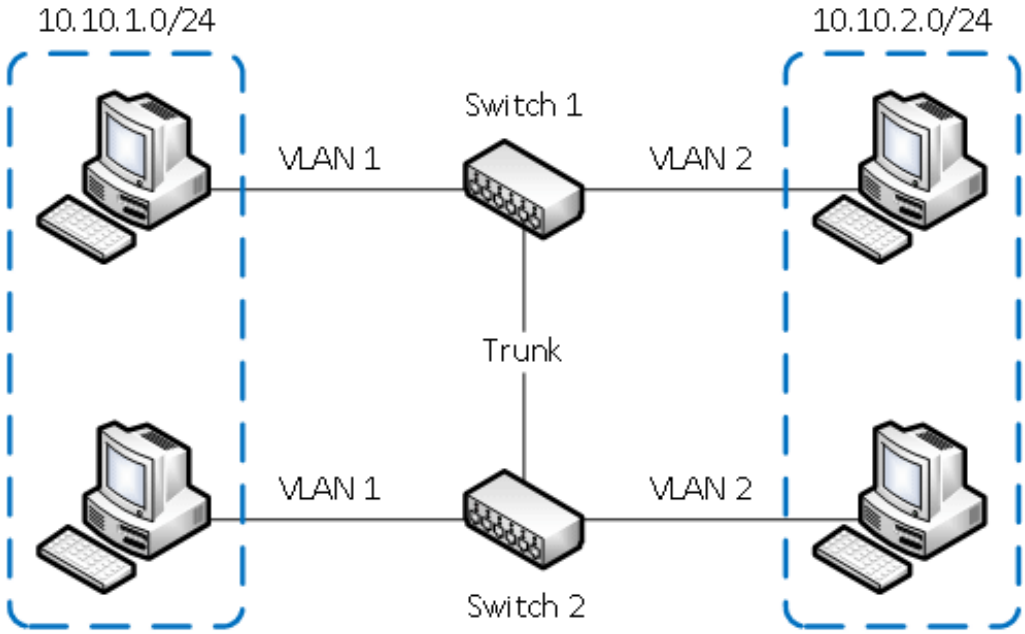
Поняття VLAN, Trunk та протоколи VTP і DTP

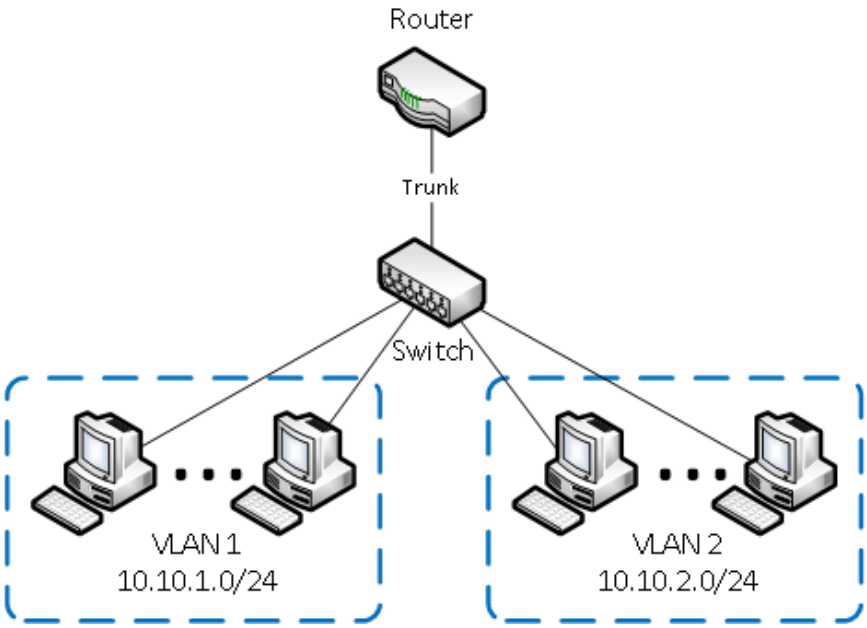
VLAN (Virtual Local Area Network, віртуальна локальна мережа) – це функція в роутерах і комутаторах, що дозволяє одному фізичному мережевому інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка не залежить від фізичної топології.

