Лабораторна робота №4.
Віртуальні локальні мережі VLAN

Мета роботи: Опанувати розбиття локальної мережі на декілька віртуальних локальних мереж з використанням пристроїв компанії Cisco.

Методичні вказівки

На сьогодні локальні мережі прийнято будувати на основі технології комутованого *Ethernet* - тому є тенденція до мінімізації кількості концентраторів (*хабів - hub*), а намагаються використовувати переважно комутатори (*світч - switch*). У комутаторі між приймачем та передавачем на час з'єднання утворюється віртуальний канал (*virtual circuit*) точка-точка (*point-to-point*). Така мережа може бути розглянута як сукупність незалежних пар приймач-передавач, кожна з яких використовує всю смугу пропускання.

Якщо комутатору необхідно передати пакет на вихідний порт, який зайнятий, то пакет поміщається в буферну пам'ять. Це дозволяє узгодити швидкості передавачів і приймачів пакетів.

Для відправки фрейму через комутатор використовуються два методи. Відправлення з проміжним зберіганням (*store-and-forward*): при цьому пакет повинен бути прийнятий повністю до того як буде розпочата його відправка; наскрізний метод (*cut-through*): комутатор приймає початок пакета, зчитує в ньому адресу пункту призначення та починає відправляти пакет ще до його повного отримання.

Ethernet-комутатор одержує *MAC*-адреси пристроїв в мережі за допомогою читання адрес джерел у прийнятих пакетах, далі він запам'ятовує у своїх внутрішніх таблицях інформацію на які порти та з яких *MAC*-адрес приходять пакети. При підключенні до одного порту декількох пристроїв через концентратор (*hub*) в таблиці одному порту буде відповідати декілька *MAC*-адрес. Таблиці зберігаються в пам'яті (content-addressable memory, CAM): якщо адреса відправника відсутня у таблиці, то вона туди заноситься. Поряд з парами адреса-порт в таблиці зберігається і мітка часу, яка в записі таблиці змінюється або при приході на комутатор пакета з такою ж адресою, або при зверненні комутатора за цією адресою. Якщо рядок таблиці не використовувався певний період часу, то він вилучається. Це дозволяє комутатору підтримувати правильний список адрес пристроїв для передачі пакетів.

Використовуючи *MAC*-таблицю адрес та адресу одержувача, який міститься в пакеті, що прийшов, комутатор організовує віртуальне з'єднання між портом відправника та портом одержувача і передає пакет через це з'єднання. Віртуальне з'єднання між портами комутатора зберігається протягом передачі одного пакета, тобто для кожного пакета віртуальне з'єднання організується заново на основі адреси одержувача, що міститься в цьому пакеті.

Оскільки пакет передається тільки в той порт, до якого підключений адресат, інші пристрої підключені до комутатора, не отримають цей пакет. У комутаторах *Ethernet* передача даних між будь-якими парами портів відбувається незалежно - тому для кожного віртуального з'єднання виділяється вся смуга каналу. При передачі широкомовного пакета в комутаторі утворюється «веер» каналів за принципом один до багатьох. Прикладами джерел широкомовного трафіку є *ARP* та маршрутизуючі протоколи.

Комутатори можна з'єднувати один з одним. При цьому група попарно прямо або побічно пов'язаних комутаторів утворює один логічний комутатор з теоретично довільним числом портів. Тобто комутатори дозволяють створювати теоретично як завгодно велику локальну мережу. Правильне поєднання комутаторів, тобто вибір топології мережі становить одну з найважливіших задач проектування локальних мереж. Рекомендується здійснювати

з'єднання комутаторів по шарах (рис.1), як наприклад: серверний шар, шар розподілу (*distribution*) та шар доступу (*access*). Рядові комп'ютери підключаються до шару доступу, а сервери до серверного шару.

