підключено кабель;

– задайте кінцеву точку кабелю: вибираємо наступний пристрій і аналогічно підключаємо порт (рис.1.5).

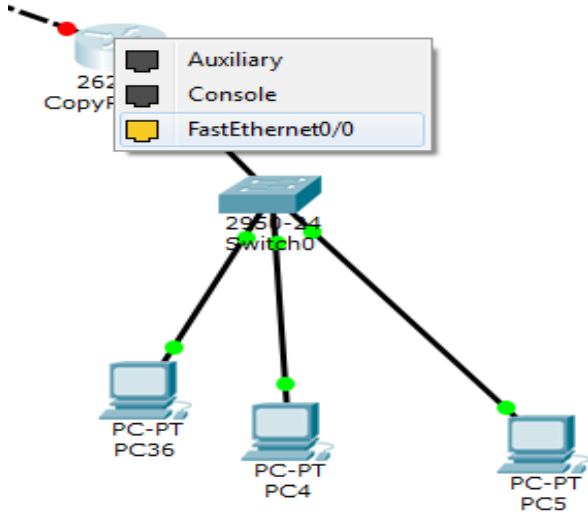

Рисунок 1.5 – Підключення кабелю

1.2.2 Налаштування маршрутизатора R1

Натисніть лівою клавішею миші на R1. Відкриється вікно налаштувань маршрутизатора, ви потрапите на вікно Physical Device View.

Вкладка CLI – командний рядок маршрутизатора. Вкладка Config – налаштування маршрутизатора.

Примітка. Усі подальші команди виконуються у вікні CLI.

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– для перейменування маршрутизатора (якщо треба) вводимо в терміналі команду:

> hostname R1, де R1 – нове ім'я маршрутизатора;

– встановлюємо пароль на привілейований режим, ввівши команду:

> Enable secret knt_4, де knt_4 - значення пароля;

Примітка. Для того, щоб перевірити чи встановився пароль необхідно вийти з режиму налаштування і режиму конфігурації:

> exit

> exit

або

> end

А потім у цьому ж вікні знову спробувати в нього увійти:

> enable

У рядок, який з'явився, введіть пароль;

Ввійдіть до режиму налаштування конфігурації:

> configure terminal

Для налаштування IP - адреси на інтерфейсах задайте:

> **interface fa0/0**

В режимі налаштування конфігурації інтерфейсу задайте параметри, згідно з таблицею 1.1:

> **ip address 192.168.1.1 255.255.255.0**

Увімкнить інтерфейс командою:

> **no shutdown**

Тепер налаштовуємо наступні інтерфейси:

> interface fa1/0

> ip address 10.1.1.1 255.255.255.224

> no shutdown

Виходимо з налаштування інтерфейсу та конфігурації:

> exit

> exit

Далі необхідно зберегти налаштування, ввівши команду:

> write

Аналогічним чином налаштовуємо маршрутизатор R2:

> **interface fa0/0**;

> **ip address 192.168.2.1 255.255.255.0.**

> **no shutdown**

> interface fa1/0

> ip address 10.1.2.1 255.255.255.224

> no shutdown

> exit

> exit

> write

Для маршрутизатора R3:

> **interface fa0/0**;
> **ip address 10.1.2.2 255.255.255.224.**
> **no shutdown**
> **interface fa1/0**
> **ip address 10.1.1.2 255.255.255.224**
> **no shutdown**
> **exit**
> **exit**
> **write**

1.2.3 Налаштування динамічної маршрутизації

Для того щоб налаштувати OSPF маршрутизацію необхідно на кожному маршрутизаторі прописати адреси та інверсні маски мереж, які безпосередньо підключені до даного маршрутизатора. Розглянемо на прикладі маршрутизатора R1.

Для налаштування маршрутизатора R1 натисніть лівою клавішею миші на R1. Відкриється вікно налаштування маршрутизатора, ви потрапите на вікно Physical Device View.

Примітка. Усі подальші команди виконуються у вікні CLI.

Заходимо в налаштування протоколу OSPF, ввівши команду:

> **router ospf 1**

Далі додаємо мережі, які безпосередньо підключені до маршрутизатора. В команді вказуємо адресу з інверсною маскою підмережі і зону дії протоколу:

> **network 192.168.1.0 0.0.0.255 area 0**
> **network 10.1.1.0 0.0.0.31 area 0**

Примітка. На всіх маршрутизаторах необхідно вказувати одну і ту ж зону дії протоколу (area 0).

Вийти з режиму налаштування командою:

> **end**

Зберегти зміни:

> **write**

Виконуємо попередні налаштування для маршрутизаторів R2, R3 враховуючи топологію мережі (рис.1.1) та таблицю 1.1.

