Міністерство освіти і науки України
Сумський державний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни «Телекомунікаційні та інформаційні мережі»
для студентів спеціальності
172 "Телекомунікації та радіотехніка"
усіх форм навчання

Суми
Сумський державний університет
2017

Методичні вказівки до виконання лабораторних робіт з дисципліни «Телекомунікаційні та інформаційні мережі» / укладачі: О. В. Д’яченко, О. Є. Горячев, Т. О. Протасова, К. О. Д’яченко. – Суми: Сумський державний університет, 2017. – 46 с.

Кафедра електроніки і комп’ютерної техніки

Лабораторна робота №3

Конфігурація і моніторинг віртуальних комп'ютерних мереж

1. Вступ

Побудова великих локальних мереж на основі технології Ethernet пов'язане з певними труднощами.

Структуризація мережі Ethernet шляхом формування логічних сегментів дозволяє скоротити навантаження на кожен сегмент і підвищити продуктивність, безпеку і керованість всієї мережі. Проте, в структурованих локальних мережах, що використовують в якості комунікаційних пристроїв комутатори, в яких обробляються передані кадри з плоскими MAC-адресами, існує ряд проблем:

можливість виникнення широкомовних штормів (Broadcast Storm);

труднощі об'єднання в одному логічному сегменті віддалених користувачів.

Нагадаємо, що комутатор забезпечує три основних алгоритму обробки переданих кадрів:

просування (Forwarding) кадру, прийнятого через даний порт, до іншого порту відповідно до запису в таблиці комутації;

фільтрація (Filtering) кадру, прийнятого через даний порт, якщо MAC-адреса одержувача доступний через цей же порт; в цьому випадку кадр відкидається, тому що користувач уже мав отримати цей кадр;

передача кадру, прийнятого через даний порт, до всіх портів комутатора - затоплення мережі (Flooding); в такому режимі передаються кадри з широкомовними MAC-адресами, а також кадри з невідомими груповими або індивідуальними адресами призначення.

При створенні локальних мереж на основі комутаторів всі вузли мережі являють собою єдиний широкомовний домен, тобто широкомовний трафік передається всім вузлам мережі.

При програмних або апаратних збоїв протоколу верхнього рівня або мережевого адаптера можлива генерація з високою інтенсивністю помилкових кадрів з широкомовною або невідомим адресами. При цьому комутатор передає помилковий трафік в усі мережеві сегменти. Така ситуація називається широкомовним штормом. Мости і комутатори не захищають мережі від широкомовних штормів.

Затоплення мережі широкомовними штормами може також викликатися широкомовними запитами або сповіщень, часто вживаними сучасними мережевими протоколами.

Наприклад, ARP (Address Resolution Protocol) - протокол визначення локального адреси по IP-адресою, передбачає розсилку по мережі широкомовних запитів. Протокол ARP передає циркулярний запит на канальному рівні, якщо необхідний локальний адресу відсутня в наявній ARP-таблиці мережевого пристрою, або формує широкосмугове повідомлення про адресації для щойно встановленого або заміненого мережевого обладнання.

При структуризації мережі за допомогою комутаторів логічні сегменти, як правило, формуються з комп'ютерів, розташованих на невеликій відстані від концентратора або комутатора, що об'єднує користувачів даного сегмента. При побудові великих мереж більш раціонально було б об'єднувати робочі станції і сервери з організаційних або функціональним вимогам.

Технологія віртуальних локальних мереж успішно вирішує зазначені проблеми. Віртуальної локальної мережею VLAN (англ. Virtual Local Area Network) називається група вузлів мережі, для яких будь-який трафік, включаючи широкомовний, повністю ізольований на канальному рівні від інших вузлів мережі. Вузли об'єднуються в локальну мережу програмними засобами, незалежно від просторового розміщення цих вузлів. Зміна

складу віртуальної мережі здійснюється без трудомістких фізичних перемикань.

Ізоляція трафіку, в тому числі широковещательного, здійснюється на канальному рівні за допомогою комутаторів з підтримкою технології VLAN (стандарт 802.1q).

Пристрої різних віртуальних мереж «не бачать» одне одного на канальному рівні. Для зв'язку між окремими віртуальними мережами необхідний вихід на мережевий рівень і застосування маршрутизаторів.

Технологія віртуальних мереж забезпечує:

створення спеціалізованих, функціонально розділених мереж, незалежно від просторового розміщення входять до неї робочих станцій або серверів;

підвищення продуктивності мережі;

перешкода для виникнення широкомовних штормів;

локалізацію широкомовного трафіка, а також трафіку з невідомими груповими або індивідуальними адресами в межах даної віртуальної мережі; підвищення безпеки роботи мереж і спрощення проведення політики розвитку мереж по відношенню до груп користувачів.

2. Технологія віртуальних мереж (VLAN)

Організація віртуальних мереж вимагає спеціальної настройки портів комутаторів.

Залежно від структури вихідної мережі в технології VLAN застосовуються різні способи налаштування комутаторів

2.1. Організація VLAN в комп'ютерних мережах з простою топологією

При організації VLAN на одному комутаторі порти цього комутатора розподіляються між створюваними віртуальними мережами, а в таблицю комутації вводиться додатковий стовпець для індексів VLAN_ID, що визначають приналежність порту до певної VLAN. Комутовані кадри можуть передаватися

тільки між портами, що відносяться до однієї віртуальної мережі.

Порти і підключення до них мережеві вузли, що входять в одну віртуальну локальну мережу, використовують окрему частину таблиці комутації.