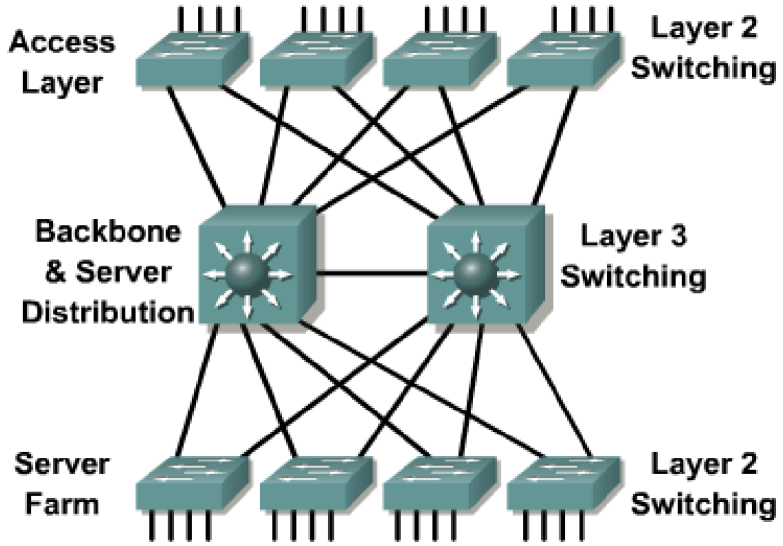

Рис.1

Головною перешкодою для створення великих локальних мереж за допомогою одних тільки комутаторів є нелінійний ріст обсягу широкомовного трафіку, який виникає з ростом кількості пристроїв у мережі. Якщо у мережі кількість пристроїв становить більше ніж 2000 (за іншими оцінками 500, за третіми 4000 - все залежить від топології мережі та класу вирішуваних задач) обсяг широкомовного трафіку різко зростає і додавання нових пристроїв різко знижує продуктивність мережі.

Наприклад, якщо в мережі з кількох тисяч пристроїв один з комп'ютерів *A* вперше здійснює *IP*-з'єднання з іншим комп'ютером *B* у цій мережі, то він повинен попередньо послати до всіх пристроїв мережі широкомовний *ARP*-запит для визначення *MAC*-адреси комп'ютера *B*.

Локальна мережа, яка створена за допомогою одних тільки комутаторів, представляє один широкомовний домен. Зменшити такий домен можна, фізично розділивши локальну мережу на незалежні підмережі (незалежні групи попарно пов'язаних комутаторів) і з'єднати їх в єдине ціле з використанням маршрутизаторів. Таке завдання можна вирішити тільки на етапі побудови мережі, але не в момент її експлуатації. Тут на допомогу приходять віртуальні локальні мережі *VLAN* (*virtual local area network*).

Віртуальна локальна мережа *VLAN* — це сукупність портів одного або більше комутаторів (рис. 2).

