

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

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

Spanning Tree Protocol. Використання NAT (PAT)

Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп'ютерні мережі" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Spanning Tree Protocol. Використання NAT (PAT) / Укл. Г.Г. Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2019. – 38 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 № 2 від 06.09.2019

Рекомендовано до видання
НМК КНТ
Протокол № 3 від 24.10.2019

ЗМІСТ

1 Лабораторна робота № 1	4
1.1 Загальні відомості	4
1.2 Модель мережі.....	5
1.3 Основні налаштування комутаторів	8
1.4 Вибір кореневого комутатору	8
1.5 Спостереження за процесом вибору STP порту, виходячи з пріоритету портів	10
1.6 Перше індивідуальне завдання	12
1.7 Створення мережі 2 і налаштування пристроїв.....	13
1.8 Друге індивідуальне завдання.....	16
1.9 Зміст звіту	18
1.10 Контрольні питання	18
2 Лабораторна робота №2.....	18
2.1 Теоретичні відомості.....	18
2.1.1 Статична трансляція NAT	21
2.1.2 Динамічна трансляція NAT	22
2.2 Організація автономного домену rmf....domain01. local	24
2.3 Налаштування NAT-серверу та перевірка його працездатності .	29
2.4 Відновлення комп'ютерів в початковий стан	33
2.5 Зміст письмового звіту.....	36
2.6 Контрольні питання	37
Рекомендована література	38

1 ЛАБОРАТОРНА РОБОТА № 1

Spanning Tree Protocol

Мета роботи: вивчення основ комутації, планування та налаштування мережевого протоколу Spanning Tree Protocol (STP).

1.1 Загальні відомості

Надлишковість дозволяє збільшити доступність пристроїв в топології мережі за рахунок усунення єдиної точки відмови. В комутованій мережі вона забезпечується за допомогою використання додаткових комутаторів або декількох додаткових каналів між комутаторами. Але коли в реальній мережі використовується фізична надмірність (рис.1.1), можливе виникнення петель і дублювання кадрів.

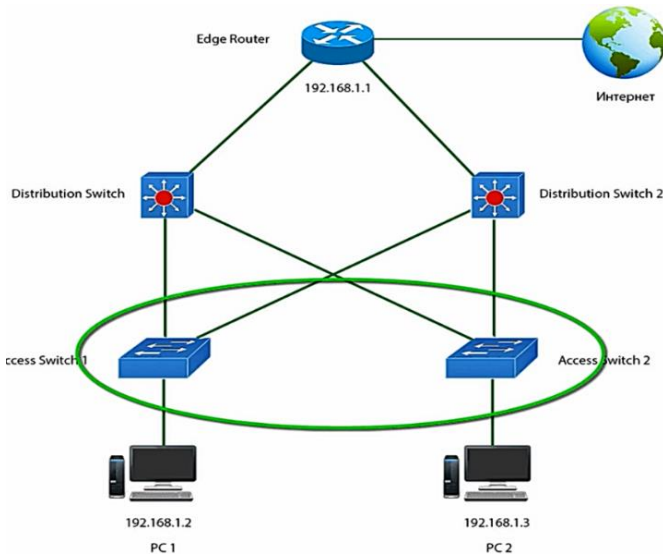


Рисунок 1.1 – Багаторівневий підхід при реалізації мереж

Протокол spanning-tree (STP) розроблено як механізм запобігання виникненню петель на 2 рівні моделі OSI (рис.1.1) при використанні додаткових каналів в комутованій мережі. Протокол STP

забезпечує активну роботу тільки одного логічного шляху між усіма вузлами призначення в мережі, шляхом навмисного блокування резервних шляхів, які могли б викликати петлю. У цій лабораторній роботі команда `show spanning-tree` використовується для спостереження за процесом вибору протоколу STP кореневого мосту. Також ви зможете спостерігати за процесом вибору портів з урахуванням вартості і пріоритету

1.2 Модель мережі

Запустіть або встановіть середовище моделювання Packet Tracer.

Зберіть мережу за схемою, представленою на рисунку 1.2, з основними параметрами комутаційного обладнання та інтерфейсів (табл.1.1). Для цього виконайте наступні дії.

З панелі приладів на робочу ділянку перенести 2 комутатори 2960-24 (для зручності можна їх перейменувати відповідно S1, S2) і 6 комп'ютерів. Для цього на панелі приладів необхідно вибрати перший елемент Network Devices, далі другий елемент - Switches (рис.1.3). Елементи 2960-24 перетягуємо на робочу ділянку.

Теж саме робимо з усім іншим обладнанням, вибираючи потрібне та розміщуючи його на робочій ділянці середовища моделювання Packet Tracer. Комутатори знаходяться на панелі приладів у розділі Network Devices - Switches. Комп'ютери знаходяться в розділі End Devices. Маршрутизатори знаходяться на панелі приладів у розділі Network Devices – Routers.

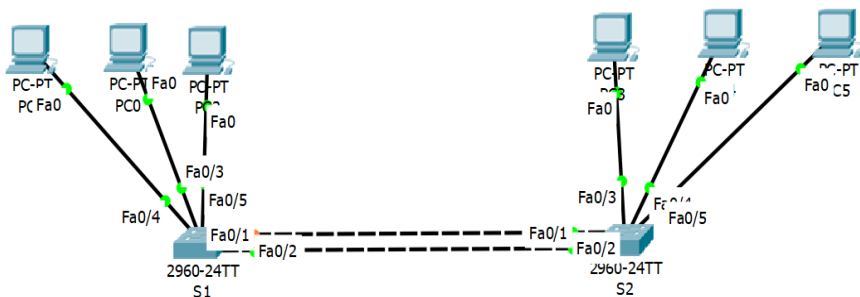


Рисунок 1.2 – Модель мережі

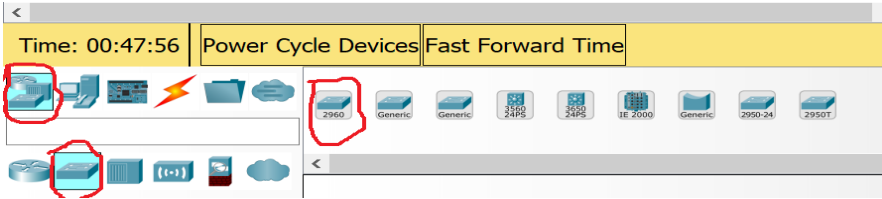


Рисунок 1.3 – Панель обладнання

Таблиця 1.1 – Параметри інтерфейсів

Пристрій	PC	Інтерфейс	ІР-адреса	Маска
S1		Fa0/1	***	255.255.255.0
		Fa0/2	***	255.255.255.0
	PC 2	Fa0/3	192.168.0.2	255.255.255.0
	PC 1	Fa0/4	192.168.0.1	255.255.255.0
	PC 3	Fa0/5	192.168.0.3	255.255.255.0
S2		Fa0/1	***	255.255.255.0
		Fa0/2	***	255.255.255.0
	PC 4	Fa0/3	192.168.0.4	255.255.255.0
	PC 5	Fa0/4	192.168.0.5	255.255.255.0
	PC 6	Fa0/5	192.168.0.6	255.255.255.0

Примітка. Щоб перейменувати елемент моделі мережі, необхідно клацнути лівою кнопкою миші по назві елементу і ввести необхідне ім'я згідно рисунку 1.2. IP-адреси в таблиці вказані для комп'ютерів, підключених до відповідних інтерфейсів комутаторів.

Додайте 3 комп'ютера (до кожного комутатора) і з'єднайте їх з комутаторами консольним кабелем (комп'ютери знаходяться в розділі End Devices).

Тепер необхідно організувати зв'язок між комп'ютерами і комутаторами, зробимо це за допомогою консольного кабелю. З'єднуємо пристрої необхідними кабелями. На панелі інструментів заходимо в розділ Connections (рис.1.3). Вибираємо консольний кабель (рис.1.4, елемент 5). На комутаторі вибираємо порт «Console», а на комп'ютері - «RS 232».

Примітка. Для вибору перехресної або прямої витої пари необхідно натиснути на елементи 3 або 4 (рис.1.4) відповідно.

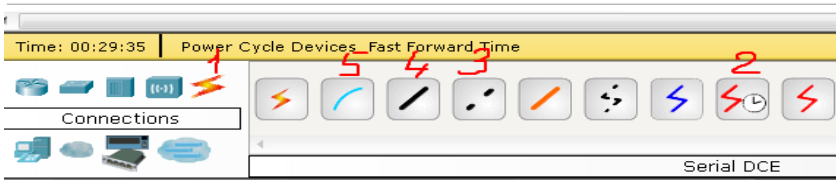


Рисунок 1.4 – Вибір типу кабелю

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

- виберіть відповідний кабель, після чого покажчик миші зміниться;
- далі клікнути лівою кнопкою по першому пристрою, який ви хочете підключити;
- у спливаючому вікні клікніть по порту, до якого підключаєте кабель;
- тепер потрібно задати кінцеву точку підключення кабелю: вибираємо наступний пристрій і аналогічно підключаємо порт (рис.1.5).