Мережі для R2:

> **network 192.168.2.0 0.0.0.255 area 0**
> **network 10.1.2.0 0.0.0.31 area 0**

Мережі для R3:

> network 10.1.1.0 0.0.0.31 area 0

> network 10.1.2.0 0.0.0.31 area 0

Примітка. Перевірку налаштувань маршрутизатора можна виконати в привілейованому режимі терміналу маршрутизатора, використовуючи команди:

>**show ip protocols** – продемонструє налаштовані протоколи маршрутизації.

>**show ip ospf** – покаже основні налаштування OSPF протоколу.

>**show ip ospf neighbour** – виводить список сусідніх маршрутизаторів, що працюють з цим протоколом.

>**show ip int brief** – необхідна для перевірки IP-адрес інтерфейсів.

>**show ip route** – таблиця маршрутизації.

1.3 Налаштування DHCP сервера та DHCP-relay

Виконаємо конфігурацію на R3 задав пули адрес для кожної локальної мережі: в режимі глобальної конфігурації визначимо адреси, які будуть виключені з пулу (це адреси інтерфейсів R1 та R2). Щоб конфігурувати пул IP адрес в консолі маршрутизатора R3 введіть команди:

> conf t (або configure terminal)

> ip dhcp excluded-address 192.168.1.1

> ip dhcp excluded-address 192.168.2.1

Створимо пул адрес з ім'ям LAN_1:

> ip dhcp pool LAN1

> network 192.168.1.0 255.255.255.0

> default-router 192.168.1.1

Створимо пул адрес з ім'ям LAN_2:

> ip dhcp pool LAN2

> network 192.168.2.0 255.255.255.0

> default-router 192.168.2.1

Наступний етап - конфігурація агентів DHCP-Relay на маршрутизаторах R1 і R2.

Суть DHCP-Relay полягає у пересиланні широкомовного пакета від клієнта одноадресним пакетом DHCP-серверу.

Вибираємо інтерфейс, на який буде приходити широкомовний запит від клієнтів, в даному випадку це інтерфейс f0/0 маршрутизатора, який підключений до сегмента мережі. Для налаштування маршрутизатора R1 як DHCP-Relay, в консолі R1 введіть команди:

> conf t

> interface fa0/0 ip helper-address 10.1.1.2

Аналогічно конфігурується маршрутизатор R2:

> conf t

> interface fa0/0 ip helper-address 10.1.2.2.

1.4 Налаштування робочої станції (ПК)

На всіх кінцевих вузлах (комп'ютер, тощо) необхідно налаштувати підключення до мережі з використанням DHCP. Налаштування розглянемо на прикладі PC1:

– на комп'ютері PC1 натисніть лівою кнопкою миші. Відкриється діалогове вікно з ім'ям комп'ютера;

– перейдіть на вкладку «Desktop» (рис. 1.6);

– оберіть пункт «IP Configuration»;

– у вікні на панелі перемикачів групи «IP Configuration» встановіть у активне положення DHCP (рис. 1.7). У разі правильних налаштувань, через деякий час будуть отримані налаштування DHCP;

– закрийте діалогове вікно;

– повторіть аналогічні дії з усіма комп'ютерами.