Приклади використання VLAN

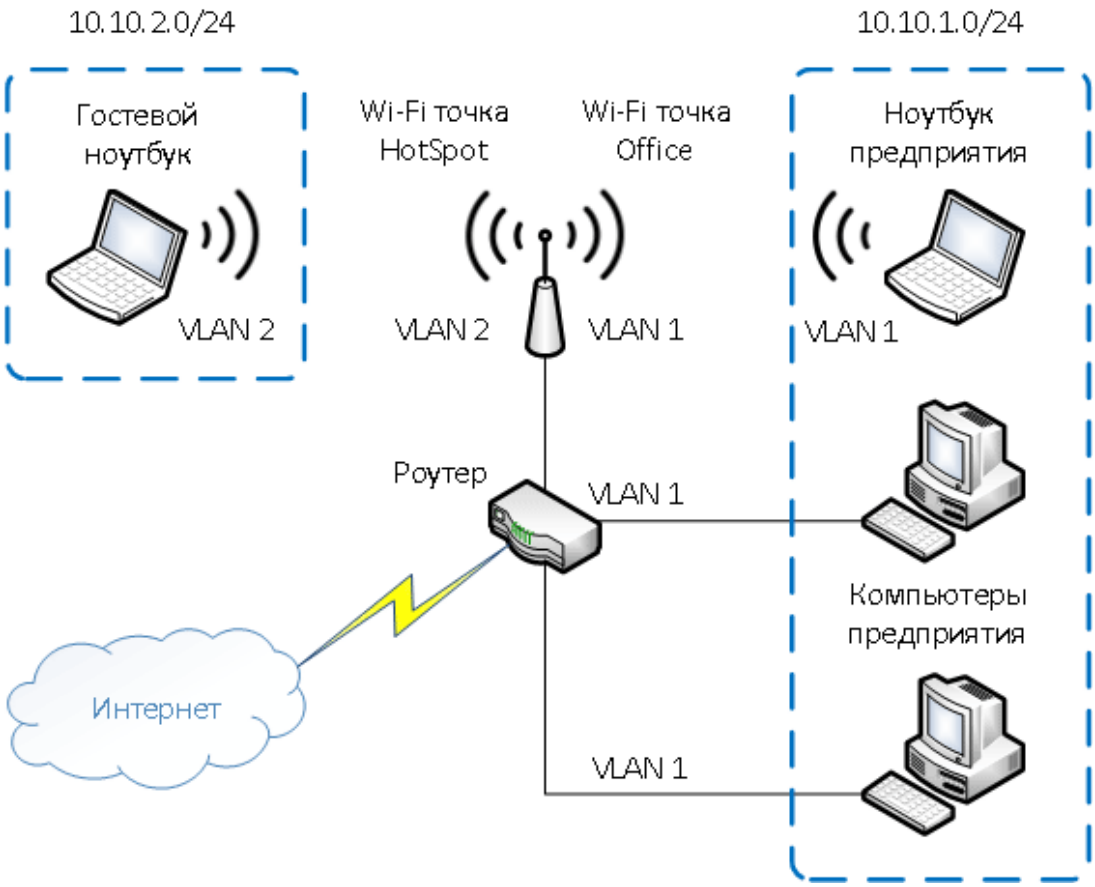
- **Об'єднання в єдину мережу комп'ютерів, підключених до різних комутаторів.** Допустимо, у вас є комп'ютери, які підключені до різних свічів, але їх потрібно об'єднати в одну мережу. Одні комп'ютери ми об'єднаємо у віртуальну локальну мережу VLAN 1, а інші — у мережу VLAN 2. Завдяки функції VLAN комп'ютери в кожній віртуальній мережі будуть працювати, немов підключені до одного й того ж свіча. Комп'ютери з різних віртуальних мереж VLAN 1 та VLAN 2 будуть невидимі один для одного.



- **Поділ у різні підмережі комп'ютерів, підключених до одного комутатора**. На рисунку комп'ютери фізично підключені до одного свіча, але розділені в різні віртуальні мережі VLAN1 та VLAN 2. Комп'ютери з різних віртуальних підмереж будуть невидимі один для одного.



- **Поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства.** На рис. до роутера підключена фізично одна Wi-Fi точка доступу. На точці створено дві віртуальні Wi-Fi точки з назвами HotSpot та Office. До HotSpot будуть підключатися Wi-Fi гостьові ноутбуки для доступу до інтернету, а до Office - ноутбуки підприємства. З метою безпеки необхідно, щоб гостьові ноутбуки не мали доступу до мережі підприємства. Для цього комп'ютери підприємства та віртуальна Wi-Fi точка Office об'єднані у віртуальну локальну мережу VLAN 1, а гостьові ноутбуки будуть знаходитись у віртуальній мережі VLAN 2. Гостьові ноутбуки з мережі VLAN 2 не матимуть доступу до мережі підприємства VLAN 1.