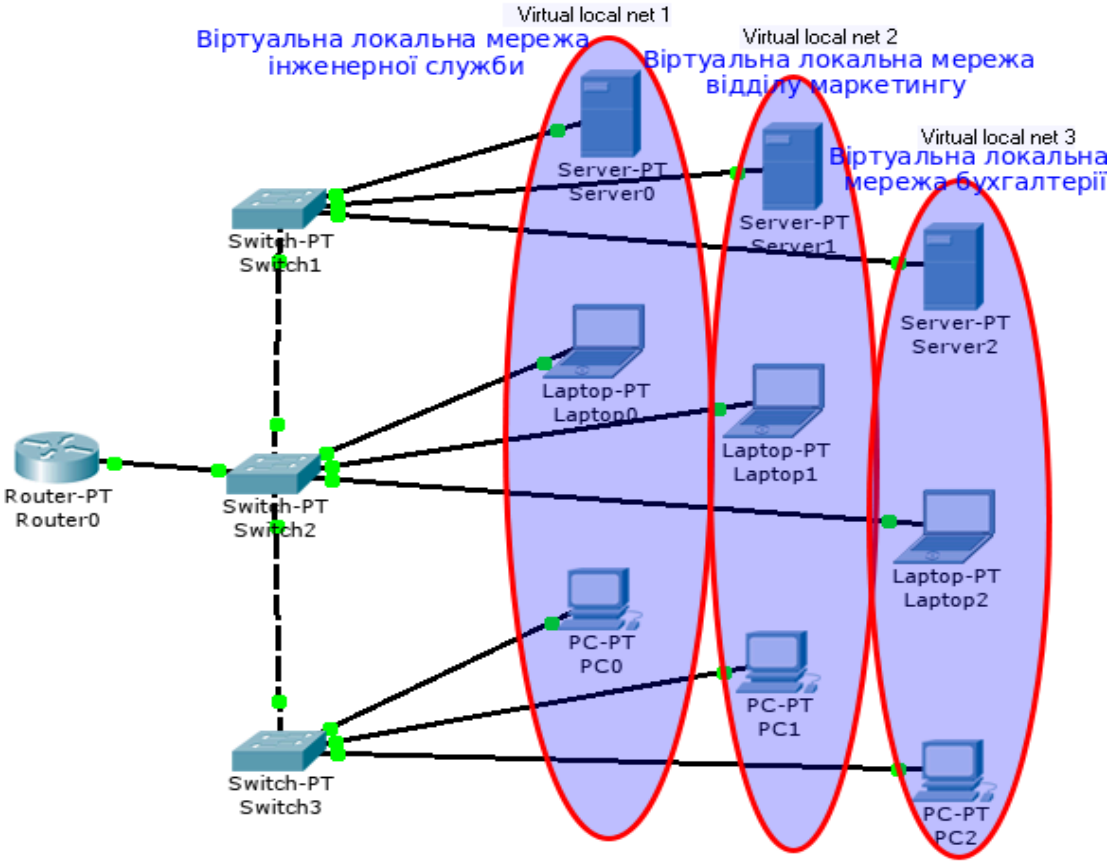

Рис.2

VLAN дозволяє логічно розбити вихідну локальну мережу на декілька незалежних локальних мереж без фізичного обриву мережевих з'єднань. Для цього адміністратор мережі повинен на кожному комутаторі призначити, які його порти відносяться до яких *VLAN*. За замовчуванням, всі порти комутатора відносяться до однієї *VLAN* з номером 1. Максимальна кількість *VLAN* в комутаторі дорівнює загальній кількості його портів. Правильне розбиття локальної мережі на *VLAN* є одним із найважливіших завдань проектування.

VLAN поводяться так само, як і фізично розділені локальні мережі. Тобто після розбиття мережі на *VLAN* одержується декілька локальних мереж, які далі необхідно об'єднати в єдине ціле за допомогою маршрутизації на третьому мережному рівні.

Концепція *VLAN*, крім вирішення проблеми з широкомовним трафіком, дає також деякі додаткові переваги: формування локальних мереж не за місцем розташування найближчого комутатора, а за належністю комп'ютерів до вирішення тієї чи іншої виробничої задачі; створення мережі за типом споживаного обчислювального ресурсу та необхідної серверної послуги (файл-сервер, сервер баз даних). *VLAN* дозволяють вести різну політику безпеки для різних віртуальних мереж; переводити комп'ютер з однієї мережі в іншу без здійснення фізичного переміщення або перепідключення.

Для обміну інформацією про *VLAN* комутатори використовують магістральний (транковий) протокол. Для здійснення обміну інформацією про *VLAN* між комутаторами потрібно створити магістральні порти. Магістральний порт - це порт, який використовується для передачі інформації про *VLAN* в інші мережеві пристрої, які приєднані до цього порту. Звичайні порти не поширюють інформацію про *VLAN*, але будь-який порт може бути налаштований для прийому/передачі інформації про *VLAN*. Потрібно активізувати магістральний протокол на потрібних портах, так як він вимкнений за замовчуванням.

Порт комутатора працює або в режимі доступу або в магістральному режимі. Відповідно зв'язок, який під'єднаний до порту, є або зв'язком доступу або магістральним зв'язком. У режимі доступу порт належить тільки одній *VLAN*, а порт доступу приєднується до кінцевого пристрою: ПК, робочої станції, сервера, хабу, тощо. Фрейми, що проходять

через порт доступу, є звичайними *Ethernet*-фреймами. Магістральні зв'язки здатні підтримувати декілька *VLAN*, які на різних комутаторах зв'язуються через магістральний протокол. Магістральні порти не належать певній *VLAN* і використовуються для приєднання до інших комутаторів, маршрутизаторів або серверів, що мають мережеві адаптери з можливістю для підключення до багатьох *VLAN*.

Магістралі можуть розширити *VLAN* по всій мережі. Для магістральних цілей призначають високошвидкісні порти комутаторів: *Gigabit Ethernet* та *10Gigabit*.

Для мультиплексування трафіку *VLAN* існують спеціальні протоколи, які дозволяють прийомним портам визначити, якому *VLAN* належить пакет. Для зв'язку між пристроями *Cisco* використовується протокол *Inter-Switch Link* (*ISL*). При наявності в мережі обладнання декількох виробників застосовується протокол *IEEE 802.1Q*.

Без магістральних зв'язків для підтримки *VLAN* повинно бути організоване по одному зв'язку доступу для кожної *VLAN*. Такий підхід є дорогим і неефективним - тому магістральні зв'язки абсолютно необхідні при проектуванні локальних мереж.