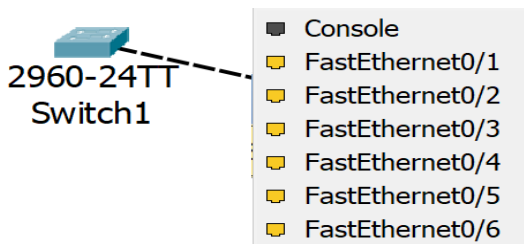


Рисунок 1.5 –Підключення кабелю

Зайдіть в налаштування комутатора у вікно CLI.

Примітка. Подальші команди ми вводимо в цьому вікні – CLI.

Відключіть порти комутаторів, ввівши в кожному терміналі команди:

Switch>**enable**

Switch#**configure terminal**

Switch(config)#**interface range fa0/1-24**

```
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#exit
```

1.3 Основні налаштування комутаторів

Для того, щоб задати ім'я та виконати налаштування комутатора S1 вводимо:

```
Switch#configure terminal
Switch(config)#hostname S1
```

У режим доступу переводимо інтерфейси, до яких безпосередньо підключені комп'ютери. Для цього в терміналі вводимо:

```
S1(config)#interface range fa0/1, fa0/2, fa0/3, fa0/4, fa0/5
S1(config-if-range)#switchport mode access
S1(config-if-range)#no shutdown
```

Для того, щоб задати ім'я та виконати налаштування комутатора S2 вводимо:

```
Switch#configure terminal
Switch(config)#hostname S2
```

У режим доступу переводимо інтерфейси, до яких безпосередньо підключені комп'ютери. Для цього в терміналі вводимо:

```
S1(config)#interface range fa0/1, fa0/2, fa0/3, fa0/4, fa0/5
S1(config-if-range)#switchport mode access
S1(config-if-range)#no shutdown
```

1.4 Вибір кореневого комутатору

Для кожного примірника протоколу spanning-tree (комутуєма мережа LAN або широкомовний домен) існує комутатор, виділений в якості кореневого мосту. Кореневої міст служить точкою прив'язки для всіх розрахунків протоколу spanning-tree, дозволяючи визначити надлишкові шляхи, які слід заблокувати. Процес вибору визначає, який з комутаторів стане кореневим мостом. Комутатор з найменшим значенням ідентифікатора моста (BID) стає кореневим мостом. Ідентифікатор BID складається із значення пріоритету моста, розширеного ідентифікатора системи і MAC-адреси комутатора

(рис.1.6). Значення пріоритету може перебувати в діапазоні від 0 до 65535 з кроком 4096. За замовчуванням використовується значення 32768. При однаковому пріоритеті, корневим стає комутатор з меншим MAC-адресом.

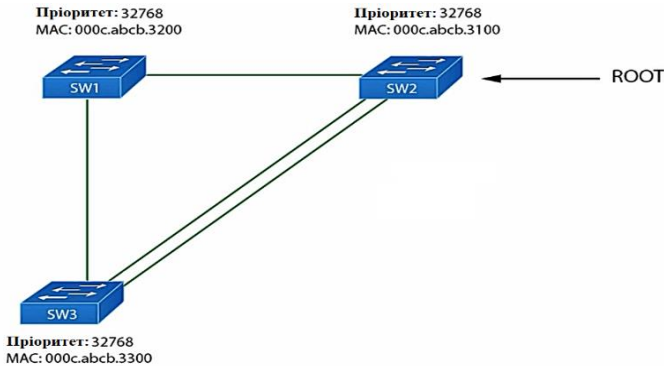


Рисунок 1.6 – Корневий комутатор

Відобразіть данні протоколу spanning-tree (рис. 1.7) на всіх комутаторах. Для кожного з них виконайте наступні дії:

- виберіть комутатор;
- перейдіть у вкладку CLI;
- натисніть клавішу Enter, щоб почати роботу;
- виконайте команди:

> **en**

> **show spanning-tree**

- збережіть скани (фото) усіх CLI комутаторів для представлення викладачу.

В інформації кореневого комутатора написано «This bridge is the root».

Примітка. Режим STP на комутаторі 2960 включений за замовчуванням – протокол STP для кожної мережі VLAN (PVST).

Physical Config CLI Attributes

IOS Command Line Interface

```

Switch>en
Switch#show spa
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address    0006.2A2C.D36C
            This bridge is the root
            Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    0006.2A2C.D36C
            Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/2          Desg FWD 19        128.2   P2p
Fa0/1          Desg FWD 19        128.1   P2p
Fa0/3          Desg FWD 19        128.3   P2p
Fa0/5          Desg FWD 19        128.5   P2p
Fa0/4          Desg FWD 19        128.4   P2p

```

Рисунок 1.7 – Перегляд даних примірника протоколу

1.5 Спостереження за процесом вибору STP порту, виходячи з пріоритету портів

Якщо вартості портів рівні, процес порівнює BID. Якщо BID рівні, для визначення кореневого моста використовуються пріоритети портів. Значення вартості порту за замовчуванням - 128. STP об'єднує пріоритет порту з номером порту, щоб розірвати зв'язки. Найбільш низькі значення є кращими.

Вам потрібно активувати надлишкові шляхи до кожного з комутаторів, щоб переглянути, яким чином протокол STP вибирає порт з урахуванням пріоритету портів.

Для початку треба визначити комутатор з заблокованим портом.

При поточній конфігурації (рис.1.2) тільки один комутатор може містити заблокований протоколом STP порт. Виконайте команду show spanning-tree на комутаторі некореневого мосту. У прикладі нижче (рис 1.8) протокол spanning-tree блокує порт F0/1 на комутаторі з найвищим ідентифікатором BID (S1).

Змініть вартість порта.

Виберіть кореневий комутатор. Виконайте наступні команди в CLI.

> **en**

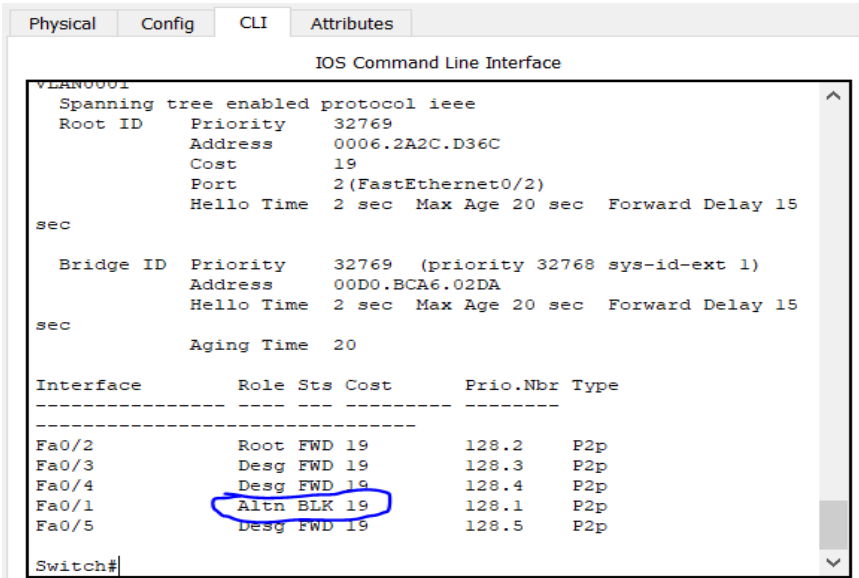
> **conf t**

> **interface fa0/2** (резервний порт)

> **spanning-tree vlan 1 port-priority 144**

Повторно виконайте команду show spanning-tree на обох комутаторах (некорневих мостів). Зверніть увагу, що раніше заблокований порт (S1 - F0/1) тепер є призначеним портом і протокол spanning-tree тепер блокує інший порт S1 - F0/2 (рис. 1.9). Поверніть порту попередню вартість.