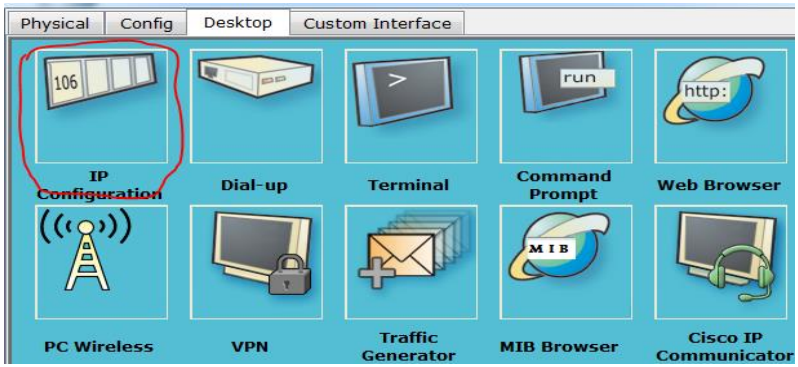

Рисунок 1.6 – Конфігурація комп'ютера

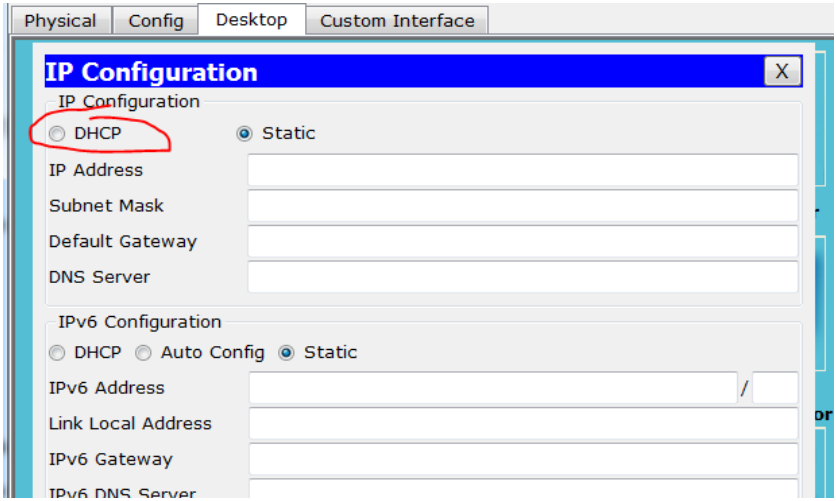

Рисунок 1.7 – Вибір конфігурації IP DHCP

1.5 Індивідуальне завдання

Змінити конфігурацію з FastEthernet на Ethernet. Для цього:

– вимкніть роутери R1, R2 та R3. Для того, щоб вимкнути роутер, необхідно клацнути по ньому лівою кнопкою миші, після чого в діалоговому вікні на вкладці «Physical» натиснути на вимикач, зображений на роутері;

– видалити всі кабелі, які підключені до роутерів. Для цього виділіть кабель, який необхідно видалити, і натисніть клавішу Delete. Підтвердіть дію.

– на кожному з роутерів замінити плату **NM-1FE2W** на плату **NM-1E2W.** Клацніть лівою кнопкою миші по роутеру. На вкладці «Physical» на зображенні вимкненого роутера натисніть на плату і потягніть її в ліву частину діалогового вікна. Плата буде видалена (рис. 1.8). Для того, щоб помістити плату **NM-1E2W,** оберіть її зі списку доступних плат і потягніть на виділене місце (рис. 1.8);

– підключіть кабелі згідно топології (рис. 1.1);

– почекайте якийсь час, поки конфігуруються комутатори.

Примітка. Дізнатися про завершення ініціалізації комутаторів можна за кольором кружечків, які супроводжують кабелі, які йдуть від

комутаторів. У разі повністю готового до роботи комутатора колір кружечків – зелений (рис. 1.9).

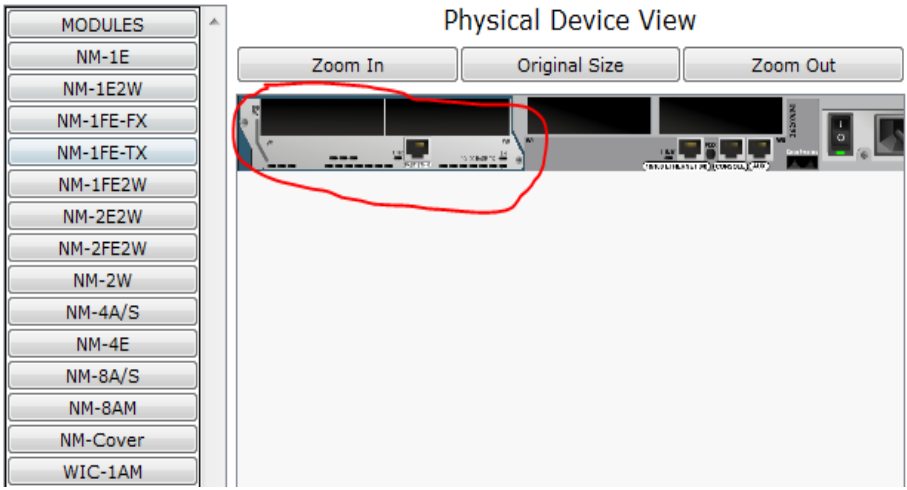

Рисунок 1.8 – Місце плати для маршрутизатора **2620XM**

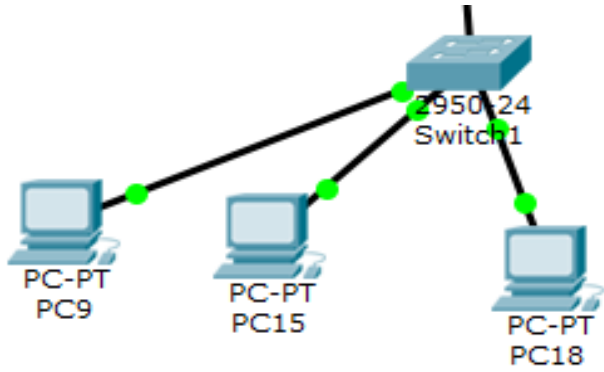

Рисунок 1.9 – Комутатор готовий до роботи

Змініть конфігурацію мережі відповідно до свого варіанту (табл. 1.2). Номери мереж наведені на рисунку 1.10.