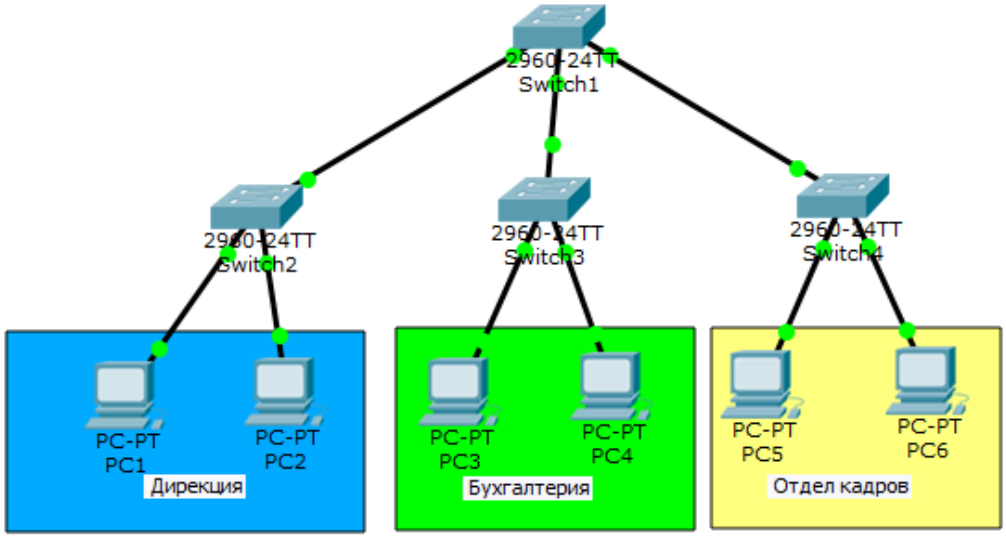


Переваги використання VLAN

- **Гнучкий поділ пристроїв на групи**. Як правило, одному VLAN відповідає одна підмережа. Комп'ютери, що знаходяться в різних VLAN, будуть ізольовані один від одного. Також можна поєднати в одну віртуальну мережу комп'ютери, підключені до різних комутаторів.
- **Зменшення широкомовного трафіку в мережі.** Кожен VLAN є окремим широкомовним доменом. Широкомовний трафік не транслюватиметься між різними VLAN. Якщо на різних комутаторах налаштувати той самий VLAN, то порти різних комутаторів утворюватимуть один широкомовний домен.
- **Збільшення безпеки та керованості мережі.** У мережі, розбитій на віртуальні підмережі, зручно застосовувати політики та правила безпеки для кожного VLAN. Політика буде застосована до цілої підмережі, а не до окремого пристрою.
- **Зменшення кількості обладнання та мережевого кабелю.** Для створення нової віртуальної локальної мережі не потрібно купувати комутатор і прокладати мережний кабель. Однак, ви повинні використовувати більш дорогі керовані комутатори з підтримкою VLAN.

Налаштування VLAN

З'являється все більше пристроїв, які навантажують мережу або ще гірше - створюють загрозу в безпеці. А, як правило, "небезпека" з'являється раніше "безпеки". Нині на найпростішому прикладі покажемо це.

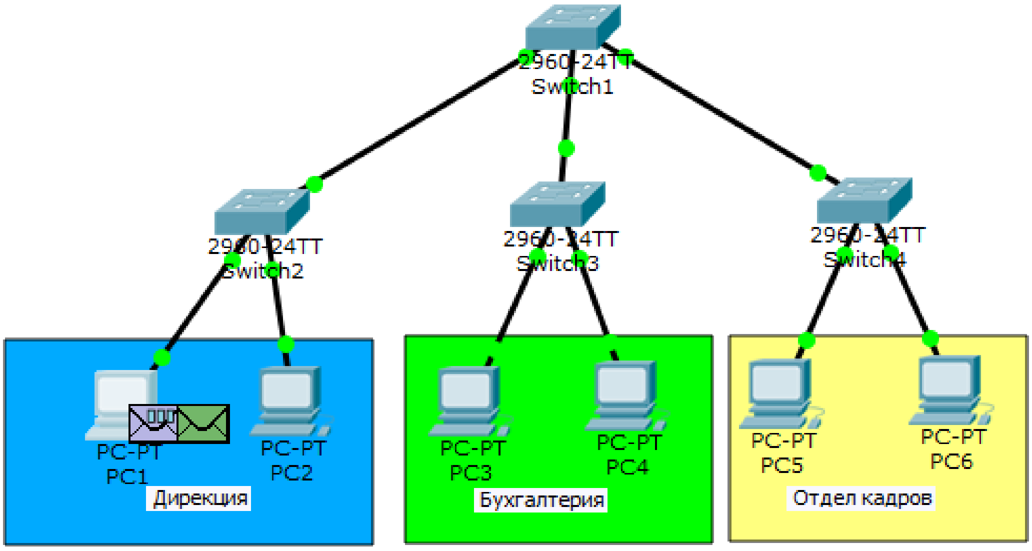


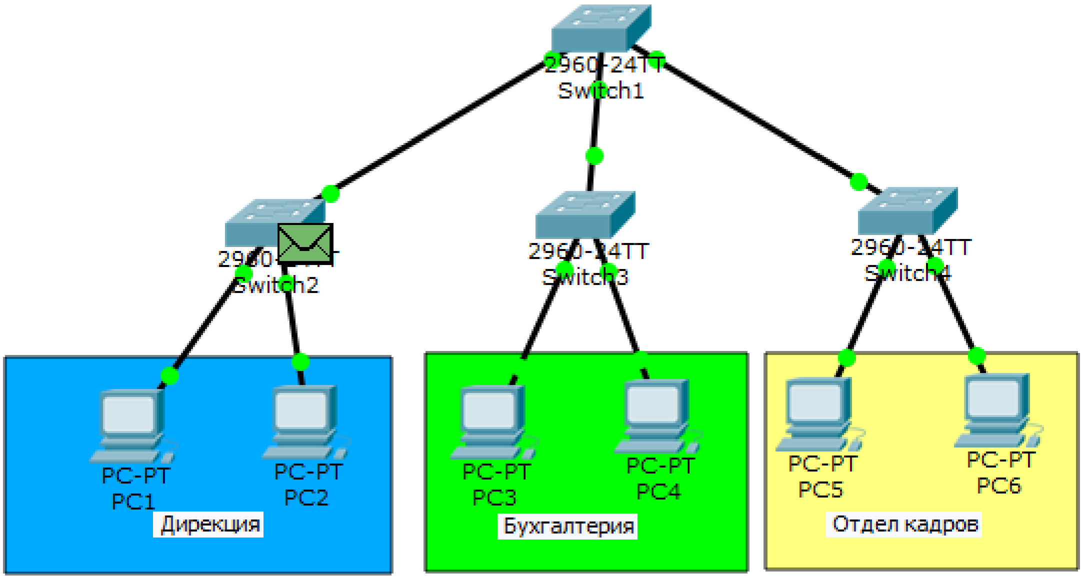
Ми поки не зачіпатимемо маршрутизатори та різні підмережі. Допустимо всі вузли знаходяться в одній підмережі.