Примітка. Протоколи STP потрібно 30 секунд, щоб завершити процес переведення порту.



```

VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address    0006.2A2C.D36C
Cost       19
Port       2 (FastEthernet0/2)
Hello Time 2 sec    Max Age 20 sec    Forward Delay 15
sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
Address    00D0.BCA6.02DA
Hello Time 2 sec    Max Age 20 sec    Forward Delay 15
sec

Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/2          Root FWD 19        128.2   P2p
Fa0/3          Desg FWD 19        128.3   P2p
Fa0/4          Desg FWD 19        128.4   P2p
Fa0/1          Altn BLK 19        128.1   P2p
Fa0/5          Desg FWD 19        128.5   P2p
Switch#
  
```

Рисунок 1.8 – Приклад заблокованого порта

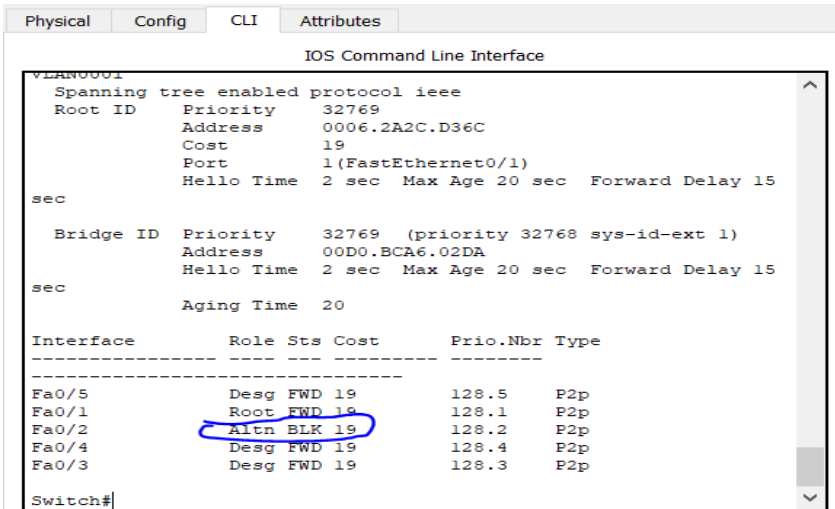


Рисунок 1.9 – Інший заблокований порт

1.6 Перше індивідуальне завдання

Під'єднайте третій Switch і комп'ютер до нього та виконайте налаштування. Встановіть IP-адресу на комп'ютері відповідно до свого варіанту (таб 1.2) та виконайте команду пінг на цю адресу з іншого комп'ютера. Виконайте команду show spanning-tree на Switch (S3).

Таблиця 1.2 – Варіанти завдань

Вар.	IP	PC_7	Вар.	IP	PC_7	Вар.	IP	PC_7	Вар.	IP	PC_7	Вар.	IP	PC_7
1	192.168	.0.7	6	192.168.	0.12	11	192.168.	0.17	16	192.168.	0.22	21	192.168.	0.27
2	192.168	.0.8	7	192.168.	0.13	12	192.168.	0.18	17	192.168.	0.23	22	192.168.	0.28
3	192.168	.0.9	8	192.168.	0.14	13	192.168.	0.19	18	192.168.	0.24	23	192.168.	0.29
4	192.168	.0.10	9	192.168.	0.15	14	192.168.	0.20	19	192.168.	0.25	24	192.168.	0.30
5	192.168	.0.11	10	192.168.	0.16	15	192.168.	0.21	20	192.168.	0.26	25	192.168.	0.31

1.7 Створення мережі 2 і налаштування пристроїв

Зберіть мережу за схемою, представленою на рисунку 1.10. Для цього виконайте такі дії.

З панелі приладів в робочу область перенесіть 4 комутатори 2960-24 (для зручності можна їх перейменувати відповідно S1, S2, S3 та S4), 4 комп'ютери, 1 маршрутизатор та 1 сервер.

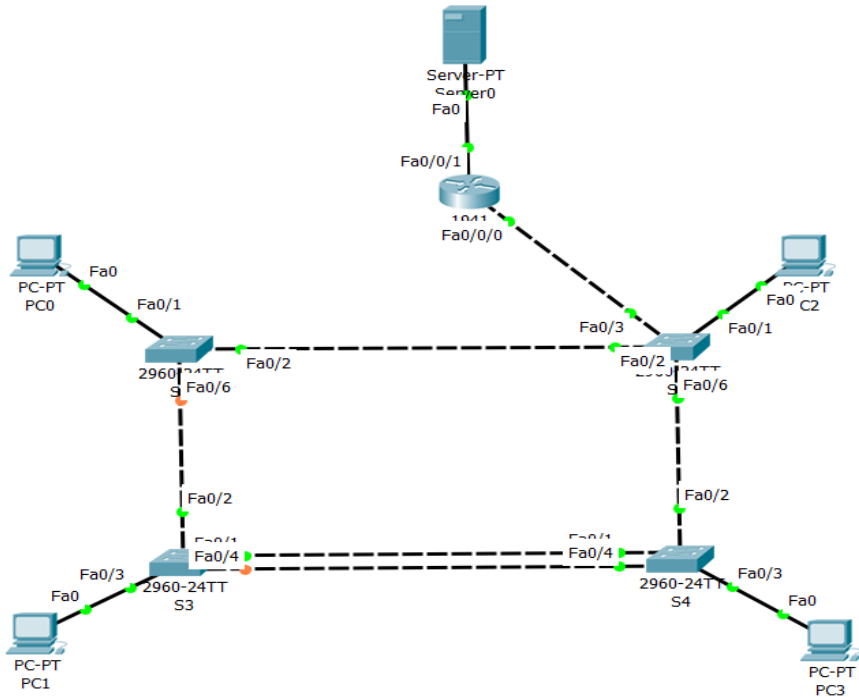


Рисунок 1.10 – Модель мережі 2

З'єднуємо пристрої необхідними кабелями, заходимо в розділ Connections (рис.1.4).

Для налаштування пристроїв скористайтесь адресом мережі **10.0.1.0/24** для серверу і маршрутизатора та **192.168.1.0/24** для маршрутизатора і комп'ютерів.

Відобразіть данні протоколу spanning-tree (рис. 1.11) на всіх комутаторах. Для кожного з них виконайте наступні дії:

- виберіть комутатор;
- перейдіть у вкладку CLI;
- натисніть клавішу Enter, щоб почати роботу;
- виконайте команди:

> **en**

> **show spanning-tree**

- збережіть скани (фото) усіх CLI комутаторів для представлення викладачу.

В інформації кореневого комутатора написано «This bridge is the root».

```
Switch>en
Switch#show spa
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0006.2A2C.D36C
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0006.2A2C.D36C
             Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

             Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/2          Desg FWD 19        128.2    P2p
Fa0/1          Desg FWD 19        128.1    P2p
Fa0/3          Desg FWD 19        128.3    P2p
Fa0/5          Desg FWD 19        128.5    P2p
Fa0/4          Desg FWD 19        128.4    P2p
```

Рисунок 1.11 – Перегляд даних протоколу

Змініть кореневий комутатор. Виконайте на некореновому комутаторі команди.

> **en**

> **conf t**

> **spanning-tree vlan 1 root primary**

В результаті пріоритет зменшиться, а комутатор стане корневим (рис 1.12 та рис 1.13).

```
Switch#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32769
                Address     0001.C78E.9434
                Cost        38
                Port        2 (FastEthernet0/2)
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
sec

                Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
                Address     00D0.BCA6.02DA
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
sec

                Aging Time   20

Interface      Role Sts Cost          Prio.Nbr Type
-----
Fa0/1          Desg FWD 19          128.1    P2p
Fa0/6          Altn BLK 19          128.6    P2p
Fa0/2          Root FWD 19          128.2    P2p
```

Рисунок 1.12 – Дані протоколу до призначення комутатора корневим

```
Switch#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    24577
                Address     00D0.BCA6.02DA
                This bridge is the root
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
sec

                Bridge ID   Priority    24577 (priority 24576 sys-id-ext 1)
                Address     00D0.BCA6.02DA
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
sec

                Aging Time   20

Interface      Role Sts Cost          Prio.Nbr Type
-----
Fa0/1          Desg FWD 19          128.1    P2p
Fa0/6          Desg FWD 19          128.6    P2p
Fa0/2          Desg FWD 19          128.2    P2p
```

Рисунок 1.13 – Дані протоколу після призначення комутатора корневим

Виконайте команду `show spanning-tree` на комутаторі S4. У прикладі (рис 1.10) протокол `spanning-tree` блокує порт F0/4 на комутаторі S3.

Змініть вартість порта. Виберіть комутатор S4. Виконайте наступні команди в CLI.

```
> en
> conf t
> interface fa0/1
> spanning-tree vlan 1 port-priority 112
```

Повторно виконайте команду `show spanning-tree`. Зверніть увагу, що раніше заблокований порт (S1 - F0/4) тепер є призначеним портом і протокол `spanning-tree` блокує інший порт (рис 1.14).

Поверніть порту попередню вартість.