Виконайте налаштування маршрутизації, DHCP-сервера і агентів DHCP-Relay згідно нової конфігурації мережі.

Таблиця 1.2 – Варіанти завдань

Варіант	Мережа 1	Мережа 2	Мережа 3	Мережа 4
1	10.3.1.0 /31	10.4.1.0 /31	192.169.1.0 /24	192.170.1.0 /24
2	10.3.2.0 /31	10.4.2.0 /31	192.169.2.0 /24	192.170.2.0 /24
3	10.3.3.0 /31	10.4.3.0 /31	192.169.3.0 /24	192.170.3.0 /24
4	10.3.4.0 /31	10.4.4.0 /31	192.169.4.0 /24	192.170.4.0 /24
5	10.3.5.0 /31	10.4.5.0 /31	192.169.5.0 /24	192.170.5.0 /24
6	10.3.6.0 /31	10.4.6.0 /31	192.169.6.0 /24	192.170.6.0 /24
7	10.3.7.0 /31	10.4.7.0 /31	192.169.7.0 /24	192.170.7.0 /24
8	10.3.8.0 /31	10.4.8.0 /31	192.169.8.0 /24	192.170.8.0 /24
9	10.3.9.0 /31	10.4.9.0 /31	192.169.9.0 /24	192.170.9.0 /24
10	10.3.10.0 /31	10.4.10.0 /31	192.169.10.0 /24	192.170.10.0 /24
11	10.3.11.0 /31	10.4.11.0 /31	192.169.11.0 /24	192.170.11.0 /24
12	10.3.12.0 /31	10.4.12.0 /31	192.169.12.0 /24	192.170.12.0 /24
13	10.3.13.0 /31	10.4.13.0 /31	192.169.13.0 /24	192.170.13.0 /24
14	10.3.14.0 /31	10.4.14.0 /31	192.169.14.0 /24	192.170.14.0 /24
15	10.3.15.0 /31	10.4.15.0 /31	192.169.15.0 /24	192.170.15.0 /24
16	10.3.16.0 /31	10.4.16.0 /31	192.169.16.0 /24	192.170.16.0 /24
17	10.3.17.0 /31	10.4.17.0 /31	192.169.17.0 /24	192.170.17.0 /24
18	10.3.18.0 /31	10.4.18.0 /31	192.169.18.0 /24	192.170.18.0 /24
19	10.3.19.0 /31	10.4.19.0 /31	192.169.19.0 /24	192.170.19.0 /24
20	10.3.20.0 /31	10.4.20.0 /31	192.169.20.0 /24	192.170.20.0 /24
21	10.3.21.0 /31	10.4.21.0 /31	192.169.21.0 /24	192.170.21.0 /24
22	10.3.22.0 /31	10.4.22.0 /31	192.169.22.0 /24	192.170.22.0 /24
23	10.3.23.0 /31	10.4.23.0 /31	192.169.23.0 /24	192.170.23.0 /24
24	10.3.24.0 /31	10.4.24.0 /31	192.169.24.0 /24	192.170.24.0 /24

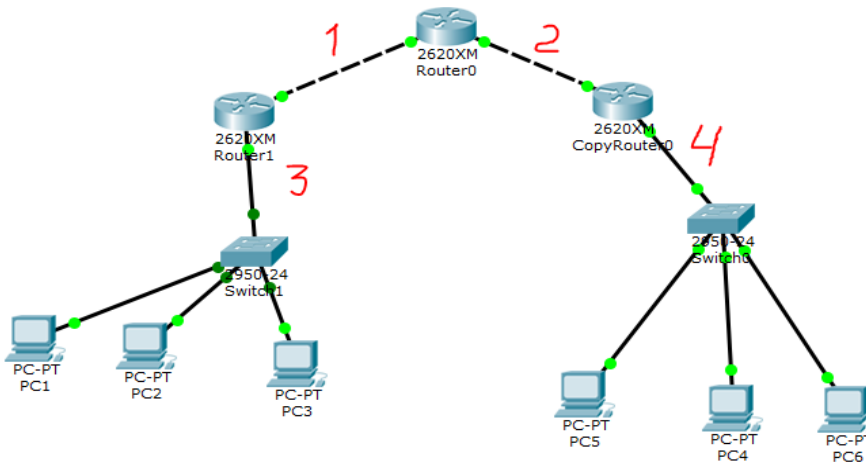

Рисунок 1.10 – Модель мережі для індивідуального завдання

1.6 Зміст звіту

– хід роботи;
– налаштування;
– оригінальна схема мережі;
– індивідуальна схема мережі;
– відповіді на контрольні питання.