Такий метод організації віртуальних мереж називається методом групування портів. Групування портів, як правило, здійснюється вручну мережевим адміністратором.

Організація VLAN методом групування портів на одному комутаторі показана на рис. 3.1.

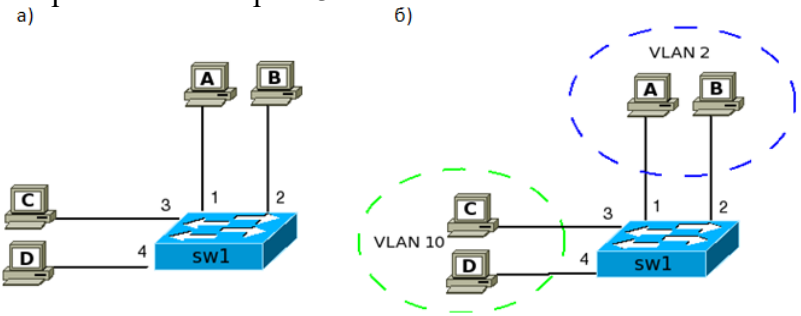

Рис. 3.1. Організація VLAN на одному комутаторі: а - схема вихідної мережі (таблиця комутації комутатора представлена в табл. 3.1); б - мережа, розділена на дві VLAN (таблиця комутації комутатора представлена в табл. 3.2))

Таблица 3.1. Таблиця коммутации до формирования VLAN
Таблица 3.2. Таблиця коммутації с VLAN

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	1	A
2	1	B
3	1	C
4	1	D

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	2	A
2	2	B
3	10	C
4	10	D

Для організації VLAN методом групування портів в комп'ютерних мережах з декількома комутаторами необхідно пов'язати комутатори, що містять порти однієї VLAN, сполучними лініями. При цьому щоб усунути переходи трафіку між віртуальними мережами, кожна віртуальна мережа повинна мати власні сполучні лінії.

Організація VLAN методом групування портів на двох комутаторах показана на рис. 3.2.

Комутатори S1 і S2 з'єднані лініями «10 - 9» для VLAN 2 і «11 - 12» для VLAN 10.

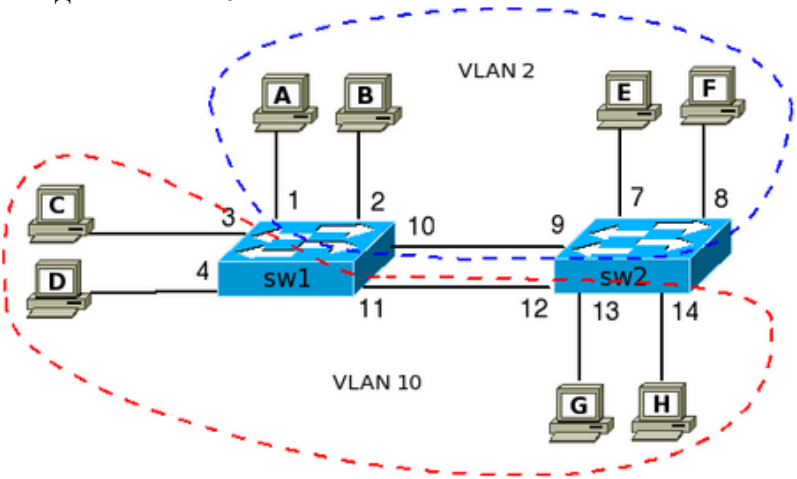

Рис.3.2. Організація VLAN на двох комутаторах методом групування портів

Таблица 3.3 - Таблица коммутации SW1 Таблица 3.4 - Таблица коммутации SW2

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	2	A
2	2	B
10	2	E
10	2	F
3	10	C
4	10	D
11	10	G
11	10	H

Порт коммутатора	VLAN ID	MAC-адрес компьютера
7	2	E
8	2	F
9	2	A
9	2	B
13	10	G
14	10	H
12	10	C
12	10	D

Застосування цього методу надлишкових зв'язків між комутаторами. При збільшенні кількості комутаторів в вихідної мережі швидко зростає число з'єднувальних ліній і суттєво збільшується обсяг робіт мережевого адміністратора по організації і зміни складу віртуальних мереж.

Тому групування портів застосовується для організації VLAN лише в простих комп'ютерних мережах, що використовують один-два комутатора.

2.2. Організація VLAN в складних комп'ютерних мережах

Комп'ютери та інші кінцеві пристрої, підключені до різних комутаторів, можуть об'єднуватися в віртуальні мережі за допомогою спеціальних міток, що вводяться в передані кадри (стандарт IEEE 802.1Q).

Всі порти комутаторів поділяються на дві групи:

порти доступу (англ. access), що включають кінцеві пристрої (комп'ютери, сервери, принтери та ін.) до комутатора;

порти ліній зв'язку (англ. trunk), що з'єднують комутатори між собою.

Порти доступу комутаторів, як і раніше, розподіляються по створюваним віртуальних мереж.

Отримавши від кінцевого пристрою кадр для передачі по мережі Ethernet, обладнання портів доступу вводить в кадр спеціальні мітки, які свідчать про належність даного кадру до певної віртуальної мережі. Кадр з такою міткою називається «тегованих» - позначеним (англ. Tag - ярлик, мітка). Усередині комутатора передаються тільки тегованих кадри.

Комутатор просуває кадр тільки між портами, що мають загальний тег, тобто входять в одну віртуальну мережу.