Примітка. Протоколу STP потрібно 30 секунд, щоб завершити процес переведення порту.

```
Switch(config-if)#do show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority      32769
                Address      0001.C78E.9434
                This bridge is the root
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID    Priority      32769  (priority 32768 sys-id-ext 1)
                Address      0001.C78E.9434
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

                Aging Time  20

Interface      Role Sts Cost          Prio.Nbr Type
-----|-----|-----|
Fa0/1          Desg FWD 19           128.1   P2p
Fa0/2          Desg FWD 19           128.2   P2p
Fa0/3          Desg FWD 19           128.3   P2p
Fa0/4          Desg LSN 19           112.4   P2p
```

Рисунок 1.14 –Зміна пріоритету порта

1.8 Друге індивідуальне завдання

Зберіть схему як на рисунку 1.15.

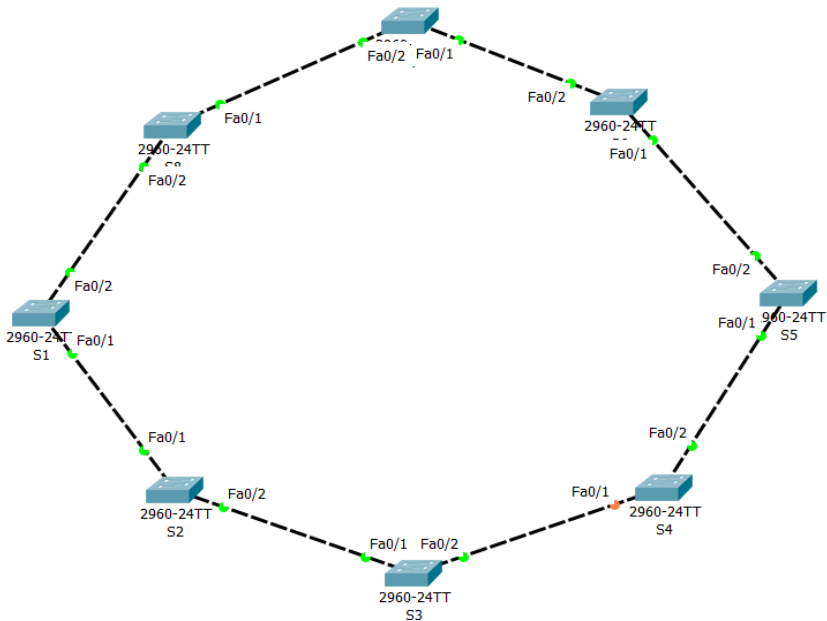


Рисунок 1.15 – Схема для індивідуального завдання 2

Зробіть корневим комутатор згідно варінту (табл. 1.3).

Виконайте команду `show span` до і після призначення комутатора корневим.

Таблиця 1.3 – Варіанти завдань

Вар.	Switch	Вар.	Switch	Вар.	Switch	Вар.	Switch	Вар.	Switch
1	S1	6	S6	11	S3	16	S8	21	S5
2	S2	7	S7	12	S4	17	S1	22	S6
3	S3	8	S8	13	S5	18	S2	23	S7
4	S4	9	S1	14	S6	19	S3	24	S8
5	S5	10	S2	15	S7	20	S4	25	S1

1.9 Зміст звіту

- хід роботи;
- індивідуальні схеми з зазначенням конфігурації інтерфейсів;
- скан (фото) налаштувань комутаторів та результатів роботи протоколу STP;
- відповіді на контрольні питання.

1.10 Контрольні питання

1. Яке значення протокол STP використовує першим після вибору кореневого комутатора, щоб визначити вибір порту?
2. Якщо вартість двох портів однакова, який параметр та його значення використовує протокол STP при виборі порту?
3. Якщо BID на двох портах комутатора рівні, як протокол STP при цьому здійснює вибір порту?

2 ЛАБОРАТОРНА РОБОТА №2

Використання NAT (PAT)

Мета роботи – ознайомитись з правилами адресації внутрішніх та зовнішніх мереж, організувати маршрутизацію з використанням мережевої технології NAT.

2.1 Теоретичні відомості

Трансляція ір NAT, що визначена в RFC 3022, дозволяє вузлу, який не має дійсної, зареєстрованої, глобальної, унікальної IP адреси, здійснювати зв'язок з іншими вузлами через мережі передачі даних. Ці вузли можуть використовувати приватні адреси. Трансляція NAT дозволяє здійснювати зв'язок з вузлами в Інтернет. NAT замінює приватні IP-адреси відкритими зареєстрованими IP-адресами в кожному пакеті протоколу IP. Перетворення мережевих адрес (Network

address translation, NAT) реалізовано програмою, вбудованою в маршрутизатор. Ця програма відіграє роль посередника між приватною мережею та Інтернет - серверами із зареєстрованими адресами. Навіть клієнтські комп'ютери з незареєстрованими адресами можуть відправляти запити серверам Інтернету та одержувати від них відповідь за допомогою NAT. Маршрутизатор NAT також змінює поле з адресою відправника у всіх дейтаграмах, отриманих від комп'ютерів з незареєстрованими IP-адресами та підтримує таблицю незареєстрованих адрес приватної мережі, яка необхідна для відстеження оброблених їм дейтаграм.

У мережі можна використовувати два типи IP-адрес: **зовнішні (зареєстровані, відкриті); внутрішні (приватні).**

Якщо мережа не підключена до Інтернету, в ній можна використовувати адреси будь-якого типу, аби тільки дотримувалася їх унікальність. Бажано використовувати один з діапазонів IP-адрес, спеціально виділених для приватних мереж:

- **10.0.0.0 - 10.255.255.255 (10.0.0.0/8)** - одна мережа класу **A**.
- **172.16.0.0 - 172.31.255.255 (172.16.0.0/12)** - група з 16 суміжних мереж класу **B**.
- **192.168.0.0 - 192.168.255.255 (192.168.0.0/16)** - група з 256 суміжних мереж класу **C**.

Технологія *трансляції мережесвих адрес* дозволяє всім вузлам внутрішньої мережі одночасно взаємодіяти із зовнішніми мережами, використовуючи єдину зареєстровану IP-адресу. Ця модель задовольняє вимогам більшості мереж середніх розмірів для доступу до зовнішніх мереж при використанні єдиної зареєстрованої IP-адреси, отриманої від постачальника послуг.

На рисунку 2.1 наведений приклад, коли внутрішня мережа використовує приватну адресу з діапазону **10.0.0.0/8**.

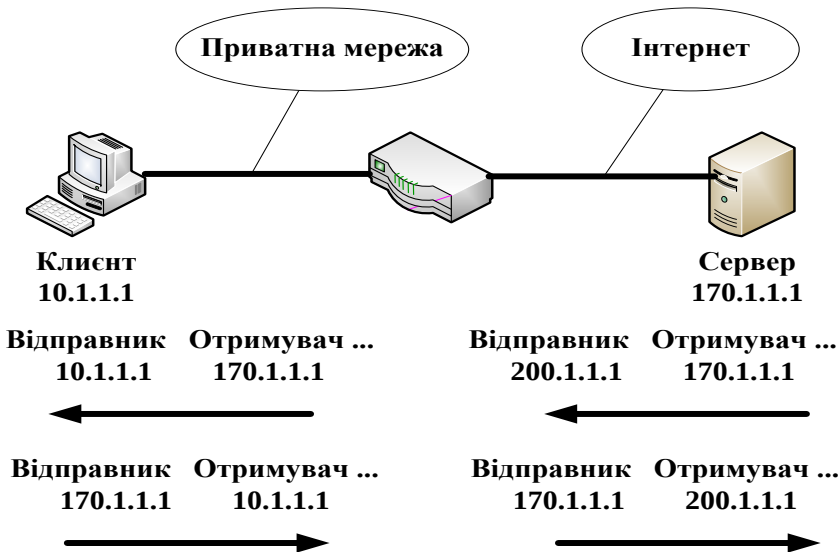


Рисунок 2.1 - Трансляція адрес у технології NAT

Маршрутизатор змінює IP адресу відправника, коли пакет залишає організацію і IP адресу одержувача кожного пакета, який повертається назад у приватну мережу. Функція NAT, яка налаштована на маршрутизаторі, виконує трансляцію адрес.

Коли хост **10.1.1.1** внутрішньої мережі посилає пакет хосту **170.1.1.1** у зовнішню мережу, то він, відправляючи пакет маршрутизатору, як адресу призначення вказує глобальну адресу **170.1.1.1**. Маршрутизатор знає шлях до мережі **170.1.0.0/16**, тому він передає пакет на зовнішній інтерфейс. При цьому пристрій NAT маршрутизатора транслює адресу джерела **10.1.1.1** у глобально унікальну адресу **200.1.1.1**.