1.7 Контрольні питання

1. Що означає термін DHCP?
2. Які конфігураційні параметри надає серевер DHCP?
3. Які ви знаєте режими роботи DHCP?
4. Надайте визначення ручного призначення статичних адрес.
5. Надайте визначення автоматичного призначення статичних адрес.
6. Надайте визначення автоматичного розподілу динамічних адрес.
7. Наведіть та опишить повідомлення DHCP при виконанні запитів на отримання конфігураційних параметрів.

2 ЛАБОРАТОРНА РОБОТА.
Стандартні списки контролю доступу

Мета роботи: навчитися безпечної маршрутизації трафіку при налаштуванні списків контролю доступу в комп'ютерних мережах.

2.1 Загальні поняття та особливості використання ACL

ACL складається з ролей і ресурсів. Ресурсами є об'єкти, на які накладаються певні дозволи за допомогою ACL. Ролями є об'єкти, які запитують доступ до ресурсів і отримують відповідь від ACL: дозволено / заборонено.

ACL (access control list) - механізм для вибору частини з усього потоку трафіку, за заданими критеріями. Наприклад, через маршрутизатор проходить безліч пакетів, і ACL вибирає тільки ті пакети, які йдуть з мережі 172.16.1.0/24: access-list 1 permit 172.16.1.0. Є два способи використання ACL: основний - фільтрація трафіку та другий - використання ACL при налаштуванні NAT. Але не має значення для яких цілей ми використовуємо ACL, правила написання ACL не змінюються.

Крім того, якщо ми тільки створили ACL, то він поки ні на що не впливає. ACL - це просто декілька непрацюючих рядків у конфігурації, до тих пір поки ми його не застосуємо, наприклад, до інтерфейсу або для фільтрації трафіку.

ACL є двох видів: стандартні і розширені. Стандартні дозволяють фільтрувати трафік тільки за одним критерієм: адреса відправника, що є не завжди достатнім.

Для конфігурування стандартних списків управління доступом IP використовуються номера 1-99 або 1300-1999. Але на приоритет номер списку не має ніякого впливу. Можна, наприклад, поставити на виході з мережі такий ACL:

access-list 1 permit host 172.16.10.50
access-list 1 permit host 172.16.10.53
access-list 1 permit host 172.16.10.60

Цей ACL дозволяє вихід в інтернет тільки з перерахованих трьох ip адрес.

ACL - набір правил. Кожне правило складається з дії (permit, deny) і критерію (для стандартних ACL - ip адреса відправника, для

розширених - безліч критеріїв). Розглянемо приклад стандартного нумерованного ACL:

access-list 1 permit host 172.16.1.1
access-list 1 deny 172.16.1.0
access-list 1 permit any

Цей ACL забороняє доступ для мережі 172.16.1.0/24 крім хоста 172.16.1.1 і надає доступ для всіх інших мереж.

Трафік на відповідність ACL перевіряється за рядком. Приходить, наприклад, пакет з адреси 172.16.2.2 на роутер, а на інтерфейсі через який він прийшов стоїть на вхід вказаний вище ACL. IP адреса відправника звіряється з даними ACL - до першого збігу.

Як тільки пакет співпадає з одним із рядків, спрацює дія (permit - пропустити пакет або deny - знищити пакет) і далі ніяких перевірок проводитися не буде. Якщо все рядки пройдені, а пакет так і не потрапив ні під одне з правил, то він за замовчуванням знищується. У нашому випадку будь-який пакет підходить під третій запис (замість адреси вжито слово «any»), будь-яка адреса підійде. Наведений ACL можна читати так:

– якщо пакет прийшов з адреси 172.16.1.1 - його треба відразу ж пропустити і не робити більше ніяких перевірок в цьому ACL;

– якщо пакет прийшов з мережі 172.16.1.0 (крім адреси 172.16.1.1), пакет треба знищити і закінчити перегляд ACL;

– якщо пакет не потрапив під перші два правила, він завжди потрапляє під правило permit any, тобто, пакет треба пропустити далі.

Дуже важливо розуміти наведений вище порядок перегляду рядків в ACL, він єдиний для всіх типів ACL (не тільки для стандартного).

Крім того, з цього порядку слідує правило: «У ACL спочатку повинні йти найбільш специфічні, вузькі, точні рядки, а найбільш абстрактні, загальні - в кінці». Якби попередній приклад був би відсортований у зворотному порядку:

access-list 1 permit any
access-list 1 deny 172.16.1.0
access-list 1 permit host 172.16.1.1

То згідно попереднього алгоритму, працює він так:

Перевіряємо перший рядок, якщо пакет з будь-якої мережі (any) то його треба пропустити і перегляд далі припинити. Крапка.