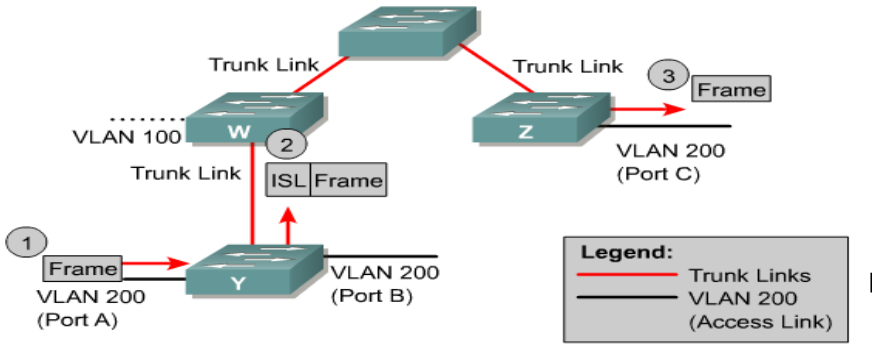

Рис. 3

На рис. 3 порти *A* і *B* на комутаторі *Y* визначені як зв'язки доступу на одній і тій же *VLAN* 200. За визначенням вони можуть належати лише одній *VLAN* і не можуть отримувати *ethernet*-фрейми, які містять ідентифікатор *VLAN*. Наприклад, коли *Y* отримує трафік з порту *A* до порту *B*, то він не додає *ISL* заголовок в *ethernet*-фрейми. Порт *C* на комутаторі *Z* також є портом доступу і також належить до *VLAN 200*. Якщо порт *A* пересилає фрейм в порт *C*, то відбувається наступне:

1. Комутатор *Y* отримує фрейм і, зіставляючи номер порту призначення з номером *VLAN*, визначає його як трафік, спрямований до *VLAN 200* на іншому комутаторі.
2. Комутатор *Y* додає до фрейму *ISL* заголовок з номером *VLAN* і пересилає фрейм через проміжний комутатор на магістральний зв'язок.
3. Цей процес повторюється на кожному комутаторі на шляху руху фрейму до кінцевого порта *C*.
4. Комутатор *Z* отримує фрейм, видаляє *ISL* заголовок і направляє фрейм на порт *C*.

Якщо порт знаходиться в магістральному режимі, то він може бути налаштований або для транспорту всіх *VLAN* або обмеженої множини *VLAN*. Магістральні зв'язки використовуються для зв'язку комутаторів з іншими комутаторами, маршрутизаторами або із серверами, які мають підтримку *VLAN*.

Згідно базової термінології магістраль - це зв'язок точка-точка, що підтримує декілька *VLAN*. Метою магістралі є збереження номерів портів при створенні зв'язку між двома пристроями, що утворюють *VLAN*.

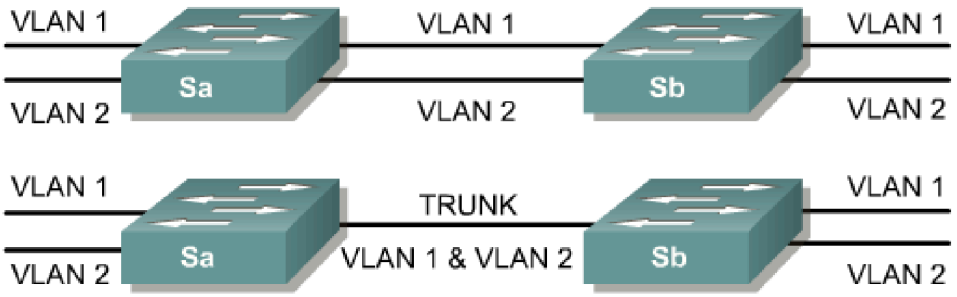

Рис. 4

Верхня фігура на рис.4 показує спосіб створення *VLAN* за допомогою використання двох фізичних зв'язків між комутаторами (по одному на кожний *VLAN*). Це рішення погано масштабується: при додаванні третьої *VLAN* потрібно "пожертвувати" ще двома портами. На нижній фігурі один фізичний зв'язок здатний нести трафік для будь-якої *VLAN*. Для досягнення цього комутатор *Sa* так оформлює фрейми, що *Sb* знає, на який *VLAN* вони прямують. Для такого оформлення пакетів використовуються або стандарт *IEEE 802.1Q* або *Cisco* протокол *ISL* (*Inter-Switch Link*).

Для великих мереж ручна конфігурація *VLAN* стає досить трудомістким завданням. *Cisco VLAN Trunk Protocol (VTP)* служить для автоматичного обміну інформацією про *VLAN* через магістральні порти. Перевагою використання *VTP* є те, що є можливість контролювати додавання, видалення або зміну мереж *VLAN* з комутаторів, на яких створені *VTP*-сервера. Після налаштування комутаторів як *VTP*-серверів, інші комутатори мережі можуть бути налаштовані як клієнти, які тільки отримують *VLAN* інформацію.

Якщо мережа містить багато комутаторів, що містять багато віртуальних мереж розташованих у різних комутаторах, можливо, варто використовувати *VTP*. Якщо мережа залишається досить статичною і *VLAN* не будуть додаватися або змінюватися по відношенню до початкової конфігурації, то краще використовувати статичне визначення віртуальних мереж.