При передачі комутованого кадру одержувачу інформації на кінцевий мережевий вузол, порт доступу вилучає з кадру раніше введений тег, і мережеві користувачі отримують вихідні інформаційні кадри без будь-яких слідів тегірованія.

Порти доступу працюють в режимі access.

На відміну від портів доступу, порти, підключені до ліній зв'язку між комутаторами, можуть приймати і передавати кадри різних віртуальних мереж.

Наявність міток в переданих кадрах дозволяє використовувати загальні з'єднувальні лінії між комутаторами для передачі кадрів декількох віртуальних мереж при забезпеченні ізоляції трафіку кожної мережі.

Порти ліній зв'язку між комутаторами працюють в режимі trunk.

За замовчуванням усі користувачі і порти комутаторів відносяться до вихідної мережі VLAN1.

При формуванні віртуальних мереж на комутаторах порти доступу вводяться в режим роботи access і розподіляються між різними віртуальними мережами, отримуючи відповідне значення ідентифікатора для кожного порту.

Порти ліній зв'язку між комутаторами вводяться в режим роботи trunk. Такі порти отримують кілька значень ідентифіка-

торів, відповідних віртуальних мереж, трафік яких повинен передаватися по даній лінії зв'язку. 44

Організація VLAN на основі тегірованія портів і використання загальною лінією зв'язку між комутаторами показана на рис.3.3. Порти 21 і 22 - транкінгові порти, які мають ідентифікатори VLAN_2 і VLAN_10.

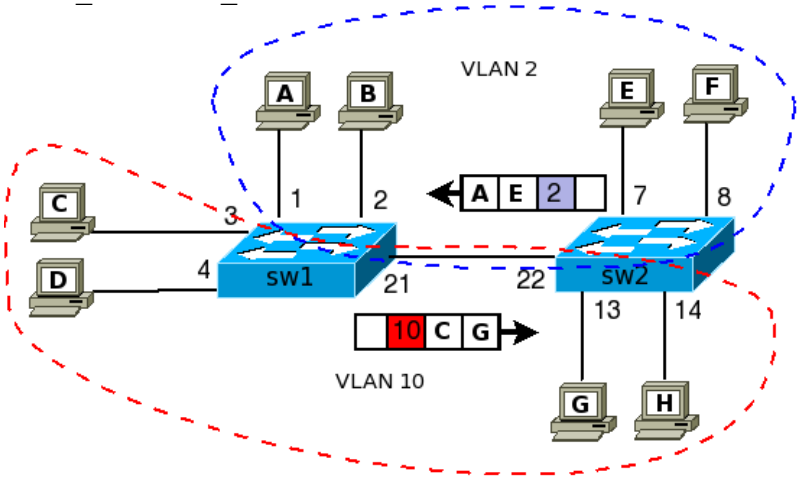

Рис. 3.3. Організація VLAN шляхом тегірованія переданих кадрів за стандартом IEEE 802.1Q.

У лабораторній роботі пропонується створити VLAN на мережі, що складається з трьох комутаторів, порти яких працюють в режимах access і trunk.

При виконанні роботи необхідно:

- побудувати вихідну комп'ютерну мережу;
- провести конфігурацію комутаторів;
- створити віртуальні мережі;
- встановити режими access і trunk для портів комутаторів;
- проаналізувати адресні таблиці комутаторів;
- перевірити проходження інформаційних пакетів в перетвореної мережі.

3. Побудова мережі на основі віртуальних локальних мереж в пакеті Cisco Packet Tracer

3.1. Створення моделі мережі

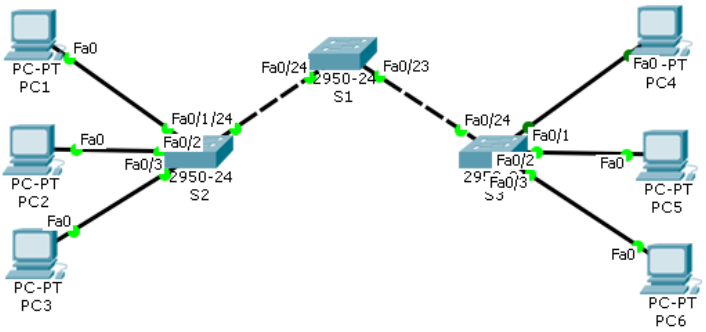

Рис. 3.4. Схема вихідної комп'ютерної мережі

У вихідній мережі, показаної на рис. 3.4., Необхідно організувати три віртуальні локальні мережі: VLAN_10, в яку входять PC1 і PC4; VLAN_20, в яку входять PC2 і PC5; VLAN_30, в яку входять PC3 і PC6.

Відкрийте Cisco Packet Tracer і створіть мережу, показану на рис. 3.4. При з'єднанні пристроїв використовуйте типи кабелів, відповідні схемою. Нагадуємо, що комп'ютери прийнято підключати до комутаторів через порти з малими номерами (fa0 / 1, fa0 / 2 і fa0 / 3), а для зв'язків між комутаторами зазвичай використовуються порти з великими номерами (fa0 / 24 і fa0 / 23).

3.2. Налаштування комп'ютерів

Використовуючи вікно IP Configuration у вікні Desktop комп'ютера, задайте комп'ютерів ip-адреси, зазначені в таблиці 1.