На цьому перегляд списку завершено і зовсім неважливо, що написано у другому, третьому і далі рядках, бо весь трафік потрапляє під дію першої команди і на цьому процес роботи ACL завершується.

ACL застосовується для різних цілей, але основна мета - фільтрація трафіку на інтерфейсі.

2.2 Rip маршрутизація та ACL

Для початку в середовищі моделювання Packet Tracer треба зібрати схему з трьох маршрутизаторів (рис.2.1). При моделюванні можна використовувати маршрутизатор моделі 1841 (вказано на схемі).

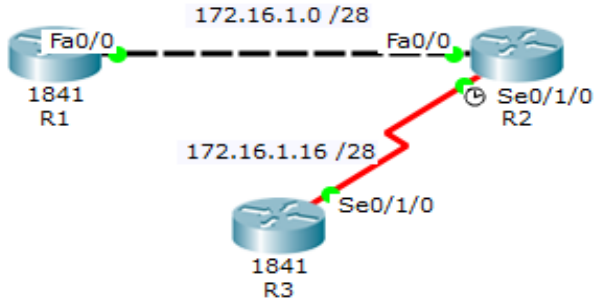

Рисунок 2.1 – Модель мережі

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

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

Далі призначимо адреси інтерфейсів згідно таблиці 2.1. При налаштуванні Serial портів не забувайте задати значення синхронізації (наприклад 64000).

Таблиця 2.1 – 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 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) Router1 з Router3).

Router3#**ping 172.16.1.2**

Успішна відповідь є такою:

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms.

Створимо стандартний список доступу, який не дозволить пінгувати маршрутизатор 1 з маршрутизатора 3.

Для цього блокуємо єдину адресу 172.16.1.18 маршрутизатора 3 і дозволимо інший трафік. Список створимо на маршрутизаторі 1 наступними командами

Router1(config)#**access-list 1 deny 172.16.1.18 0.0.0.0**

Router1(config)#**access-list 1 permit 0.0.0.0 255.255.255.255**

Застосуємо список до інтерфейсу Ethernet маршрутизатора 1

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip access-group 1 in**

Перевіримо, що список доступу запущено. Для цього переглянемо працюючу конфігурацію

Router1#**show running-config**

Router1#**show ip interface**

Можемо бачити, що список застосовано до інтерфейсу, використовуючи команду "show ip interface".

Знайдіть в виведеній інформації рядок з "Innbound access list is 1". Команда "show access-lists" покаже нам вміст створеного списку доступу.

Router1#**show access-lists**

Standard IP access list 1

10 deny host 172.16.1.18

20 permit any (4 match (es))

host 172.16.1.18 теж саме 172.16.1.18 0.0.0.0.

Тепер при спробі пінгувати інтерфейс Ethernet (172.16.1.2) маршрутизатора 1 з маршрутизатора 3:

Router3#**ping 172.16.1.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

UUUUU

Success rate is 0 percent (0/5)

Отримали рядок "UUUUU", який означає, що список доступу є коректним.

2.3 OSPF та стандартний ACL

Створимо і завантажимо в симулятор топологію з рисунку 2.2, Призначимо адреси інтерфейсів згідно з таблицею 2.2.

Примітка. Уважно перевіряйте реальні порти, в реальних мережах.

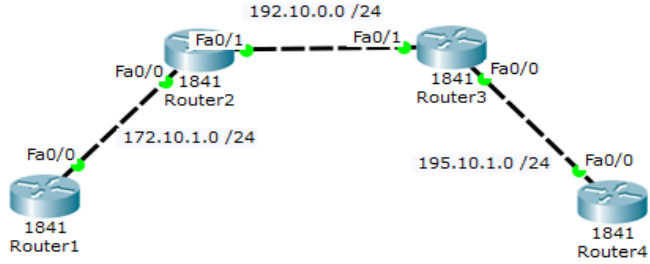

Рисунок 2.2 – Модель мережі

Таблиця 2.2 – Налаштування

	Router1	Router2	Router3	Router4
Ea0/0	172.10.1.2	172.10.1.1	195.10.1.2	195.10.1.1
Ea0/1		192.10.0.1	192.10.0.2	

Виконуємо налаштування конфігурації OSPF маршрутизації.