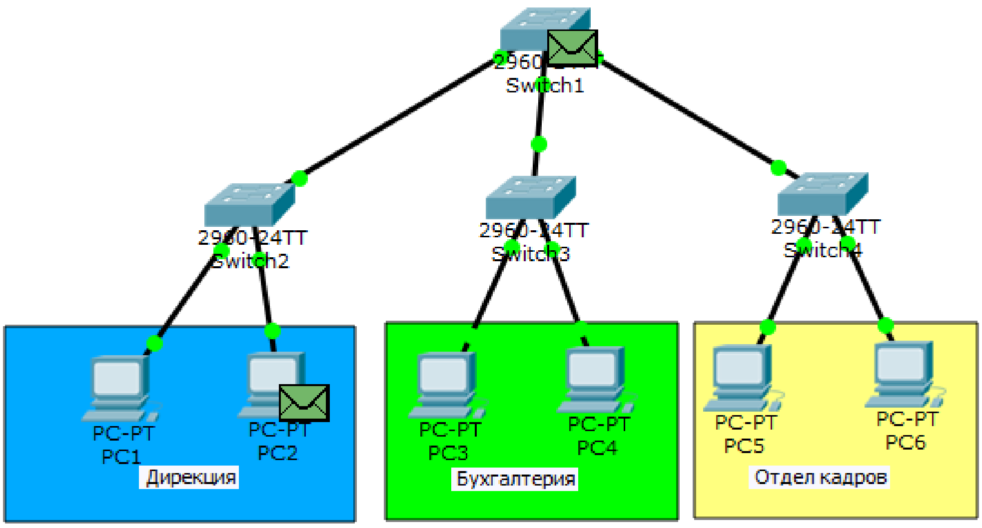
Наведемо список IP-адрес:

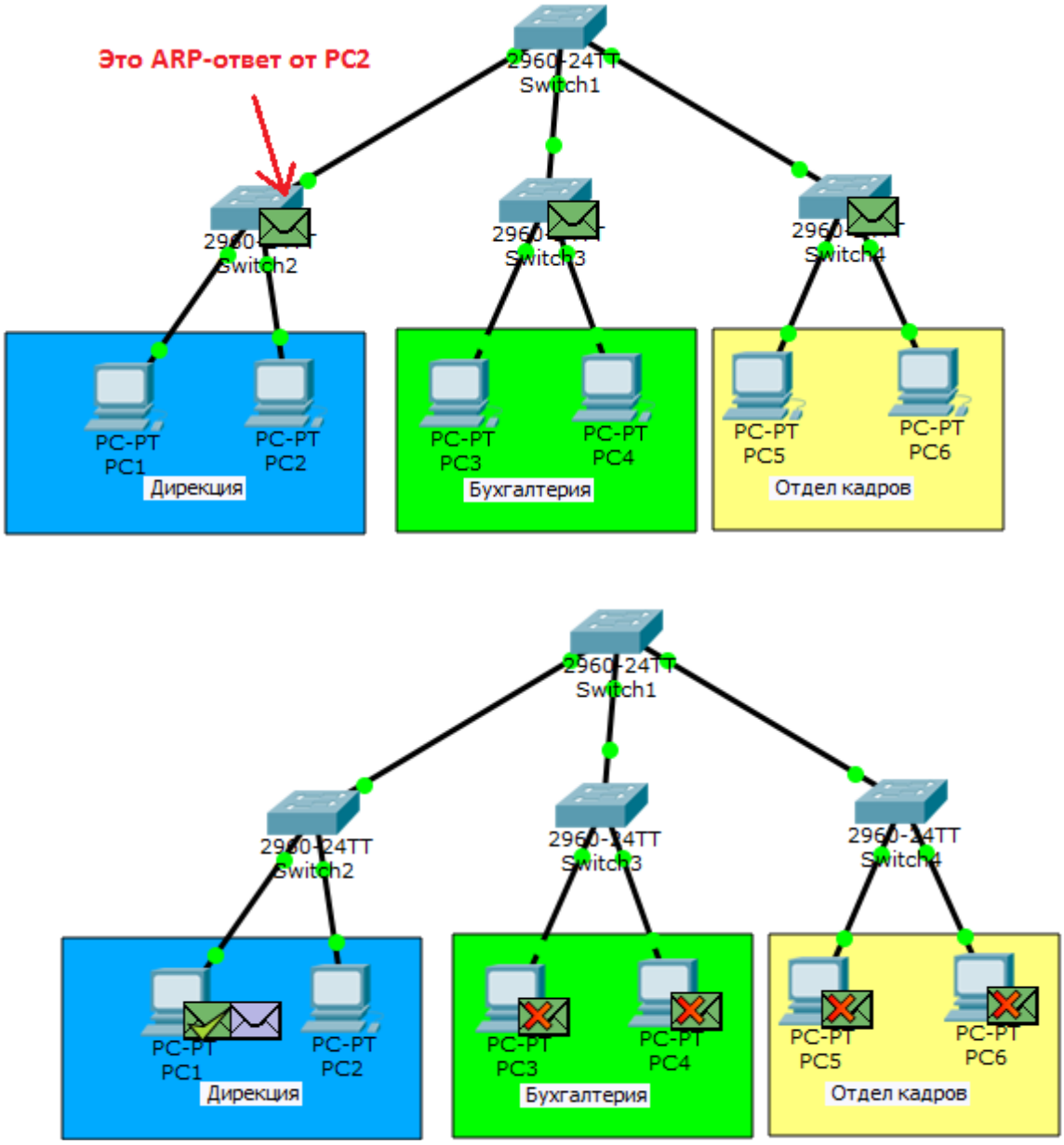
1. PC1 – 192.168.1.2/24
2. PC2 – 192.168.1.3/24
3. PC3 – 192.168.1.4/24
4. PC4 – 192.168.1.5/24
5. PC5 – 192.168.1.6/24
6. PC6 – 192.168.1.7/24