Таблиця 3.5

Устройство	VLAN	IP-адрес	Маска
PC1	10	172.17.10.21	255.255.0.0
PC2	20	172.17.20.22	255.255.0.0
PC3	30	172.17.30.23	255.255.0.0
PC4	10	172.17.10.24	255.255.0.0
PC5	20	172.17.20.25	255.255.0.0
PC6	30	172.17.30.26	255.255.0.0

За допомогою команди ping в режимі командного рядка (Command Prompt) для одного з комп'ютерів, наприклад PC1, перевірте доступність всіх комп'ютерів мережі.

3.3. Початкова конфігурація комутаторів

Початкова конфігурація комутаторів в даній роботі не відрізняється від конфігурації, розглянутої в лабораторній роботі 2. Використовуючи вкладку командного рядка (CLI) у вікні кожного комутатора, виконайте наступні команди на комутаторах S1, S2 і S3:

```
Switch> enable
Switch # configure terminal
Enter configuration commands, one per line. End with Ctrl Z.
Switch (config) #hostname S1
S1 (config) #enable secret class
S1 (config) #line console 0
S1 (config-line) #password cisco
S1 (config-line) #login
S1 (config-line) #line vty 0 15
S1 (config-line) #password cisco
S1 (config-line) #login
```

S1 (config-line) #end
% SYS-5-CONFIG_I: Configured from console by console
S1 # copy running-config startup-config
Destination filename [startup-config]? [OK]
Building configuration ...
[OK]
Не забудьте дати комутаторів різні імена.

3.4. Перевірка стану мережевих інтерфейсів

Перевірте, чи правильно підключено портів комутатора, виконавши на S2 в привілейованому режимі команду show **ip interface brief.**

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status                Proto
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/23       unassigned      YES manual down                  down
 …
FastEthernet0/24       unassigned      YES manual up                    up
Vlan1                  unassigned      YES manual administratively down down
```

Переконайтеся, що порти, до яких підключені комп'ютери і інші комутатори знаходяться в стані up.

Проробіть аналогічні дії на комутаторах S1 і S3.

3.5. Відключення додаткових протоколів

Для спрощення таблиць комутації слід відключити ряд протоколів, що працюють на комутаторах.

У режимі глобального конфігурування відключіть cdp і spanning-tree (приклад для S1):

```
S1(config)#no cdp run
S1(config)#no spanning-tree vlan 1-4096
```

Встановіть заборону на відправку пакетів dtp через цей інтерфейс (приклад для S1):

```
S1(config)#interface fa0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
```

Виконайте цю команду на всіх інтерфейсах, що з'єднують комутатори (для S1 це fa0 / 24 і fa0 / 23).

У режимі привілейованого користувача зробіть очищення таблиць комутації на всіх комутаторах:

```
S1#clear mac-address-table
```

3.6. Перевірка таблиць комутації

Згенеруйте трафік за допомогою команди ping, перевіривши доступність всіх комп'ютерів з PC1.

Спочатку все комп'ютери входять в одну локальну мережу (за замовчуванням на комутаторах cisco це VLAN 1). Переконайтеся в цьому, виконавши команду #show mac-address table в привілейованому режимі.

```
S1#show mac-address-table
          Vlan    Mac Address       Type        Ports
          ----    -----------       --------    -----

             1    0004.9a19.1418    DYNAMIC     Fa0/23
             1    00d0.bc4b.b818    DYNAMIC     Fa0/24
             1    0001.c98d.9d66    DYNAMIC     Fa0/23
             1    0002.1656.528a    DYNAMIC     Fa0/24
             1    0001.9614.d392    DYNAMIC     Fa0/23
             1    00d0.bce5.234a    DYNAMIC     Fa0/24
             1    0001.97e1.8486    DYNAMIC     Fa0/24
             1    0001.c958.a094    DYNAMIC     Fa0/23
```

Важливо! *Якщо довго (понад 10 хв) не було обміну пакетами між пристроями (комп'ютерами), таблиці комутації можуть очиститися. Для їх відновлення необхідно знову -пропінгувати всі комп'ютери в мережі.*

3.7. Створення віртуальних мереж на комутаторах

Створіть нові віртуальні мережі vlan_10, vlan_20 і vlan_30 на кожному комутаторі (S1, S2 і S3), ввівши команди у вкладці CLI в привілейованому режимі.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name vlan_10
S1(config-vlan)exit
S1(config)#vlan 20
S1(config-vlan)#name vlan_20
S1(config-vlan)exit
S1(config)#vlan 30
S1(config-vlan)#name vlan_30
S1(config-vlan)#exit
```

Перевірте стан vlan-ів, виконавши в привілейованому режимі команду show vlan brief:

```
S1#show vlan brief
VLAN Name                         Status    Ports
---- ---------------------------- --------- -------------------------
1    default                      active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                            Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                            Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                            Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   vlan_10                      active
20   vlan_20                      active
30   vlan_30                      active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Вивчіть висновок команди. Переконайтеся, що на комутаторі організовані 10, 20, 30 vlan.

Зверніть увагу, що всі порти комутатора знаходяться на даний момент в vlan з номером 1. Віртуальні мережі з номерами 1, 1002, 1003, 1004, 1005 були автоматично створені комутатором і використовуються для службових завдань.

3.8. Налаштування віртуальних мереж на портах комутаторів

В режимі конфігурації інтерфейсів налаштуйте порти комутаторів, підключення до комп'ютерів, з урахуванням номерів портів і vlan-ів.

На комутаторі S2 переведіть порти, що з'єднують S2 с комутатором S1, в режим транка за допомогою команди switchport mode trunk, а потім додайте в транк необхідні VLANи за допомогою команди switchport trunk allowed vlan add <vlan_id>:

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int fa0/1
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#int fa0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#int fa0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#int fa0/24
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan add 10
S2(config-if)#switchport trunk allowed vlan add 20
S2(config-if)#switchport trunk allowed vlan add 30
S2(config-if)#no shutdown
S2(config-if)#exit
```

У привілейованому режимі знову виконайте команду show vlan brief:

S2 # show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22,Fa0/23
10   vlan_10                           active    Fa0/1
20   vlan_20                           active    Fa0/2
30   vlan_30                           active    Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Зверніть увагу на зміни в виділених рядках.