У топології локальних мереж можливі також цикли (петлі). Наприклад, вже три комутатори, які з'єднані один з одним по колу, утворять цикл в топології. Петлі призводять до неоднозначності при визначенні шляху від джерела пакетів до приймача. Для вирішення цієї серйозної проблеми був розроблений протокол сполучного дерева *STP (Spanning tree protocol)*. Для графа топології кожної *VLAN*, яка визначена в мережі, будується дерево (яке мінімально покриває, граф без циклів) з вершиною в деякому комутаторі. Для фізичної реалізації таких дерев *STP* переводить надлишкові порти в стан блокування. Розрахунок дерев проводиться паралельно на всіх комутаторах. Далі пакети у *VLAN* йдуть тільки по шляхах, які визначені у побудованих деревах. При зміні топології (активації/зупинці портів) відбувається перерахунок покриваючих дерев.

Для створення топології сполучного дерева існують спеціальні фрейми, які називаються модулями даних мостового протоколу (*bridge protocol data units, BPDU*). Ці фрейми відправляються і приймаються усіма комутаторами в мережі через рівні проміжки часу.

Конфігурування статичних VLAN

1. Статичні *VLAN* - це сукупність портів на комутаторі, які вручну призначаються командою *IOS* при конфігуруванні інтерфейсу. Для створення порожньої *VLAN* з номером *№ VLAN* на комутаторах *Cisco* серії *2950* використовуються команди

Switch# **vlan database**

Switch(vlan)# **vlan № VLAN**

Switch(vlan)# **exit**

Наприклад, команди

Switch# **vlan database**

Switch(vlan)# **vlan 33**

Switch(vlan)# **exit**

створять порожню *VLAN* з номером 33 і система дасть *VLAN* ім'я *VLAN0033*.

Зауважимо, що команди виконуються не в режимі конфігурації. Команда **switchport mode** використовується для установки інтерфейсу в динамічний режим, режими доступу або режим магістралі (*trunk*).

Switch (config-if)# **switchport mode [access | dynamic | trunk]**

Хоча режим доступу є режимом за замовчуванням, але в деяких випадках пристрій, який приєднаний до порта комутатора, може перевести його в магістральний режим. Тому рекомендується всі немагістральні порти переводити в режим доступу командою **switchport mode access**.

Для статичного переведення поточного інтерфейсу під VLAN використовуються команди

Switch (config-if)# **switchport mode access**

Switch (config-if)# **switchport access vlan № number**

де № number - число - номер *VLAN*.

*Ком*анда **interface range** визначає діапазон інтерфейсів для подальших конфігурацій. Наприклад, порти з першого по шостий можуть бути поміщені під *VLAN 10* командами

Switch (config)# **interface range fa0/1–6**

Switch (config-if-range)# **switchport access vlan 10**

Після налаштування *VLAN* перевірте налаштування командами **show running-config**, **show vlan** і **show vlan brief**. При налаштуванні *VLAN* варто пам'ятати, що, за замовчуванням, всі порти перебувають під *VLAN 1*.

Для створення або конфігурування магістралі *VLAN* потрібно налаштувати порт як магістральний

Switch (config-if)# **switchport mode trunk**

За замовчуванням, остання команда визначає порт як магістральний для всіх *VLAN* в мережі. Однак, існують ситуації, коли магістраль не повинна підтримувати всі *VLAN*. Типовою є ситуація з усуненням широкомовлення, яке надсилається на кожен порт по *VLAN*. Магістральний зв'язок виступає як елемент VLAN і повинен пропускати всі широкомовлення. Якщо на іншому кінці магістралі немає портів потрібної *VLAN*, то смуга пропускання і процесорний час пристроїв витрачається даремно.

Якщо *VLAN* не використовується на іншому кінці магістралі, немає потреби дозволяти цю *VLAN* на цій магістралі. За замовчуванням, магістральні порти приймають і передають трафік з усіх VLAN в мережі. Для скорочення магістрального трафіку можна використовувати команду

Switch (config-if)# **switchport trunk allowed vlan vlan-list**

Наприклад, команда

Switch (config-if)# **switchport trunk allowed vlan 3**

Switch (config-if)# **switchport trunk allowed vlan 6-10**

дозволяє на магістралі *VLAN 3* і потім *VLAN* з 6 по 10. Інформацію про *VLAN,* які дозволені на магістралі, можна подивитися командою **show running-config**.

Для видалення значної частини *VLAN* з магістралі простіше спочатку видалити всі *VLAN*, а потім вибірково дозволити необхідні.