Коли одержувач (хост **170.1.1.1**) генерує відповідне повідомлення, то він як адресу призначення вказує єдину зареєстровану глобальну адресу внутрішньої мережі, яка є адресою зовнішнього інтерфейсу пристрою NAT (у даному прикладі це **200.1.1.1**). При надходженні відповідного пакета на пристрій NAT внутрішньої мережі визначається внутрішня IP-адреса вузла. Ця процедура трансляції повністю прозора для кінцевих вузлів.

2.1.1 Статична трансляція NAT

Статична трансляція NAT - IP-адреси перетворюються один в одну статично (рис.2.2).

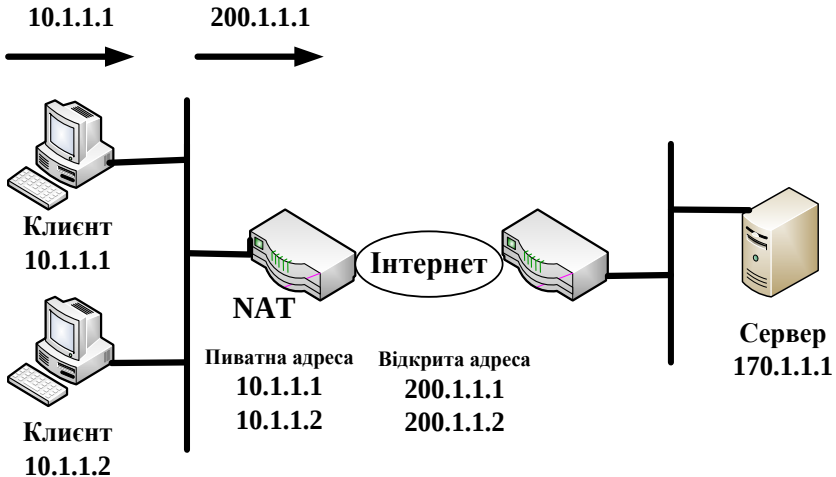


Рисунок 2.2 – Статична трансляція NAT

Розглянемо основні принципи. ISP- провайдер компанії призначає їй зареєстрований номер мережі 200.1.1.0. Маршрутизатор NAT робить так, щоб приватна адреса виглядала таким чином, як ніби вона знаходиться в мережі 200.1.1.0 . Для цього маршрутизатор NAT змінює IP адресу відправника в пакетах.

У даному прикладі маршрутизатор NAT змінює адресу відправника 10.1.1.1 на адресу 200.1.1.1. При використанні статичної трансляції NAT маршрутизатор просто здійснює взаємно однозначне перетворення між приватною та зареєстрованою адресою, від імені якої він виступає. На маршрутизаторі NAT зроблено статичне перетворення приватної адреси 10.1.1.1 у відкриту зареєстровану адресу 200.1.1.1.

Підтримка двох IP- вузлів у приватній мережі вимагає наступного взаємно однозначного перетворення з використанням другої IP- адреси в діапазоні відкритих адрес. Наприклад, для підтримки адреси 10.1.1.2

маршрутизатор просто перетворює адресу 10.1.1.2 на адресу 200.1.1.2. Оскільки підприємство має одну зареєстровану мережу класу С , використовуючи трансляцію NAT, воно може підтримувати до 254 приватних IP- адрес (при цьому зарезервовані дві звичайні адреси - номер мережі та її ширококомовна адреса).

У таблиці NAT приватні IP- адреси наводяться як «приватні», а відкриті, зареєстровані адреси мережі 200.1.1.0 - як «відкриті». Компанія Cisco використовує термін «внутрішні локальні адреси» для приватних IP- адрес і «внутрішні глобальні адреси» для відкритих IP-адрес.

2.1.2 Динамічна трансляція NAT

Динамічна трансляція NAT - маршрутизатор NAT здійснює взаємно однозначне перетворення між внутрішніми локальними і внутрішніми глобальними адресами та змінює IP- адреси в пакетах динамічно.

Динамічна трансляція NAT створює пул можливих внутрішніх глобальних адрес і визначає критерій відповідності для визначення того, які внутрішні глобальні IP- адреси повинні транслюватися за допомогою NAT.

Нижче (рис.2.3) встановлено пул з п'яти глобальних IP-адрес в діапазоні 200.1.1.1 - 200.1.1.5. Трансляція NAT налаштована для трансляції всіх внутрішніх локальних адрес, які починаються з октетів 10.1.1.

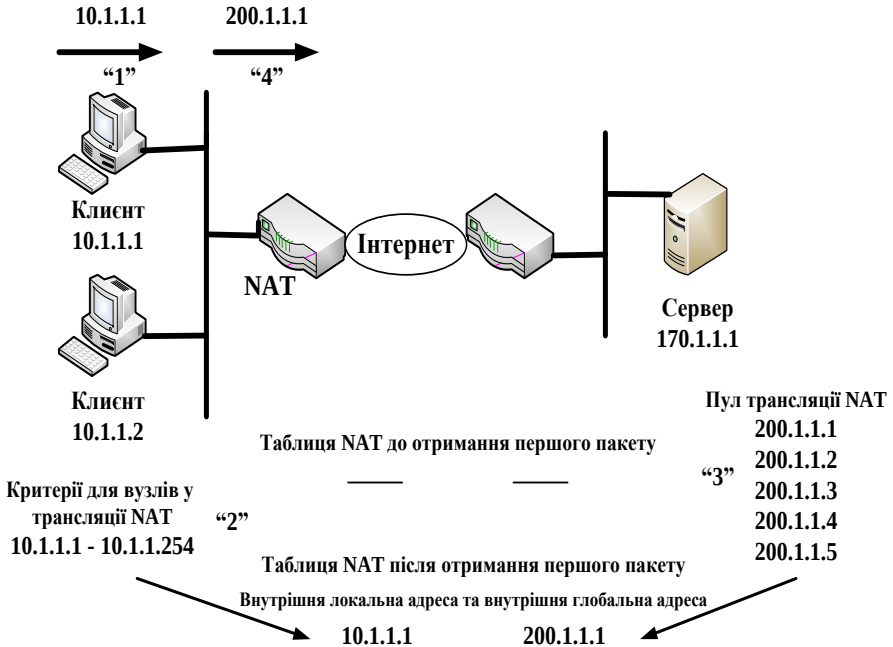


Рисунок 2.3 – Динамічна трансляція NAT

Номери 1, 2, 3 і 4 на рисунку 2.3 відносяться до такої послідовності подій:

- вузол 10.1.1.1 посилає свій перший пакет на сервер, розташований за адресою 170.1.1.1;
- коли пакет поступає на маршрутизатор NAT, маршрутизатор застосовує логіку перевірки відповідності та вирішує, чи слід застосувати до цього пакету трансляцію NAT. Оскільки логіка маршрутизатора налаштована на відповідність IP-адресам відправника, які починаються з 10.1.1, маршрутизатор додає запис в таблицю NAT для адреси 10.1.1.1 в якості внутрішньої адреси;
- маршрутизатору NAT потрібно виділити IP адресу з пулу дійсних внутрішніх глобальних адрес. Він вибере першу доступну адресу (в даному випадку 200.1.1.1) і додасть її в таблицю NAT для завершення запису;

– маршрутизатор NAT трансліює IP адресу відправника і пересилає пакет.

Динамічний запис залишається в таблиці поки триває передача даних. Можна задати значення тайм- ауту, який визначає, як довго повинен чекати маршрутизатор поки не трансліюються пакети з такою адресою, перед видаленням цього динамічного запису.

Трансляція NAT може бути налаштована з великою кількістю IP-адрес у списку внутрішніх локальних адрес, ніж в пулі внутрішніх глобальних адрес. Маршрутизатор виділяє адреси з пулу до тих пір, поки всі вони не будуть виділені.

Якщо надходить новий пакет від ще одного внутрішнього вузла і йому потрібен запис NAT, а всі IP- адреси, які знаходяться в пулі, вже використовуються, то маршрутизатор просто відкидає цей пакет. Користувач повторює спробу до тих пір, поки не закінчиться час тайм-ауту для запису NAT, в цей момент функція NAT працює для наступного вузла, який відправляє пакет.

Розмір внутрішнього глобального пулу адрес повинен відповідати максимальній кількості конкуруючих вузлів, яким потрібен одночасний доступ до мережі інтернет (крім випадку використання трансляції NAT) .