Для виведення стану транків використовуйте команду show interfaces trunk в привілейованому режимі:

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/24      10,20,30

Port        Vlans allowed and active in management domain
Fa0/24      10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      10,20,30
```

З виведення команди видно, що віртуальні мережі 10,20,30 включені в режимі транка на інтерфейсі Fa0 / 24

Конфігурація для S1 буде виглядати наступним чином:

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

S1(config)#interface fa0/24
S1(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/24,
changed state to down
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/24,
changed state to up
S1(config-if)#switchport trunk allowed vlan add 10
S1(config-if)#switchport trunk allowed vlan add 20
S1(config-if)#switchport trunk allowed vlan add 30
S1(config-if)#exit
S1(config)#interface fa0/23
S1(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/23,
changed state to down
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/23,
changed state to up
S1(config-if)#switchport trunk allowed vlan add 10
S1(config-if)#switchport trunk allowed vlan add 20
S1(config-if)#switchport trunk allowed vlan add 30
S1(config-if)#no shutdown
S1(config-if)#exit
```

Аналогічним чином настройте порти комутатора S3.Прі допомоги команд #show running config, #show vlan brief і #show interfaces trunk перевірте конфігурацію віртуальних мереж на комутаторах S1 і S3.

3.9. Перевірка роботи віртуальних мереж

За допомогою команди ping знову перевірте з комп'ютера PC1 доступність всіх комп'ютерів мережі. Як змінилася доступність кінцевих вузлів у порівнянні з результатами, отриманими в п. 3.4? Перевірте доступність вузлів мережі з PC2, PC3.

Перегляньте таблицю mac-адрес на кожному комутаторі, для цього в привілейованому режимі виконайте команду show mac-address-table:

```
S1#show mac-address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.c98d.9d66    DYNAMIC     Fa0/23
  10    0002.1656.528a    DYNAMIC     Fa0/24
  20    0001.9614.d392    DYNAMIC     Fa0/23
  20    00d0.bce5.234a    DYNAMIC     Fa0/24
  30    0001.97e1.8486    DYNAMIC     Fa0/24
  30    0001.c958.a094    DYNAMIC     Fa0/23
```

Визначте фізичні пристрої, відповідні mac-адресами, вказаними в таблиці в вікні CLI.

3.10. Створення віртуальних інтерфейсів і призначення IP-адрес

Основною відмінністю комутаторів від маршрутизаторів є те, що, як правило, на маршрутизаторах IP-адреси призначаються на фізичних інтерфейсах, а у комутаторів - на віртуальних інтерфейсів, прив'язаних до існуючих в комутаторі віртуальних мереж. Так, наприклад, для віртуальної мережі 10 можна створити віртуальний інтерфейс vlan10.

Створіть і налаштуйте на комутаторах у віртуальній мережі 10 інтерфейси для мережі управління (використовуйте дані з таблиці 3.6):

Таблиця 3.6 – IP адреса комутаторів

Назва пристрою	Interface	IP	Mask
S1	Vlan10	172.17.10.11	255.255.0.0
S2	Vlan10	172.17.10.12	255.255.0.0
S3	Vlan10	172.17.10.13	255.255.0.0

```
S2(config)#interface vlan 10
S2(config-if)#ip address 172.17.10.12 255.255.0.0
S2(config-if)#no shutdown
```

Налаштуйте основний шлюз комутаторів командою ip default-gateway 172.17.10.1 (необхідно для доступу до комутатора з іншої мережі)

```
S2(config)ip default-gateway 172.17.10.1
```

Виконайте в привілейованому режимі команду show ip interface brief:

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
…
FastEthernet0/23       unassigned      YES manual down                  down