Для Router1
Router1(config)#**router ospf 1**
Router1(config- router)#**network 172.10.1.0 0.0.0.255 area 0**
Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Для Router2
Router2(config)#**router ospf 1**
Router2(config- router)#**network 172.10.1.0 0.0.0.255 area 0**
Router2(config- router)#**network 192.10.0.0 0.0.0.255 area 0**
Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Для Router3
Router3(config) #**router ospf 1**
Router3(config- router)#**network 192.10.0.0 0.0.0.255 area 0**
Router3(config- router)#**network 195.10.1.0 0.0.0.255 area 0**
Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Для Router4
Router4(config)#**router ospf 1**
Router4(config- router)#**network 195.10.1.0 0.0.0.255 area 0**
Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Для перевірки пропінгуйте крайні точки.
Router1 #**ping 195.10.1.1**
Router4 #**ping 172.10.1.2**

Створимо стандартний список доступу для фільтрації трафіку, що приходить на інтерфейс 172.10.1.1 router2 і дозволяє трафік від мережі 192.10.0.0 (router3) і блокує трафік від інших пристроїв.
Router2 (config) #**access-list 1 permit 192.10.0.0 0.0.0.255**
Перевірте, що він створився
Router2#**show access-list**
Standard IP access list 1
permit 192.10.0.0 0.0.0.255

Приєднайте список як вхідний до інтерфейсу Ethernet 1.
Router2 (config) #**interface FastEthernet0/1**
Router2 (config-if) #**ip access-group 1 in**

Перевірте приєднання командою
Router2 #**show running-config**

Перевірте зв'язок між 3 і 1 маршрутизаторами та між 4 і 1.
Router3 #**ping 172.10.1.2**
Router4 #**ping 172.10.1.2**
Зв'язок між 3 і 1-м роутерами повинен бути, а між 4 і 1 - ні.

Змінимо список доступу - дозволимо трафік від мережі 195.10.1.0 (R4) і заблокуємо трафік від інших пристроїв.
Router2 (config) #**no access-list 1 permit 192.10.0.0 0.0.0.255**
Router2 (config) #**access-list 1 permit 195.10.1.0 0.0.0.255**

Перевірте, що він змінився
Router2 #**show access-list**

Standard IP access list 1
permit 195.10.1.0 0.0.0.255

Від'єднайте список як вхідний до інтерфейсу Ethernet 1
Router2(config)#**interface FastEthernet0/0**
Router2(config-if)#**no ip access-group 1 in**

Приєднайте список як вихідний до інтерфейсу Ethernet 0
Router2(config)#**interface FastEthernet0/0**
Router2(config-if)#**ip access-group 1 out**

Перевірте приєднання командою
Router2#**show running-config**

Перевірте зв'язок між 3 і 1 маршрутизаторами та між 4 і 1.
Router3#**ping 172.10.1.2**
Router4#**ping 172.10.1.2**
Зв'язок між 4 і 1-м роутерами повинен бути, а між 3 і 1 - ні.

2.4 Міжмережні налаштування ACL

Здійсніть і перевірте конфігурацію IP для мережі на рисунку 2.3 (табл. 2.3) і застосуєте OSPF для організації динамічної маршрутизації.

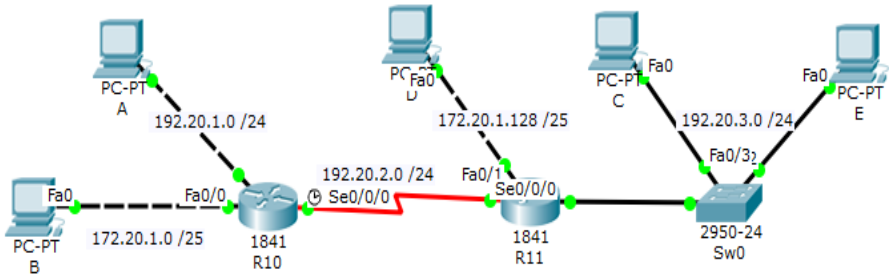

Рисунок 2.3 – Модель мережі

Таблиця 2.3 – Налаштування

	Ea0/0	Ea0/1	S0/0/0	Ea0
R10	172.20.1.1/25	192.20.1.1/24	192.20.2.1/24	
R11	192.20.3.1/24	172.20.1.128/25	192.20.2.2/24	
PC A				192.20.1.2 /24
PC B				172.20.1.2 /25
PC C				192.20.3.2 /24
PC D				172.20.1.129 /25
PC E				192.20.3.3 /24

Для маршрутизатора R10

Router10 (config)#**router ospf 1**

Router10 (config-router)#**network 192.20.1.0 0.0.0.255 area 0**

Router10 (config-router)#**network 192.20.2.0 0.0.0.255 area 0**

Router10 (config-router)#**network 172.20.1.0 0.0.0.127 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Для маршрутизатора R11

Router11(config)#**router ospf 1**

Router11(config-router)#**network 172.20.1.128 0.0.0.127 area 0**

Router11(config-router)#**network 192.20.3.0 0.0.0.255 area 0**

Router11(config-router)#**network 192.20.2.0 0.0.0.255 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write.**

Перевірте працездатність мережі: ви повинні з будь-якого пристрою пінгувати будь-який інтерфейс. Або простіше: всі комп'ютери A, B, C, D, E повинні взаємно попарно пінгуватись.