2.2 Організація автономного домену **rmf....domain01. local**

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання роботи на комп'ютерах з фізичними іменами **RMF01, RMF02 і RMF03.**

Для цих комп'ютерів маємо:

– при завантаженні на них клієнтської ОС **MS Windows 7:**

- 1) IP-адреси: **10.0.9.51, 10.0.9.52 і 10.0.9.53** відповідно;
- 2) мережеві імена: **rmf51, rmf52 і rmf53** відповідно;

– при завантаженні на них серверної ОС **Microsoft Windows Server 2008:**

- 1) IP-адреси: **10.0.9.151, 10.0.9.152 і 10.0.9.153** відповідно;
- 2) мережеві імена: **rmf151, rmf152 і rmf153** відповідно;
- 3) повні імена: **rmf151.domain01.local, rmf152.domain02.local і**

rmf153.domain03.local відповідно.

Так як більшість з вас працює за комп'ютерами з іншими фізичними іменами, то при виконанні роботи вам доведеться використовувати відповідно інші IP-адреси, короткі і повні мережеві імена.

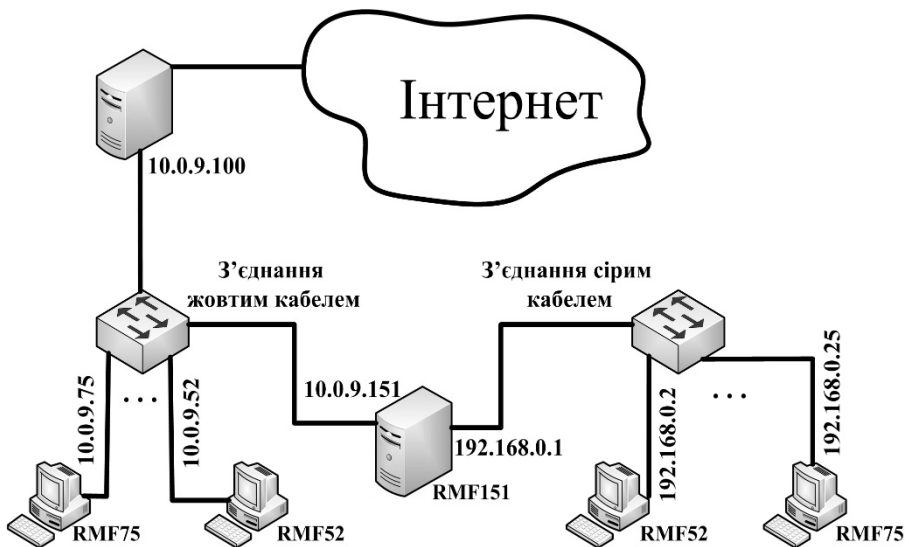


Рисунок 2.4 – Комп'ютерна мережа з підмережею з використанням комутаторів

На рисунку 2.4 наведена комп'ютерна мережа:

- мережа **10.0.9.0/24** - відповідає з'єднанню **жовтого кабелю** (до складу підмережі включені сервер (**10.0.9.100**) комп'ютери з фізичними іменами **RMF01**, ..., **RMF25** і комутатор);
- підмережа **192.168.0.0/24** - відповідає з'єднанню **сірого кабелю** (до складу підмережі включені комп'ютери з фізичними іменами **RMF01**, ..., **RMF25** і комутатор);
- функції маршрутизатора виконує комп'ютер **RMF01** (фізичне ім'я).

IP-адреси комп'ютерів основної мережі, які вказані на рисунку, відповідають завантаженню на комп'ютері з фізичним ім'ям **RMF01** ОС

Microsoft Windows Server 2008, а на комп'ютерах з фізичними іменами **RMF02, ..., RMF25** - ОС **Microsoft Windows 7**.

На рисунку 2.5 наведена комп'ютерна мережа **10.0.9.0/24** з підмережею **192.168.0.0/24**, у складі якої всього лише одна робоча станція (**RMF02**).

IP-адреси комп'ютерів основної мережі, які вказані на рисунку, відповідають завантаженню на комп'ютері з фізичним ім'ям **RMF01** ОС **Microsoft Windows Server 2008**, а на комп'ютері з фізичним ім'ям **RMF03** - ОС **Microsoft Windows 7**.

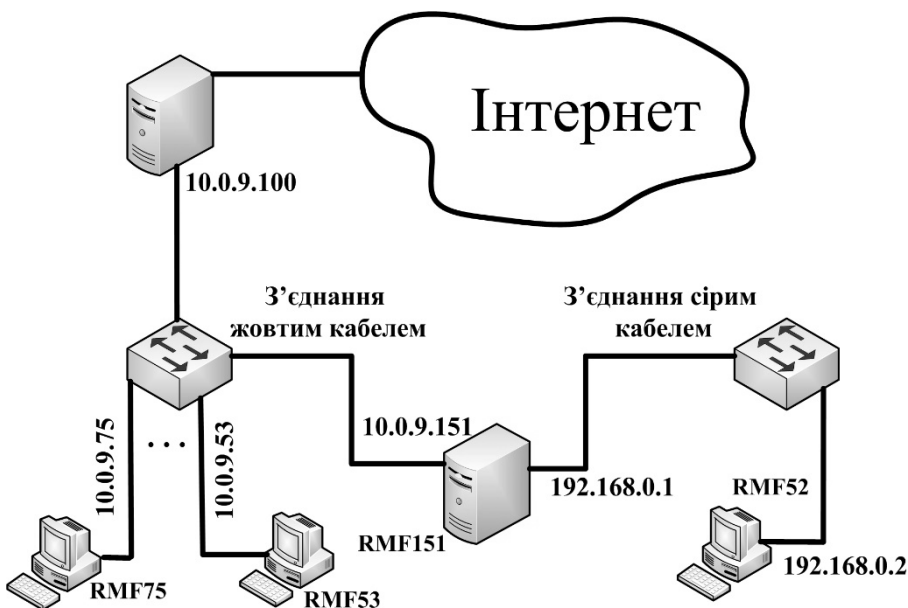


Рисунок 2.5 – Робоча схема мережі

Зберіть робочу схему мережі згідно рисунку 2.5:

На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні операції:

- завантажте ОС **Microsoft Window Server 2008** (користувач – **Адміністратор**, Пароль – **1q2w3e4r&** або **1q2w3e4r5t& (RU)**);
- настройте мережевий інтерфейс верхнього адаптера (інтерфейс із підмережею **192.168.0.0/24**):

Пуск => Панель управления => Сеть и интернет (якщо режим просмотра Категория) => Центр управления сетями и общим доступом;

– в лівій частині вікна натисніть по **Изменение параметров адаптера** натисніть правою кнопкою миші по **Подключение по локальной сети 2 (сірий кабель) => виберіть Свойства => виділіть Протокол Интернета версии 4 (TCP/IPv4) => натисніть Свойства;**

– установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: 192.168.0.1

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.9.151 (у вас, відповідно, інша адреса)

Предпочитаемый DNS-сервер: 10.0.9.151 (у вас, відповідно, інша адреса)
натисніть **ОК**.

Перевірте налаштування мережевого інтерфейсу нижнього адаптера (інтерфейс із мережею **10.0.9.0/24**);

– перебуваючи у вікні **Сетевые подключения**, натисніть правою кнопкою миші **Подключение по локальной сети (жовтий кабель) => виберіть Свойства => виділіть Протокол Интернета версии 4 (TCP/IPv4) => натисніть Свойства;**

– установіть наступні параметри:

IP-адрес: 10.0.9.151 (у вас, відповідно, інша адреса)

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.9.100

Предпочитаемый DNS-сервер: 10.0.2.1

і натисніть **ОК**.

Створіть користувача **Active Directory**:

– **Пуск => Администрирование => Active Directory – пользователи и компьютеры;**

– розкрийте список вузла вашого сервера (якщо він не розкритий);

– натисніть ліворуч правою кнопкою миші по **Users** і виберіть **Создать => Пользователь;**

– у вікні **Новый объект-Пользователь:**

– у полі **Имя** введіть **user1;**

- у полі **Имя входа пользователя** введіть **user1**;
- натисніть **Далее**;
- у вікні **Новый объект-Пользователь**:
- у полі **Пароль** введіть **1q2w3e4r5t&** або **1q2w3e4r& (RU)** (залежно від паролю адміністратора));
- у полі **Подтверждение** введіть **1q2w3e4r5t&** або **1q2w3e4r& (RU)**;
- установіть прапорець **Запретить смену пароля пользователем**;
- установіть прапорець **Срок действия пароля не ограничен**;
- натисніть **Далее**;
- натисніть **Готово**;
- закрийте вікно **Active Directory – пользователи и компьютеры**.