У нас 3 відділи: дирекція, бухгалтерія, відділ кадрів. У кожного відділу свій комутатор і з'єднані через центральний верхній. І ось PC1 надсилає ping на комп'ютер PC2.









ping от PC1 до PC5

Робота протоколу ARP. Оскільки PC1 не знає MAC-адресу (або адресу к анального рівня) PC2, то він відправляє в розвідку ARP, щоб той йому повідомив. Він приходить на комутатор, звідки ретранслюється на всі активні порти, тобто PC2 і на центральний комутатор. З центрального комутатора вилетить на сусідні комутатори і так далі, доки не дійде до всіх. Ось такий маленький трафік викликало одне ARP-повідомлення. Його отримали усі учасники мережі. Великий і непотрібний трафік – це перша проблема. Друга проблема – це безпека. Думаю, помітили, що повідомлення сягнуло навіть бухгалтерії, комп'ютери якої взагалі не брали участі в цьому. Будь-який зловмисник, підключившись до будь-якого комутатора, матиме доступ до всієї мережі. У принципі, мережі раніше так і працювали. Комп'ютери знаходилися в одному канальному середовищі та поділялися лише за допомогою маршрутизаторів. Але час минав і треба було вирішувати цю проблему на канальному рівні. Cisco, як піонер, вигадала свій протокол, який тегував кадри і визначав приналежність до певного канального середовища. Він називався ISL (Inter-Switch Link). Ідея ця сподобалася всім та IEEE вирішили розробити аналогічний відкритий стандарт. Стандарт отримав назву 802.1q. Набув він величезного поширення і Cisco вирішила теж перейти на нього. І ось технологія VLAN грунтується на роботі протоколу 802.1q. Давайте вже почнемо говорити про неї.

Вигляд ethernet-кадру. Вигляд не тегованого кадру.

Ethernet-кадр					
8 байт	6 байт	6 байт	2 байта	46-1500 байт	4 байта
Преамбула	MAC-адрес полу-чателя	MAC-адрес источника	Тип(длина)	SNAP/LLC и данные	FCS(Frame Check Sequence)-контроль суммы

Тегований.

Кадр 802.1Q						
8 байт	6 байт	6 байт	4 байта	2 байта	46-1500 байт	4 байта
Преамбула	MAC-адрес получателя	MAC-адрес отправи-теля	Тег	Тип (Длина)	SNAP/LLC и данные	FCS

2 байта	3 бита	1 бит	12 бит
TPID (Tag Protocol ID)	PCP (Priority Cod Point)	CFI (Canonical Format Indicator)	VID (VLAN ID)

З'являється **Тег**. Складається з 4-х частин.

1) **TPID (англ. Tag Protocol ID) або Ідентифікатор тегованого протоколу** – складається з 2-х байт і для VLAN завжди рівний 0x8100.
2) **PCP (англ. Priority Code Point) или значение приоритета** — складається з 3-х біт. Використовується для пріоритезації трафіка. Адміністратори знають, як правильно їм керувати, коли в мережі є різний трафік (голос, відео, дані)
3) **CFI (англ. Canonical Format Indicator) або індикатор канонічного формату –** просте поле, складається з одного біта. Якщо стоїть 0, то це стандартний формат MAC-адреси.
4) **VID (англ. VLAN ID) або ідентифікатор VLAN** — складається з 12 біт і показує, в якому VLAN знаходиться кадр.

Тегування кадрів здійснюється між мережними пристроями (комутатори, маршрутизатори тощо), а між кінцевим вузлом (комп'ютер, ноутбук) та мережевим пристроєм кадри не тегуються. Тому порт мережного пристрою може бути в 2-х станах: **access** або **trunk**.

- **Access port або порт доступу** — порт, що знаходиться в певному VLAN і передає не теговані кадри. Як правило, це порт, що дивиться на пристрій користувача.
- **Trunk port або магістральний порт** — порт, який передає тегований трафік. Як правило, цей порт піднімається між мережними пристроями.

Покажемо це на практиці. Відкриємо комутатор і подивимось що в нього з VLAN.

Набираємо команду **show vlan**.

```
Switch#show vlan

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
                                                 Gig0/1, Gig0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Вишиковуються кілька таблиць. Нам по суті важлива лише перша. Тепер покажу, як її читати.

1 стовпець – це номер VLAN. Тут спочатку є номер 1 — це стандартний VLAN, який спочатку є на кожному комутаторі. Він виконує ще одну функцію, яку трохи нижче напишу. Також присутні зарезервовані із 1002-1005. Це для інших канальних середовищ, які навряд чи зараз використовуються. Видалити їх також не можна.