FastEthernet0/24       unassigned      YES manual up                    up
Vlan1                  unassigned      YES manual administratively down down
Vlan10                 172.17.10.11    YES manual up                    up
```

Зверніть увагу на наявність віртуальних інтерфейсів VLan1 і Vlan10.

Аналогічним чином створіть і налаштуйте віртуальні інтерфейси на комутаторах S1 і S3, використовуючи наступні адреси.

Перевірте з PC1, PC2 і PC3 доступність віртуальних інтерфейсів комутаторів. Чому з одних ПК віртуальні інтерфейси доступні, а з інших недоступні, і як це можна використовувати в мережі?

3.11. Перевірка і збереження конфігурації

Перевірте конфігурацію комутатора, виконавши команду show running-config.

Збережіть конфігурація комутатора, виконавши в привілейованому режимі команду copy running-config startup-config.

4. Контрольні питання

1. Як змінилася доступність вузлів мережі після додавання віртуальних мереж?

2. Як змінилася таблиця комутації?

3. Чим відрізняється висновок команд show vlan, show vlan brief, show interface trunk?

4. Які переваги дає використання віртуальних мереж (VLAN)?

5. Чому VLAN 10 в роботі можна назвати службовим?

Лабораторна робота №4

Побудова мережі з використанням безкласової адресацією

1. Вступ

Для організації локальної комп'ютерної мережі Інтернет-провайдер надає в розпорядження користувача деяку, як правило, безперервну область адрес.

Область виділених адрес або відповідає одному із стандартних класів IP-адрес, або задається певною адресною маскою. У будь-якому випадку всі адреси виділеної області мають однаковий префікс, тобто однакову цифрову послідовність в старших розрядах.

Адміністратор може керувати наданими йому адресним простором, забезпечуючи гнучку логічну структуризацію новостворюваної мережі.

Гнучка структуризація мережі використовує безкласову адресацію, засновану на змінної довжині маски підмережі (англ. VLSM - Variable Length Subnet Mask). Маска вказується в налаштуваннях кожного мережевого пристрою з IP-адресою і визначає межу між номером мережі і номером вузла. Двійковий запис маски має одиниці в розрядах, що визначають номер мережі, і нулі в розрядах, відповідних номеру вузла.

Використання масок змінної довжини дозволяє сформувати підмережі з перекриваються адресними просторами. Так, адресні простори підмереж S3-1 і S3-2 розмістилися всередині адресного простору підмережі S3.

Підключення мережі користувача до глобальної мережі здійснюється мережевим провайдером (Internet Service Provider), як правило, через окремий маршрутизатор (роутер), що позначається як RISP.

Можлива структура мережі користувача, параметри яких відповідають умовам даного прикладу і проведеним поділу адресного простору, показана на рис.4.1.

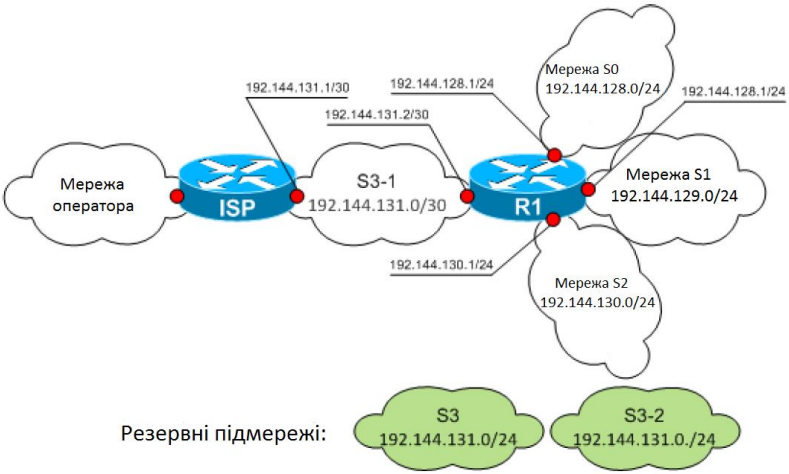

Рис. 4.1 - сконфігурованої мережу користувача

Використання безкласової технології дозволяє гнучко формувати в мережі Інтернет окремі адресні простори (домени); при цьому інформація про внутрішні подсетях використовується тільки в межах цього адресного простору. Поза такого простору всім внутрішнім подсетям, які мають загальний префікс, відповідає одна запис адреси призначення в таблицях маршрутизації.

При передачі інформації від зовнішнього джерела до даного домену все підмережі цього адресного простору фактично об'єднуються (агрегатуються) в одну загальну мережу, що істотно скорочує час обробки переданих повідомлень, особливо в магістральних маршрутизаторах.

Агрегатування підмереж може застосовуватися і при передачі інформації всередині домену. Використовуючи однакові символи в старших розрядах префікса, можна виробляти об'єд-

нання декількох підмереж для підвищення продуктивності маршрутизаторів всередині домену.

При проведенні лабораторної роботи необхідно:

– розділити адресний простір вихідної мережі між декількома підмережами;

– привласнити адреси мережних інтерфейсів комп'ютерів і маршрутизаторів;

– зібрати мережу із заданою топологією;

– провести настройку використовуваних мережевих пристроїв;

– перевірити роботу складовою мережі;

– виконати індивідуальне завдання.

2. Розрахунок підмереж

Розділіть вихідну мережа класу C 198.133.219.0/24 на 16 підмереж, використовуючи 4 старших біта останнього байта заданого адреси. Визначте маску для нових підмереж. У перших двох подсетях LAN_1 і LAN_2 (Рис. 4.2) визначте діапазон адрес, доступних для використання, адреса мережі і широкомовна адресу.

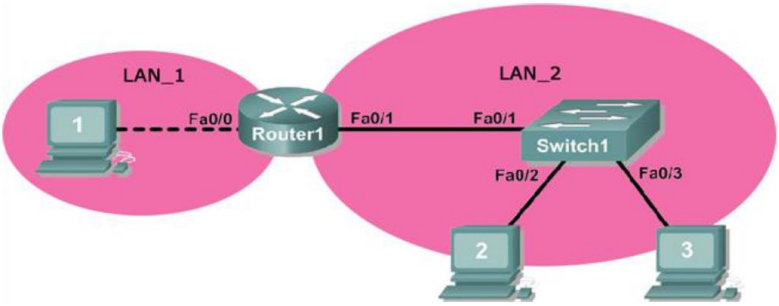

Рис. 4.2 Схема мережі із зазначенням двох підмереж

Портів маршрутизатора надайте перші адреси, а портам мережевих карт комп'ютерів - останні адреси в подсетях.

Результати розрахунків занесіть в таблицю 4.3.

Таблиця 4.3.

Назва пристрою	Інтерфейс	Підмережа	IP-адреса	Маска	Шлюз
R	Fa0/0	LAN_1			-
PC1	Eth0	LAN_1			
R	Fa0/1	LAN_2			-
PC2	Eth0	LAN_2			
PC3	Eth0	LAN_2			

3. Створення моделі мережі в програмі Cisco Packet Tracer

Відкрийте Cisco Packet Tracer і створіть мережу зі структурою, наведеною на рис. 4.3. Для цього використовуйте пристрої, зазначені в таблиці 4.4.

Таблиця 4.4.

Група пристроїв	Назва пристрою	Кіль-сть
Маршрутизатор	1841	1
Комутатор	2950-24	1
Кінцеві пристрої	PC-PT (комп'ютер)	3

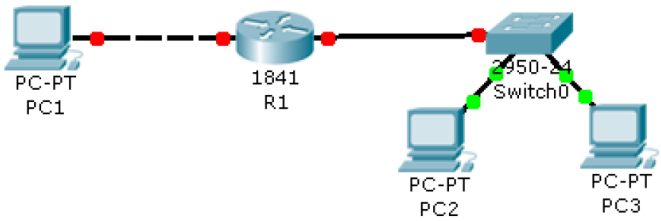

Рис. 4.3 - Модель мережі в Cisco Packet Tracer

3.1. Налаштування мережевих інтерфейсів комп'ютерів

Налаштуйте комп'ютери PC1, PC2, PC3, вказавши IP-адреса, маску і шлюз з таблиці 4.3. Налаштування IP-адрес персональних комп'ютерів в Cisco Packet Tracer була описана в методичних вказівках до лабораторної роботи №1.

3.2. Перевірка налаштувань комп'ютерів

Перевірте правильність налаштувань мережевого інтерфейсу комп'ютера PC1, PC2, PC3, виконавши команду ipconfig / all. У висновку команди на екран знайдіть встановлені раніше значення IP-адреси, маски і шлюзу.

3.3. Перевірка доступності вузлів мережі

Перевірте доступність мережевих вузлів за допомогою команди ping. При тестуванні мережі спочатку необхідно перевірити доступність найбільш близьких вузлів. Так, для PC1 необхідно спочатку перевірити доступність шлюзу:

```
PC>ping 198.133.219.1

Pinging 198.133.219.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.133.219.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Мережеве обладнання ще не налаштоване, тому частина мережевих пристроїв не доступна.

Виконайте таку послідовність дій:

- перевірте доступність інтерфейсу маршрутизатора Fa0 / 1 з комп'ютерів PC2 і PC3.

- досліджуйте доступність далеких інтерфейсів маршрутизатора (Fa0 / 0 с PC2, PC3; Fa0 / 1 з PC1)

- перевірте взаємну доступність PC2, PC3 і PC1.

Поясніть отримані результати.

3.4. Початкова настройка маршрутизатора

Початкова настройка маршрутизаторів практично не відрізняється від настройки комутаторів, розглянутої в роботі 2. Використовуючи вкладку командного рядка (CLI), виконайте наступні команди на маршрутизаторі R1:

```
Router>enable
Router #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
SR1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]? [OK]
Building configuration...
[OK]
```

3.5. Налаштування мережевих інтерфейсів маршрутизатора

Налаштування мережевих інтерфейсів маршрутизаторів також не відрізняється від настройки інтерфейсів комутаторів, однак на маршрутизаторах IP адреса задається на інтерфейсах, відповідних фізичним мережевим портам пристрою, а не на віртуальних інтерфейсів (interface VLAN), як це прийнято в комутаторах. Для настройки мережевого інтерфейсу маршрутизатора необхідно:

1. З привілейованого режиму перейти в режим конфігурації за допомогою команди configure terminal.

2. Вибрати фізичний інтерфейс, який ви плануєте налаштовувати. Зайти в режим конфігурації цього інтерфейсу, виконавши команду interface <Назва інтерфейсу>. У нашому випадку це інтерфейси FastEthernet0 / 0 і FastEthernet0 / 1 (список доступних інтерфейсів можна отримати в привілейований режим за допомогою команди #show ip interface brief).

3. У режимі конфігурації інтерфейсу задати опис інтерфейсу за допомогою команди description <будь-який текст>. Дія не є обов'язковим, але робити це настійно рекомендується.

4. В режимі конфігурації задати мережеву адресу. Для завдання IP адреси в IOS використовується команда ip address <IP> mask <MASK>, яка виконується в режимі конфігурації інтерфейсу.

5. Включити мережевий інтерфейс, для цього в режимі конфігурації інтерфейсу необхідно виконати команду no shutdown.

Нижче наведено приклад конфігурації інтерфейсу FastEthernet 0/0. При включенні інтерфейсу виводиться діагностичне повідомлення про -поднятіі‖ інтерфейсу FastEthernet0 / 0 (виділено сірим):

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#description --< link to LAN_1> --
R1(config-if)#ip address 198.133.219.1 255.255.255.240
R1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

R1(config-if)#
```

Аналогічним чином настройте інтерфейс fastEthernet 0/1:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/1
R1(config-if)#description --< link to LAN_2> --
R1(config-if)#ip address 198.133.219.17 255.255.255.240
R1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

R1(config-if)#
```

3.6 Перевірка настройки маршрутизатора

Перевірте правильність конфігурації маршрутизатора, виконавши в привілейованому режимі команду #show run:

```
R1#show running-config
Building configuration...
…
!
interface FastEthernet0/0
description --< link to LAN_1> --
ip address 198.133.219.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet0/1
description --< link to LAN_2 >--
ip address 198.133.219.17 255.255.255.240
duplex auto
speed auto
!
…
```

Сірим виділені зміни, які повинні з'явитися в налаштуваннях.