Найпростіший спосіб перевести зв'язок у режим доступу - це задати на інтерфейсах з двох сторін команди

SwitchA (config-if)# **switchport mode access**

Найпростіший спосіб перевести зв'язок у магістральний режим - це задати на інтерфейсах з двох сторін команди

SwitchA (config-if)# **switchport mode trunk**

Хід роботи

1. Складіть топологію зображену на рис. 5. Комутатори з'єднайте двома GigabitEthernet (gi1/1 і gi1/2) з'єднаннями. Комп'ютери приєднайте до інтерфейсів згідно з таблицею 1. Призначте комп'ютерам адреси, відповідно до таблиці 1. Всі комп'ютери входять в одну підмережу 172.16.0.0 255.255.0.0. Маршрути за замовчуванням на комп'ютерах не встановлюйте. Пропінгуйте мережу.

Організуємо в нашій мережі два VLAN. Комп'ютери 20_1 і 20_2 помістимо у VLAN з номером 20, а комп'ютери 30_1 і 30_2 помістимо у VLAN з номером 30.

Switch1 (conf)# **interface fa0/2**
Switch1(conf-if)# **switchport access vlan 20**
Switch1(conf-if)# **interface fa0/3**
Switch1(conf-if)# **switchport access vlan 30**
Switch2(conf)# **interface fa0/2**
Switch2(conf-if)# **switchport access vlan 20**
Switch2(conf-if)# **interface fa0/3**
Switch2(conf-if)# **switchport access vlan 30**

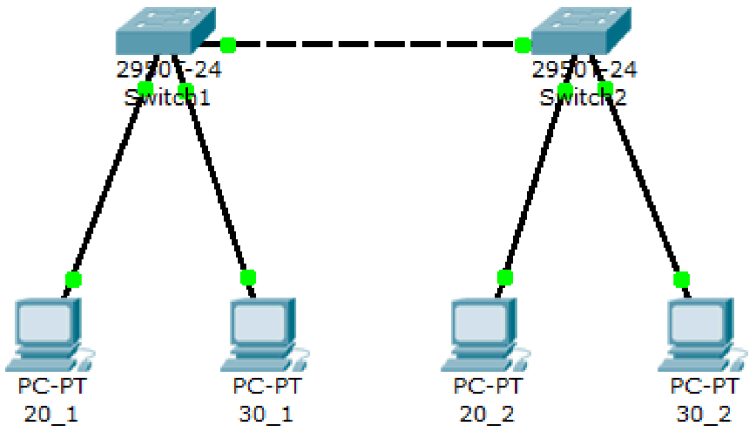

Рис. 5

Таблиця 1

Комп’ютер	Switch1	Switch2	Адрес
20_1	Fa0/2		172.16.20.1/16

30_1	Fa0/3		172.16.20.2/16
20_2		Fa0/2	172.16.30.1/16
30_2		Fa0/3	172.16.30.2/16
	Gi1/1	Gi1/1	

На обох комутаторах перевірте результати створення VLAN за допомогою наступних команд

Switch1# **sh vl name 20**

та

Switch1# **sh vl br**

Так як немає обміну інформації про VLAN між комутаторами, то комп'ютери будуть пінгувати тільки самих себе.

Організуємо магістралі на комутаторах. Для цього використовуємо GigabitEthernet порт

Switch1 (conf)# **interface gi1/1**
Switch1 (conf-if)# **switchport trunk allowed vlan add 20**
Switch1 (conf-if)# **switchport trunk allowed vlan add 30**
Switch1 (conf-if)# **no shutdown**
Switch2 (conf)# **interface gi1/1**
Switch2 (conf-if)# **switchport trunk allowed vlan add 20**
Switch2 (conf-if)# **switchport trunk allowed vlan add 30**
Switch2 (conf-if)# **no shut**

Тепер комп'ютери в межах однієї VLAN повинні пінгуватися, а комп'ютери, які знаходяться в різних VLAN не повинні пінгуватись (див. таблицю 2)

Таблиця 2

Ping із/в	20_1	30_1	20_2	30_2
20_1	Так	Ні	Так	Ні
30_1	Ні	Так	Ні	Так
20_2	Так	Ні	Так	Ні
30_2	Ні	Так	Ні	Так

2. Збережемо топологію попереднього завдання в новому файлі. У цій топології маршрутизатор з'єднаний двома зв'язками з інтерфейсами fa0/1 комутаторів (рис. 6). Знову перевірте, що комп'ютери в межах однієї *VLAN* пінгуються, а комп'ютери, які знаходяться в різних *VLAN* не пінгуються.