```
Switch(config)#no vlan 1005
Default VLAN 1005 may not be deleted.
```

Коли ви видаляєте Cisco, виводиться повідомлення, що цей VLAN не можна видалити. Тому живемо і ці 4 VLAN не чіпаємо.

2 стовпець – це ім'я VLAN. При створенні VLAN, ви можете на власний розсуд вигадувати їм осмислені імена, щоб потім їх ідентифікувати. Тут вже є default, fddi-default, token-ring-default, fddinet-default, trnet-default.

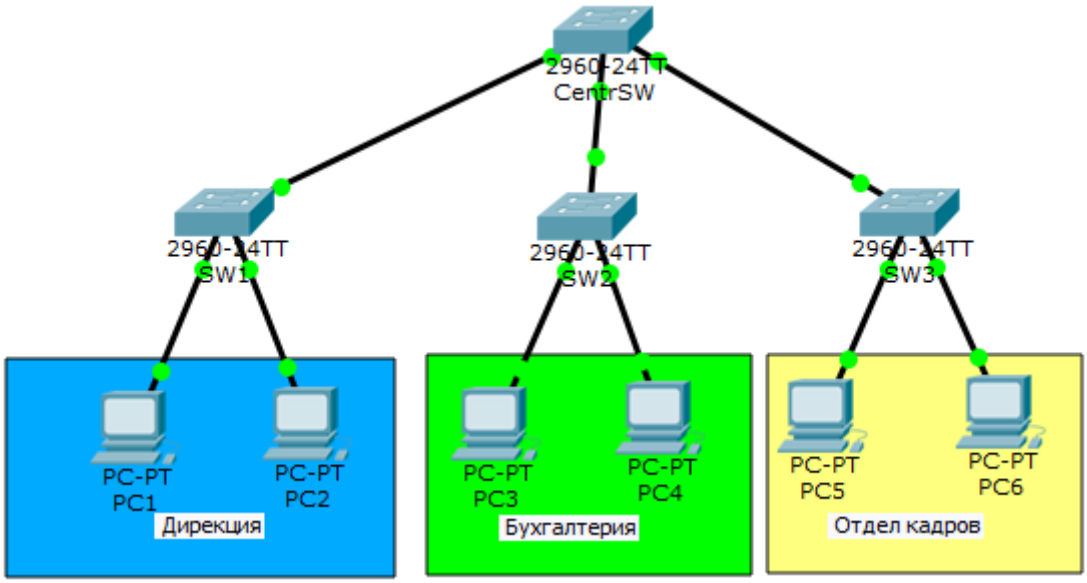
3 стовпець - статус. Тут з'являється який стан VLAN. На даний момент VLAN 1 або default може active, а 4 наступних act/unsup (хоч і активні, але не підтримуються).

4 стовпець - порти. Тут показано до яких VLAN належать порти. Зараз, коли ми ще нічого не чіпали, вони перебувають у default.

Приступаємо до настроювання комутаторів. Правилом гарного тону дати комутаторам осмислені імена. Чим і займемося. Наводжу команду.

```
Switch(config)#hostname CentrSW
CentrSW(config)#
```

Інші налаштовуються аналогічно, тому покажу оновлену схему топології.



Почнемо налаштування з комутатора SW1. Для початку створимо VLAN на комутаторі.

```
SW1(config)#vlan 2 -  создаем VLAN 2 (VLAN 1 по замовчанню зарезервований, тому беремо наступний).
SW1(config-vlan)#name Dir-ya - попадаємо в налаштування VLAN та задаємо йому ім’я.
```

VLAN створено. Тепер переходимо до портів. Інтерфейс FastEthernet0/1 дивиться на PC1, а FastEthernet0/2 на PC2. Як говорили раніше, кадри з-поміж них повинні передаватися не тегованими, тому переведемо в стан Access.

```
SW1(config)#interface fastEthernet 0/1 - переходимо до налаштування 1-го порта.
SW1(config-if)#switchport mode access - переводимо порт в режим access.
SW1(config-if)#switchport access vlan 2 - закріпляємо за портом 2-й VLAN.
SW1(config)#interface fastEthernet 0/2 - переходим к настройке 2-го порта.
SW1(config-if)#switchport mode access - переводимо порт в режим access.
SW1(config-if)#switchport access vlan 2 - закріпляємо за портом 2-й VLAN.
```

Так як обидва порти закріплюються під однаковим VLAN-ом, їх ще можна було налаштувати групою.

```
SW1(config)#interface range fastEthernet 0/1-2 - тобто вибираємо пул и далі налаштування аналогічне.
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 2
```

Налаштували access порти. Тепер налаштуємо trunk між SW1 та CentrSW.

```
SW1(config)#interface fastEthernet 0/24 - переходимо до налаштування 24-го порта.
SW1(config-if)#switchport mode trunk - переводимо порт в режим 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

Відразу бачимо, що порт переналаштувався. У принципі, для роботи цього достатньо. Але з точки зору безпеки дозволяти для передачі потрібно тільки ті VLAN, які дійсно необхідні. Приступимо.

SW1(config-if)#switchport trunk allowed vlan 2 - дозволяємо передавати тільки 2-ой VLAN.

Без цієї команди будуть передаватися всі наявні VLAN. Подивимося, як змінилася таблиця командою **show vlan**.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gig0/1, Gig0/2
2    Dir-ya                           active    Fa0/1, Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

З'явився другий VLAN з ім'ям Dir-ya і бачимо порти, що належать йому fa0/1 і fa0/2.

Щоб вивести лише верхню таблицю, можна скористатись командою **show vlan brief**.

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gig0/1, Gig0/2
2    Dir-ya                           active    Fa0/1, Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Можна ще зменшити вивід даних, якщо вказати певний ID VLAN.

```
SW1#show vlan id 2

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
2    Dir-ya                              active    Fa0/1, Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Або його ім’я

```
SW1#show vlan name Dir-ya

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
2    Dir-ya                              active    Fa0/1, Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Вся інформація про VLAN зберігається у flash пам'яті у файлі vlan.dat.

```
SW1#show flash:
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    6  -rw-        1196          <no date>  config.text
    5  -rw-         616          <no date>  vlan.dat

64016384 bytes total (59599651 bytes free)
```

Як ви помітили, в жодній з команд немає інформації про trunk. Її можна переглянути іншою командою **show interfaces trunk**.

```
SW1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      2

Port        Vlans allowed and active in management domain
Fa0/24      2

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      2
```

Тут є інформація і про trunk порти, і про те, які VLAN вони передають. Ще тут є стовпець Native vlan. Це якраз той трафік, який не має тегуватись. Якщо на комутатор приходить не тегований кадр, він автоматично зараховується до Native Vlan (за замовчуванням і в нашому випадку це VLAN 1). Native VLAN можна, а багато хто говорить, що потрібно міняти з метою безпеки. Для цього в режимі налаштування транкового порту потрібно застосувати команду - **switchport trunk native vlan X, де X - номер VLAN, що присвоюється**. У цій топології ми не змінюватимемо, але знати, як це робити корисно.