Далі налаштуємо списки контролю доступу.

Спочатку виконаємо налаштування на маршрутизаторі R10.

Router10 (config)#**access-list 2 deny 172.20.1.128 0.0.0.127**

Router10 (config)#**access-list 2 permit host 192.20.3.2**

Router10 (config)#**access-list 2 deny 192.20.3.0 0.0.0.255**

Router10 (config)#**access-list 2 permit 0.0.0.0 255.255.255.255**

і застосуємо його до інтерфейсу Ea0/0 як вихідний

Router10 (config)#**interface FastEthernet0/0**

Router10 (config-if)#**ip access-group 2 out**

Створити скріншот результату виконання команди
Router10#**show access-list**
Після успішного виконання команди отримали наступні рядки.
Standard IP access list 2
10 deny 172.20.1.128 0.0.0.127
20 permit host 192.20.3.2
30 deny 192.20.3.0 0.0.0.255
40 permit any

Попарно пропінгуємо A, B, C, E, D. У результаті отримали наступну схему доступу 1 (табл. 2.4).

Таблиця 2.4 – Схема доступу 1

	A	B	C	E	D
A	+	+	+	+	+
B	+	+	+	-	-
C	+	+	+	+	+
E	+	-	+	+	+
D	+	-	+	+	+

Бачимо, що політика безпеки повністю реалізована для PC з ідентифікатором B.

Тепер трафік між мережами 172.20.1.0/25 і 172.20.1.128/25 заборонено. Неможливий також трафік між мережею 172.20.1.0/25 і мережею 192.20.3.0/24 за винятком комп'ютера C з адресою 192.20.3.2/24.

Вилучимо ACL с інтерфейсу ea0/0 і застосуємо як вхідний до інтерфейсу s0/0/0.

Router10(config)#**interface fa0/0**
Router10(config-if)#**no ip access-group 2 out**
Router10(config-if)#**int s0/0/0**
Router10(config-if)#**ip access-group 2 in**
Попарно пропінгуем A, B, C, E, D.
У результаті отримали наступну схему доступу 2 (табл. 2.5).

Таблиця 2.5 – Схема доступу 2

	A	B	C	E	D
A	+	+	+	-	-
B	+	+	+	-	-
C	+	+	+	+	+
E	-	-	+	+	+
D	-	-	+	+	+

Політика безпеки тепер повністю реалізована і для PC з ідентифікатором A.

Тепер трафік також заборонено між мережами 192.20.1.0/24 і 172.20.1.128/25. Неможливий також трафік між мережею 192.20.1.0/25 і мережею 192.20.3.0/24 за винятком комп'ютера C з адресою 192.20.3.2/24.

2.5 Самостійне завдання

Виконання даного завдання є обов'язковим при зарахуванні цієї лабораторної работи.

Використовуючи модель мережі міжмережного налаштування ACL (рис.2.3), додайте та підключить до маршрутизатора R11 додатковий маршрутизатор R12. Якщо треба додайте плату до R12 та ще одну плату до R11.

До маршрутизатора R12 підключить ноутбук або PC (назва – перша літера прізвища студента англійською і номер у списку групи (Приклад. Василенко (№ за списком 12) **V12**)).

Адреса мережі між R11 та R12 – 10.(номер студента у списку групи).1.0 маска /28 – (приклад:10.**12**.1.0/28).

Адреса локальної мережі R12 - ноутбук – 10.(номер студента у списку групи).1.16 маска /28 – (приклад:10.**12**.1.16/28).

Створити список ACL, який дозволить доступ пакетів к ноутбуку тільки з компьютерів A та E.

З усіх інших пристроїв доступ закрити.

2.6 Зміст звіту

- хід роботи;
- налаштування;

– схеми мереж;
– відповіді на контрольні питання.

2.7 Контрольні питання

1. Наведіть визначення ACL?
2. Види та типи ACL. Їх характеристики.
3. Загальні команди налаштування стандартних ACL?
4. Які номера використовуються для налаштування стандартних списків контролю доступу?
5. Сформулюйте загальне правило порядку перегляду списків контролю лоступу. Його особливості.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. 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.

2. 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.

3. 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.

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

5. Палмер М. Проектирование и внедрение компьютерных сетей / М.Палмер, Р. Синклер. – СПб.: БХВ-Петербург, 2004. – 752с.

6. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft / Т. Нортроп, Дж.К. Макин // Пер. с англ. – М.: Издательство «Русская Редакция», 2009. – 592с. : ил.

7. Моримото Р. Microsoft Windows Server 2008 R2. Полное рук-во / Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. // Пер. с англ. – М.: ООО "И.Д. Вильямс", 2011. – 1456с. : ил.