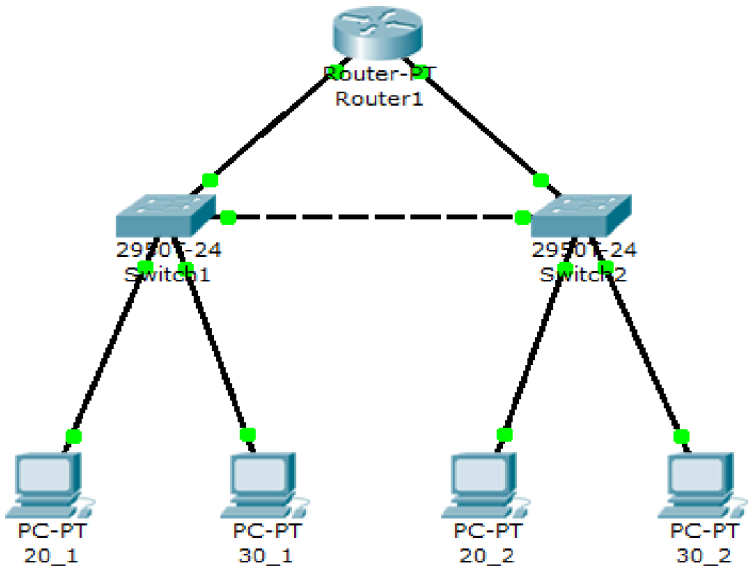

Рис. 6

Поставимо задачу об'єднання віртуальних мереж за допомогою маршрутизатора. Для цього потрібно розбити мережу 172.16.0.0/16 на дві підмережі 172.16.20.0/24 і 172.16.30.1/24. (для цього просто поміняємо маски в комп'ютерів на 255.255.255.0).

Тепер комп'ютери пінгуються в межах однієї VLAN і в межах однієї IP підмережі. Введемо на комутаторах інтерфейси, які приєднані до маршрутизатора в віртуальні мережі

Switch1(conf)# **interface fa0/1**

Switch1(conf-if)# **switchport access vlan 20**

Switch2(conf)# **interface fa0/1**

Switch2(conf-if)# **switchport access vlan 30**

Налаштуємо IP адреси на маршрутизаторі

Router (conf)# **interface fa0/0**

Router (conf-if)# **ip address 172.16.20.100 255.255.255.0**

Router (conf-if)# **no shutdown**

Router (conf-if)# **interface fa1/0**

Router (conf-if)# **ip address 172.16.30.100 255.255.255.0**

Router (conf-if)# **no shutdown**

Тепер маршрутизатор маршрутизує наші дві мережі 172.16.20.0/24 і 172.16.30.1/24. Додамо на наших комп'ютерах маршрутизацію за замовчуванням на інтерфейси маршрутизатора.

Host	Gataway
20_1	172.16.20.100
30_1	172.16.30.100
20_2	172.16.20.100
30_2	172.16.30.100

Тепер з усіх пристроїв нашої мережі є можливість пінгувати всі *IP*-адреси.

3. Покажемо, як з використанням транзитних ліній, можна заощадити порти. Змінимо топологію, перекинувши магістраль gi1/2 від комутаторів до інтерфейсу fa0/0 марш-рутизатора (рис. 7). Завантажимо топологію в симулятор. Завантажимо по порядку в кожен пристрій, крім маршрутизатора, збережені конфігурації. Зауважимо, що в конфігурації комутатора Switch2 установка магістралі на gi1/2 не потрібна, хоча вона і не заважає.