Залишилося налаштувати інші пристрої.

CentrSW:
Центральний комутатор є сполучною ланкою, а значить він повинен знати про всі VLAN-и. Тому спочатку створюємо їх, а потім переводимо усі інтерфейси у транковий режим.

```
CentrSW(config)#vlan 2
CentrSW(config-vlan)# name Dir-ya
CentrSW(config)#vlan 3
CentrSW(config-vlan)# name buhgalter
CentrSW(config)#vlan 4
CentrSW(config-vlan)# name otdel-kadrov
CentrSW(config)#interface range fastEthernet 0/1-3
CentrSW(config-if-range)#switchport mode trunk
```

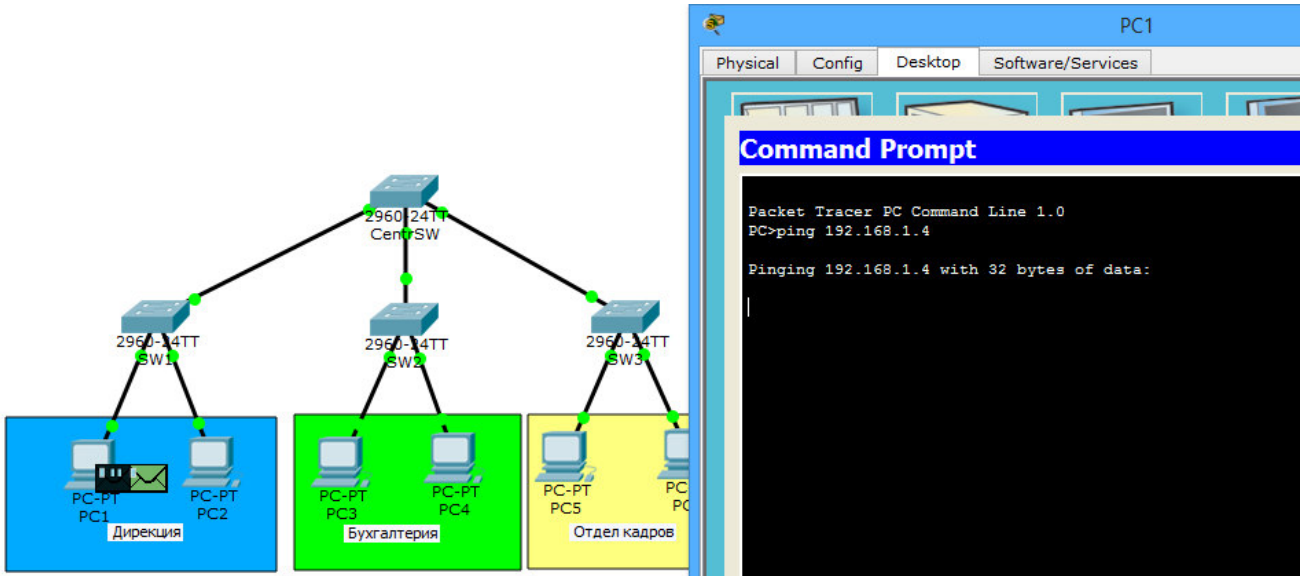
Не забуваємо зберігати конфіг. Команда **copy running-config startup-config.**
SW2:

```
SW2(config)#vlan 3
SW2(config-vlan)#name buhgalter
SW2(config)#interface range fastEthernet 0/1-2
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 3
SW2(config)#interface fastEthernet 0/24
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 3
```

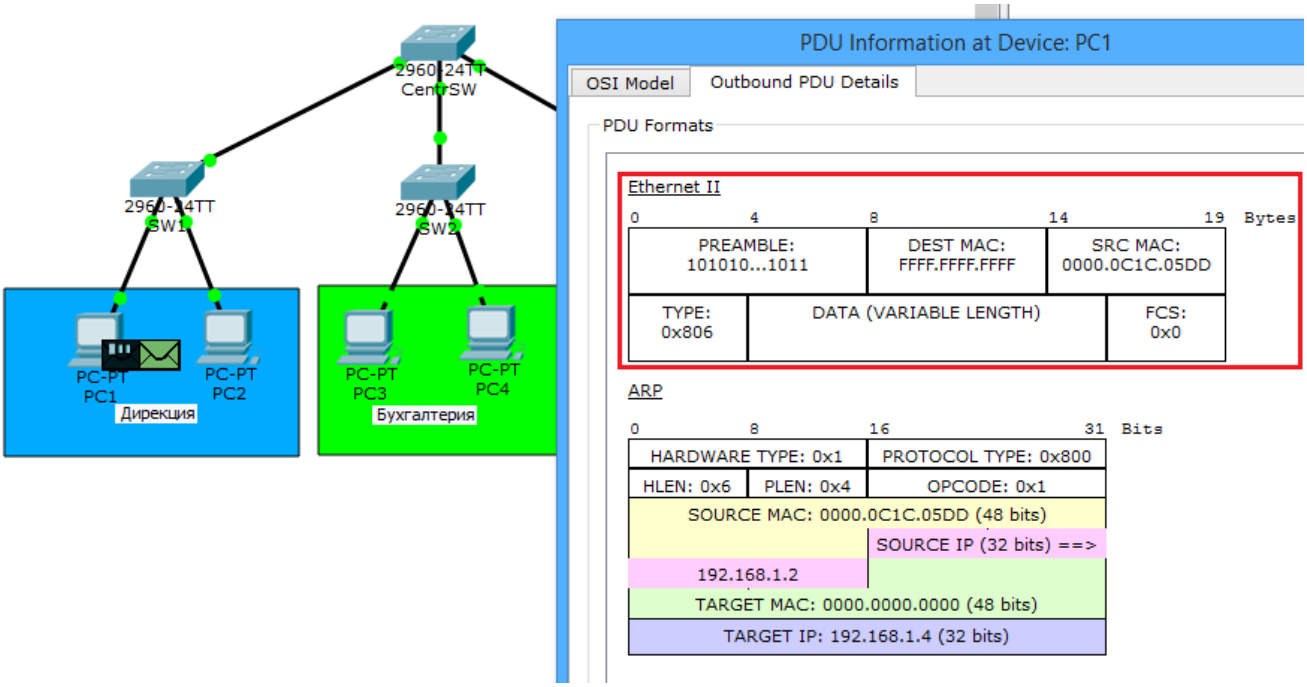
SW3:

```
SW3(config)#vlan 4
SW3(config-vlan)#name otdel kadrov
SW3(config)#interface range fastEthernet 0/1-2
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 4
SW3(config)#interface fastEthernet 0/24
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk allowed vlan 4
```