Потім виконайте в привілейованому режимі команду перегляду стану інтерфейсів show ip interface brief:

```
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0    198.133.219.1    YES manual up up
FastEthernet0/1    198.133.219.17   YES manual up up
Vlan1                unassigned        YES unset administratively down
down
```

Переконайтеся, що інтерфейси FastEthernet0 / 0 і FastEthernet0 / 1 знаходяться в стані -up‖.

3.7 Перевірка роботи мережі

Перевірте доступність комп'ютерів в мережі, виконавши на маршрутизаторі команду #ping:

```
R1#ping 198.133.219.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.14, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1
```

Знову перевірте доступність вузлів мережі з комп'ютера PC1. Нагадуємо, що при тестуванні необхідно спочатку перевірити доступність найбільш близьких вузлів і адрес, потім більш далеких, поступово наближаючись до кінцевого вузла. Так, для PC1 необхідно спочатку перевірити доступність шлюзу (адреса інтерфейсу FastEthernet0 / 0):

```
PC>ping 198.133.219.1

Pinging 198.133.219.1 with 32 bytes of data:
Reply from 198.133.219.1: bytes=32 time=0ms TTL=255
Reply from 198.133.219.1: bytes=32 time=0ms TTL=255
Reply from 198.133.219.1: bytes=32 time=10ms TTL=255
Reply from 198.133.219.1: bytes=32 time=10ms TTL=255

Ping statistics for 198.133.219.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 5ms
```

Потім перевірте доступність далекого інтерфейсу маршрутизатора fastEthernet0 / 1. Після цього можна перевірити доступність комп'ютерів PC2 і PC3.

3.8 Перегляд arp-таблиць

Перегляньте arp-таблицю маршрутизатора, виконавши в привілейованому режимі команду show arp:

```
R1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
  Internet  198.133.219.1                  -      0005.5ED4.7201  ARPA
FastEthernet0/0
Internet  198.133.219.14          8   00E0.8F2B.D86D  ARPA   FastEthernet0/0
Internet  198.133.219.17          -   0005.5ED4.7202  ARPA   FastEthernet0/1
Internet  198.133.219.29          6   00E0.8FA5.290C  ARPA   FastEthernet0/1
Internet  198.133.219.30          7   0030.F232.A79B  ARPA   FastEthernet0/1
```

Потім перегляньте arp-таблицю на комп'ютерах PC1, виконавши команду arp -a (рис. 4. 4).

```
PC>arp -a
  Internet Address      Physical Address      Type
  198.133.219.1         0005.5ed4.7201        dynamic

PC>
```

Рис. 4.4. Виведення arp-таблиці

Поясніть, чому в таблиці містяться тільки адреси пристроїв, що знаходяться в одній підмережі з комп'ютером, на якому виконувалася команда, а у маршрутізаторав таблиці присутні всі адреси.

Аналогічним чином виконайте наступні дії:

– Перевірте доступність шлюзу з комп'ютерів PC2 і PC3.

– Перевірте доступність -дальнего інтерфейса маршрутизатора з комп'ютерів PC2 і PC3.

– Переконайтеся за допомогою команди ping, що комп'ютерів PC2, і PC3 доступний PC1.

– Перевірте доступність комп'ютерів з маршрутизатора.

– Вивчіть arp-таблиці на комп'ютерах і маршрутизатор.

4. Контрольні питання

1. У чому полягає основна відмінність між комутатором і маршрутизатором?

2. Перерахуйте переваги технології VLSM перед класової адресацією?

3. Що зберігається в arp-таблиці?

4. Для чого використовуються arp-таблиці?

СПИСОК ЛІТЕРАТУРИ

1. М.А.Плоткін. Лекції з курсу «Мережі зв'язку та системи комутації». Тема 1 Комп'ютерні мережі. Основні визначення. Розділ «Комунікаційні пристрої і структуризація комп'ютерних мереж».
2. В.Г.Оліфер і ін. Комп'ютерні мережі. 4-е видання, ПІТЕР, 2010р. Глава 2 Загальні принципи побудови мереж.
3. Cisco Network Academy (netacad.com)
4. Джо Хабракена. Як працювати з маршрутизаторами Cisco. Пер. з англ. - М .: ДМК Пресс. 2005.
5. Пакет Cisco Packet Tracer, Tutorials (Getting Started, Logical Workspace, Configuring Devices, Realtime and Simulation Modes).

Навчальне видання

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни «Телекомунікаційні та інформаційні мережі»
для студентів спеціальності
172 " Телекомунікації та радіотехніка"
усіх форм навчання

Відповідальний за випуск А.С. Опанасюк
Редактор Н.З. Клочко
Комп'ютерне верстання К О. Д'яченко

Підп. до друку 11.06.2017, поз.
Формат 60х84/16. Ум. друк. арк. 2,09. Обл.-вид.арк. 1,62. Тираж 60 пр. Зам. №
Собівартість вид. грн.. к.

Видавець і виготовлювач
Сумський державний університет,
Вул. Римського – Корсакова, 2, м. Суми, 40007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.2007.