На комп'ютері з фізичним ім'ям **RMF02** виконайте наступні дії:

- завантажте ОС **Microsoft Windows 7** (Користувач – **admin**, Пароль – **1234567**);

- настройте мережевий інтерфейс:

Пуск => Панель управления => Сеть и интернет (якщо режим просмотра **Категория**) **=> Центр управления сетями и общим доступом**;

- в лівій частині вікна натисніть по **Изменение параметров адаптера** натисніть правою кнопкою миші по **Подключение по локальной сети 2 (сірий кабель)** **=> виберіть Свойства => виділіть Протокол Интернета версии 4 (TCP/IPv4) => натисніть Свойства**;

- установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: 192.168.0.2

Маска подсети: 255.255.255.0

Основной шлюз: 192.168.0.1

Предпочитаемый DNS-сервер: 192.168.0.1 (10.0.2.1) (у вас, відповідно, інша адреса) і натисніть **ОК**,

- закрийте вікно **Сетевые подключения**.

Підключіть комп'ютер з мережевим ім'ям **rmf52** до домену **domain01.local**, тобто до домену, у котрому контролером домену є комп'ютер з фізичним ім'ям **RMF01**:

- **Мой компьютер** (правою кнопкою миші) **=> Свойства => у**

розділі **Имя компьютера, имя домена и параметры рабочей группы** натисніть **Изменить параметры** => натисніть кнопку **Изменить...**;

- у вікні **Изменение имени компьютера или домена** виберіть опцію **Является членом домена**, у текстовому полі впишіть **domain01.local** (у вас, відповідно, інше ім'я домена), натисніть **ОК**,

- у вікні **Имя и пароль пользователя в домене**:

- 1) у полі **Пользователь** введіть **Администратор**;

- 2) у полі **Пароль** введіть **1q2w3e4r&** або **1q2w3e4r5t& (RU)**;

- натисніть **ОК**;

- через деякий час відкриється вікно з запрошенням в домен **domain01.local**, натисніть **ОК**;

- погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши **ОК** (при цьому ви вертаєтесь у вікно **Свойства системы**), натисніть **Закреть**, потім – **Да**;

- після перезавантаження комп'ютера (не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему за трьома параметрами:

Користувач – **user1**;

Пароль – **1q2w3e4r5t&** або **1q2w3e4r& (RU)**;

Вхід в – **DOMAIN01** (у вас, відповідно, буде “своє” ім'я домену).

2.3 Налаштування NAT-серверу та перевірка його працездатності

На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні операції:

- запустіть службу **Брандмауэр Windows**;

- **пуск => Администрирование => Службы**;

- в правій частині натисніть правою кнопкою миші по пункту **Брандмауэр Windows => Свойства**;

- встановіть **Тип запуска => Авто**;

- якщо служба ще не запущена, запустіть її – натисніть на кнопку **=> Запустить**;

- натисніть **=> ОК**;

- закрийте вікно **=> Службы**;

- додайте роль **=> Службы политики сети и доступа**;

- **пуск => Администрирование => Диспетчер сервера;**
 - в лівій частині вікна виберіть пункт **Роли**;
 - в правій частині вікна натисніть **=> Добавить роли**, відкриється **Мастер добавления ролей**;
 - якщо першою сторінкою є **Перед началом работы**, пропускаємо її, натисніть **Далее**;
 - на сторінці **Роли сервера** встановіть прапорець **Службы политики сети и доступа => Далее**;
 - пропускаємо сторінку **Службы политики сети и доступа**, натисніть **Далее**;
 - на сторінці **Службы ролей** встановіть прапорець **Службы маршрутизации и удаленного доступа => Далее**;
 - підтвердить обрані налаштування, натисніть **Установить**;
 - по завершенні установки натисніть **Закрыть**;
 - закрийте вікно **Диспетчер сервера**.
- Запустіть службу Маршрутизация и удаленный доступ:**
- **пуск => Администрирование => Маршрутизация и удаленный доступ**;
 - на лівій панелі виділіть рядок **Состояние сервера**. Праворуч відобразиться його статус: **зупинений** або **запущенный**. Якщо він **зупинений** (на його значку присутня червона стрілка), то натисніть на ньому (на записі **RMF151** (локально)) правою кнопкою миші й виберіть **Настроить и включить маршрутизацию и удаленный доступ**;
 - натисніть **Далее**;
 - у вікні **Конфигурация** виберіть опцію **Преобразование сетевых адресов (NAT)** і натисніть **Далее**;
 - у вікні **Подключение к Интернету на основе NAT** виберіть опцію **Использовать общедоступный интерфейс для подключения к Интернету** та оберіть мережевий інтерфейс **Внешняя сеть**, натисніть **Далее**;
 - натисніть **Готово**;
 - закрийте вікно **Маршрутизация и удаленный доступ**.
- Перевірте мережеві підключення за допомогою команди **ping**:
- на комп'ютері **RMF02** виконайте **Пуск => Все программы => Стандартные => Командная строка**;

– виконайте команди **ping 192.168.0.1** і **ping 10.0.9.151** (у вас, відповідно, інша адреса). Обидві команди повинні виконатися коректно (Пакетов: отправлено = 4, получено = 4, потеряно = 0);

– закрийте вікно **Командная строка**.

Перевірте працездатність протоколу NAT за допомогою мережевого монітора:

– на комп'ютері **RMF01** установіть мережевий монітор:

– **пуск => Все программы => Стандартные => Выполнить;**

– у рядку **Открыть** введіть: **“C:\Install\NetworkMonitor\NM32_x86.exe”** та натисніть **ОК**;

– натисніть **Да**;

– натисніть **Next**;

– погоджуйтесь із ліцензійним погодженням, оберіть **I accept the terms in the License Agreement**, натисніть **Next**;

– оберіть пункт **I do not want to use Microsoft Update**, натисніть **Next**;

– натисніть **Typical**;

– натисніть **Install**;

– по завершенні установки натисніть **Finish**.

Виконайте перехоплення кадрів:

– на комп'ютері **RMF03**:

– завантажте ОС Windows 7 (Користувач – **admin**, Пароль – **1234567**);

– перевірте налаштування мережевого інтерфейсу, воно повинно бути наступним:

IP-адрес: 10.0.9.53 (у вас, відповідно, інша адреса)

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.9.100

Предпочитаемый DNS-сервер: 10.0.2.1

– створіть спільний мережевий ресурс:

– **Мой компьютер => диск C => папка TEMP** (при її відсутності - створіть);

– скопіюйте в папку **C:\TEMP** будь-який файл невеликого розміру;

– натисніть правою клавішею миші на папці **C:\TEMP** і виберіть **Общий доступ => Конкретные пользователи**;

- у верхньому рядку оберіть варіант **Все**, натисніть **Добавить**;
- натисніть => **Общий доступ**;
- натисніть => **Готово**.

На комп'ютері **RMF01** визначте фізичну адресу мережевого адаптера для зовнішньої мережі:

- **Пуск => Выполнить**;
- у полі **Открыть** впишіть **cmd** і натисніть **ОК**;
- у вікні, яке відкрилося, виконайте команду **ipconfig /all**;
- прочитайте фізичну адресу адаптера для **Подключение по локальной сети** і запишіть її;
- закрийте вікно **F:\SERVER\System32\cmd.exe**;
- на комп'ютері **RMF01** запусить процес перехоплення кадрів:
- **Пуск => Все программы => Microsoft Network Monitor 3.4 => Microsoft Network Monitor 3.4**;
- якщо відкрилося вікно **Microsoft Update Opt-In**, то зніміть прапорець **Periodically check for updates when Network Monitor starts**, та натисніть **No**;

- натисніть **File => New => Capture**;
- натисніть **Capture => Start**.