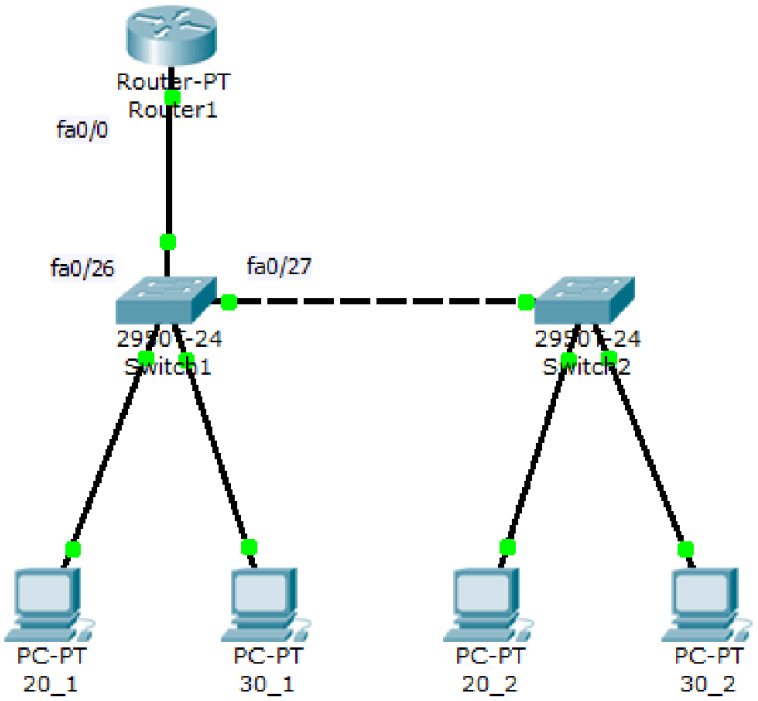

Рис. 7

На маршрутизаторі розіб'ємо інтерфейс *fa0/0* на два під-інтерфейси *fa0/0.20* і *fa0/0.30*. Визначимо на них інкапсуляцію dot1q і помістимо їх у віртуальні мережі 20 і 30, відповідно.

Router(conf)# **interface FastEthernet0/0.20**

Router(conf-subif)# **encapsulation dot1q 20**

Router(conf-subif)# **ip address 172.16.20.100 255.255.255.0**

Router(conf-subif)# **interface FastEthernet0/0.30**

Router(conf-subif)# **encapsulation dot1q 30**

Router(conf-subif)# **ip address 172.16.30.100 255.255.255.0**

Подивимося таблицю маршрутів

Router# **show ip route**

Перевірте, що з кожного пристрою є можливість пінгувати всі адреси в мережі. Виконайте на *Router* команду розширеного пінгу від адреси *172.16.20.1* комп'ютера *20_1* з *VLAN 20*, який підключений до комутатора *Switch1,* до адреси *172.16.30.2* комп'ютера *30_2* з *VLAN 30*, який підключений до комутатора *Switch2.*

Контрольні запитання

1. Чому надають перевагу будувати локальні мережі за допомогою комутаторів, а не концентраторів ?
2. Які існують методи для відправки фрейму через комутатор ?
3. Як комутатор дізнається *MAC*-адреси підключених пристроїв ?
4. Де і як в комутаторі зберігаються адреси підключених пристроїв ?
5. Що таке віртуальне з'єднання і як довго воно існує ?
6. Як завелику локальну мережу можна створити за допомогою комутаторів ?
7. Як прийнято будувати великі локальні мережі ?
8. Що є головною перешкодою для створення великих локальних мереж за допомогою одних тільки комутаторів ?
9. Що таке домен широкомовлення ?
10. Як зменшити домен широкомовлення ?
11. Що таке *VLAN* ?
12. Які проблеми локальних мереж вирішує *VLAN* ?
13. Як в локальній мережі організувати обмін інформацією про *VLAN* ?
14. У яких режимах працюють порти комутатора ?
15. Який *VLAN* належить магістральний порт ?
16. Як поширити одну *VLAN* на кілька комутаторів ?
17. Чи можна організувати декілька *VLAN* на декількох комутаторах без використання магістралей ?
18. Навіщо потрібні протоколи *ISL* та *IEEE 802.1Q* ?
19. Навіщо потрібні магістралі в в локальній мережі ?
20. Які завдання вирішує *VTP* ?
21. Які завдання вирішує *STP* ?
22. Якими командами можна організувати *VLAN* ?
23. Якою командою перевести порт в режим доступу та в режим магістралі ?
24. Якою командою можна отримати інформацію про *VLAN* ?
25. У локальній мережі присутні десять *VLAN*. Скільки маршрутизаторів потрібно для об'єднання всіх 10 *VLAN* в єдине ціле ?

Порядок виконання та здачі роботи

1. Одержати індивідуальне завдання.
2. Вивчити теоретичну частину та методику виконання роботи.
3. Виконати усі пункти практичної частини.
4. В середовищі Packet Tracer виконати індивідуальне завдання.
5. Оформити звіт.
6. Відповісти на контрольні запитання.
7. Продемонструвати виконання індивідуального завдання.

Завдання для самостійної роботи

1. Одержати варіант *v* у викладача.
2. Виконайте практичну частину роботи для мережі підприємства *v.1.0.0/16*.
3. Зробити скріншоти, які відповідають процесу виконання роботи.

Зміст звіту

Звіт готується в електронному вигляді і друкується. Звіт містить:

1. Скріншот топології, яка створена при виконанні практичної частини.

2. Конфігурації всіх маршрутизаторів із .txt файлів, створених при виконанні практичної частини.

3. Скріншот топології вашого варіанту з адресами і масками, які зазначені в завданні для самостійної роботи.

4. Конфігурації всіх маршрутизаторів із .txt файлів, створених при виконанні завдання для самостійної роботи.

5. Всі скріншоти, які вказані в завданні для самостійної роботи.