З комп'ютера **RMF02** (фізичне ім'я) запросіть інформацію на комп'ютері **RMF03** (фізичне ім'я):

- **Пуск => Все программы => Стандартные => Выполнить**;
- у полі **Открыть** впишіть **\\10.0.9.53\temp** (у вас, відповідно, інша адреса) і натисніть **ОК**;
- з вікна **temp на 10.0.9.53** скопіюйте файл **GHOSTERR** або **інший** на робочий стіл комп'ютера; це запусить трафік у мережі, який і буде перехоплений мережним монітором;
- закрийте вікно **temp на 10.0.9.53**;
- на комп'ютері **RMF01** (фізичне ім'я) зупиніть процес перехоплення кадрів (**Capture => Stop**);
- на комп'ютері **RMF01** (фізичне ім'я) перегляньте перехоплені дані, які перебувають у буфері;
- перелік перехоплених кадрів можна побачити у вікні **Frame Summary**;
- для перегляду вмісту окремого кадру натисніть мишею на будь-якому (можна першому в переліку) кадрі, де адреса відправника

(див. колонку **Source**) дорівнює IP-адресі комп'ютера **RMF03** (тобто **10.0.9.53**; у вас, відповідно, інша адреса);

- у вікні **Frame Details** розкрийте значок + поруч із назвою протоколу IPv4 і знайдіть у заголовку дейтаграми поле з адресою відправника (**Source Address**) і поле з адресою одержувача (**Destination Address**), запишіть ці адреси (це будуть наступні адреси: **10.0.9.53** і **10.0.9.151**; у вас, відповідно, “свої”);

- розкрийте значок + поруч із назвою протоколу TCP і знайдіть у заголовку сегмента TCP поле с номером порту відправника (**SrcPort**) і поле з номером порту одержувача (**DstPort**), запишіть ці номери портів;

- **переконайтесь** що комп'ютер **RMF03** не знає IP- адресу комп'ютера **RMF02**, який знаходиться в підмережі, а знає тільки IP-адресу та порт комп'ютера **RMF01** (тобто **10.0.9.151**; у вас, відповідно, інша адреса), якому він і пересилав кадри. Служба NAT на комп'ютері **RMF01** виконувала пересилання кадрів на комп'ютер **RMF02** (структура внутрішньої мережі (**192.168.0.0/24**) від комп'ютерів у зовнішній мережі схована);

- закрийте значок “мінус” (-) поруч с назвою протоколу TCP;
- закрийте значок “мінус” (-) поруч с назвою протоколу IPv4;
- закрийте вікно **Microsoft Network Monitor 3.4 ...** (без збереження зібраних даних і без збереження бази даних адрес).

2.4 Відновлення комп'ютерів в початковий стан

(даний розділ підлягає обов'язковому виконанню!)

На комп'ютері з фізичним ім'ям **RMF03** виконайте наступні дії:

- видаліть з папки **C:\TEMP** файл;
- зніміть спільний доступ до папки **C:\TEMP**:

- 1) натисніть правою клавішею миші на папці **C:\TEMP**, виберіть **Свойства**;

- 2) у вікні **Свойства** перейдіть до вкладки **Доступ**, натисніть **Расширенная настройка**, зніміть прапорець **Открыть общий доступ к этой папке**, клацніть **ОК** потім **Закрыть**;

- закрийте вікно **C**;

– перезавантажите комп'ютер із завантаженням ОС, яка встановлюється за замовчуванням.

На комп'ютері з фізичним ім'ям **RMF02** виконайте наступні дії:

– видаліть з робочого стола комп'ютера файл **GHOSTERR** (або інший, який був скопійований з комп'ютера **RMF03**);

– відключіть цей комп'ютер від домену **domain01.local**:

Мой компьютер (правою кнопкою миші) => **Свойства** => у розділі **Имя компьютера, имя домена и параметры рабочей группы** натисніть => **Изменить параметры** => натисніть кнопку **Изменить...**;

– у вікні => **Изменение имени компьютера или домена**:

1) виберіть опцію => **Является членом рабочей группы**;

2) у текстовому полі впишіть **WORKGROUP**;

3) натисніть **Дополнительно**;

4) у вікні **DNS-суффикс и NetBIOS-имя компьютера** у текстовому полі видаліть DNS-суфікс **domain01.local** (у вас, відповідно, “свій” DNS-суфікс), зробіть чистим текстове поле, і натисніть => **ОК**;

5) с поверненням у вікно => **Изменение имени компьютера или домена** натисніть => **ОК**;

– через деякий час відкриється вікно **Сетевая идентификация** із запрошенням в робочу групу, натисніть => **ОК**;

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши => **ОК**;

– у вікні **Свойства системы** натисніть => **ОК**.

Важливо!!! Якщо вікно **Изменение имени компьютера или домена** не є активним, змініть Користувача:

– у полі **Пользователь** введіть:

DOMAIN01\Администратор (у вас, відповідно, буде “своє” ім'я домену);

– у полі **Пароль** введіть **1q2w3e4r&** або **1q2w3e4r5t&** (RU);

– натисніть **ОК**;

– потім виконайте відключення від домену **domain01.local**.

Перевірте, що комп'ютер з фізичним ім'ям **RMF02** відключено від домену **domain01.local**.

– після перезавантаження комп'ютера (не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему за двома параметрами:

Користувач – **admin**;

Пароль – **1234567. Да**;

– відновіть початковий стан мережевого інтерфейсу (верхньої мережевої плати);

– **Пуск => Панель управління => Сеть и интернет** (якщо режим просмотра **Категория**) => **Центр управления сетями и общим доступом**;

– в лівій частині вікна натисніть => **Изменение параметров адаптера** натисніть правою кнопкою миші => **Подключение по локальной сети 2** => виберіть **Свойства** => виділіть **Протокол Интернета (TCP/IP)** => натисніть **Свойства**;

– установіть опції => **Получить IP–адрес автоматически** і **Получить адрес DNS–сервера автоматически** і натисніть => **ОК**;

– з поверненням у вікно **Подключение по локальной сети** => **Свойства** натисніть => **ОК**;

– з поверненням у вікно **Сетевые подключения** закрийте його;

– перезавантажте комп'ютер із завантаженням ОС, яка установлюється за замовчуванням.

На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні дії:

– відновіть налаштування мережевого інтерфейсу верхнього адаптера (**сірий кабель**):

– **Пуск => Панель управління => Сеть и интернет** (якщо режим просмотра **Категория**) => **Центр управления сетями и общим доступом**;

– в лівій частині вікна натисніть => **Изменение параметров адаптера** натисніть правою кнопкою миші => **Подключение по локальной сети 2** => виберіть **Свойства** => виділіть **Протокол Интернета (TCP/IP)** => натисніть **Свойства**;

– установіть опції:

Получить IP–адрес автоматически і **Получить адрес DNS–сервера автоматически** і натисніть => **ОК**;

– натисніть **ОК**;

– закрийте вікно **Сеть и удаленный доступ к сети**;

– видаліть роль **Службы политики сети и доступа**;

1) **Пуск => Администрирование => Диспетчер сервера**;

2) на лівій панелі натисніть правою кнопкою миші => **Роли**;

3) у вікні => **Роли** натисніть => **Удалить роли**;

4) якщо першою сторінкою майстра є => **Перед началом работы**, натисніть => **Далее**;

5) У вікні => **Удаление ролей сервера** зніміть прапорець => **Службы политики сети и доступа**;

6) натисніть **Далее**;

7) натисніть **Удалить**;

Видаліть мережевий монітор:

– **Пуск** => **Панель управления** => **Программы и компоненты**;

– у вікні **Программы и компоненты** => виділіть **Microsoft Network Monitor 3.4** і => натисніть **Удалить**;

– натисніть **Да**;

– закрийте вікно **Программы и компоненты**;

– закрийте вікно **Панель управления**.

Видаліть реєстраційний запис комп'ютера **RMF02** у домені **domain01.local**:

– **Пуск** => **Администрирование** => **Active Directory – пользователи и компьютеры**;

– с відкриттям вікна **Active Directory – пользователи и компьютеры** натисніть на значку + у рядку **domain01.local** (у вас, відповідно, “своє” ім'я);

– виділіть **Computers**;

– на полі праворуч натисніть правою кнопкою миші на записі **rmf52 Компьютер** (у вас, відповідно, аналогічний запис) і виберіть **Удалить**, потім – **Да**;

– закрийте вікно **Active Directory – пользователи и компьютеры**;

– перезавантажте комп'ютер із завантаженням ОС, яка встановлюється за замовчуванням.

2.5 Зміст письмового звіту

– теоретичні відомості;

– загальні схеми;

– хід роботи;

- відповіді на контрольні питання.

2.6 Контрольні питання

1. Причини використання технології NAT?
2. Пули IP-адрес, які зарезервовані для адресації в приватних мережах?
3. Статична трансляція NAT. Приклад.
4. Динамічна трансляція NAT. Приклад.

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. Моримото Р. Microsoft Exchange Server 2013. Полное руководство / Р. Моримото, М. Ноэл, Г. Ярдени, К. Амарис, Э. Аббейт // Пер. с англ. – М.: ООО "И.Д. Вильямс", 2014. – 800 с.
5. Методичні вказівки до проходження професійного тесту «Загальні поняття мережної взаємодії. Технології та стандарти локальних мереж» з дисципліни "Комп'ютерні мережі" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Частина 1 / Укл. Г.Г. Киричек. – Запоріжжя: ЗНТУ, 2017. – 38 с.
6. Методичні вказівки до проходження професійного тесту «Загальні поняття мережної взаємодії. Технології та стандарти локальних мереж» з дисципліни "Комп'ютерні мережі" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Частина 2 / Укл. Г.Г. Киричек. – Запоріжжя: ЗНТУ, 2017. – 38 с.
7. 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.