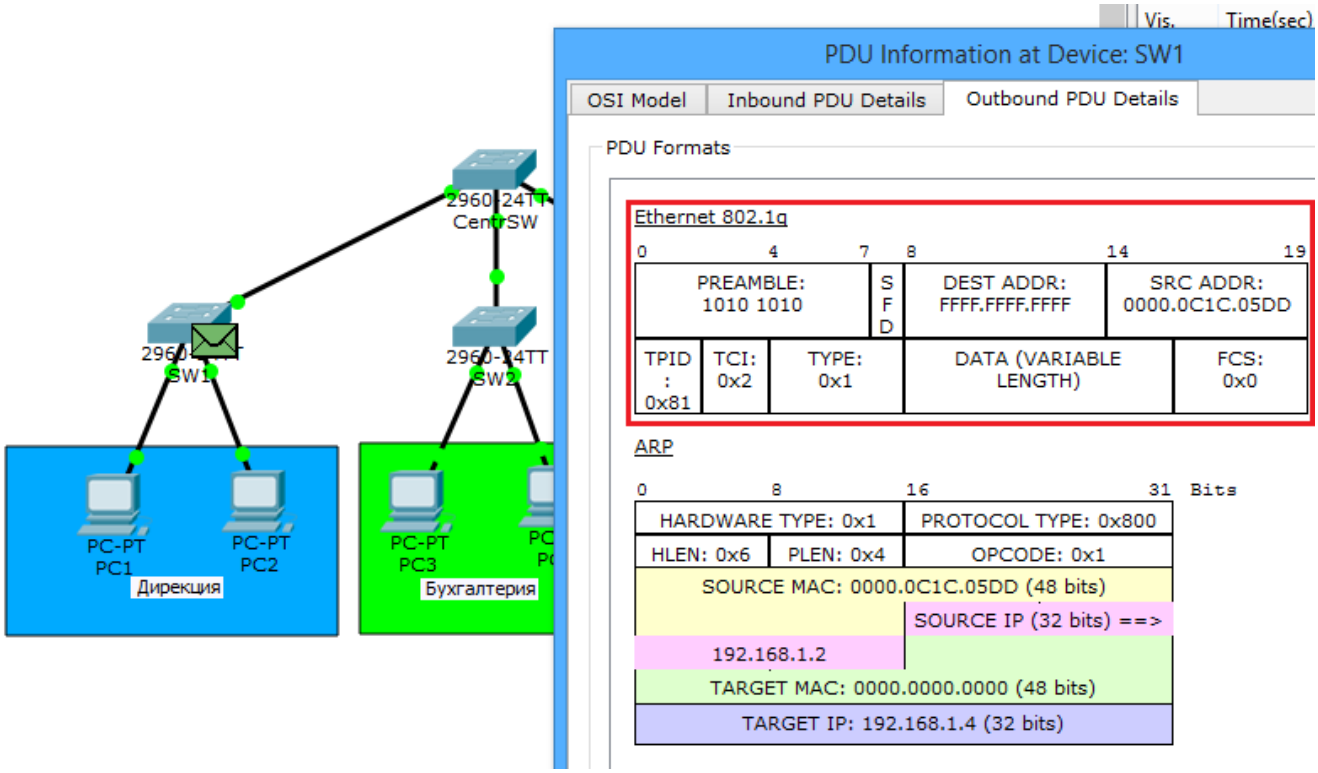
Зверніть увагу на те, що ми підняли та налаштували VLAN, але адресацію вузлів залишили такою самою. Тобто фактично всі вузли в одній підмережі, але розділені VLAN-ами. Так робити не можна. Кожному VLAN треба виділяти окрему мережу. Я це зробив виключно у навчальних цілях. Якби кожен відділ сидів у своїй підмережі, то вони б апріорі були обмежені, тому що комутатор не вміє маршрутизувати трафік з однієї підмережі до іншої (плюс це вже обмеження на мережному рівні). А нам треба обмежити відділи на канальному рівні.
Знову відправляю ping з PC1 PC3.



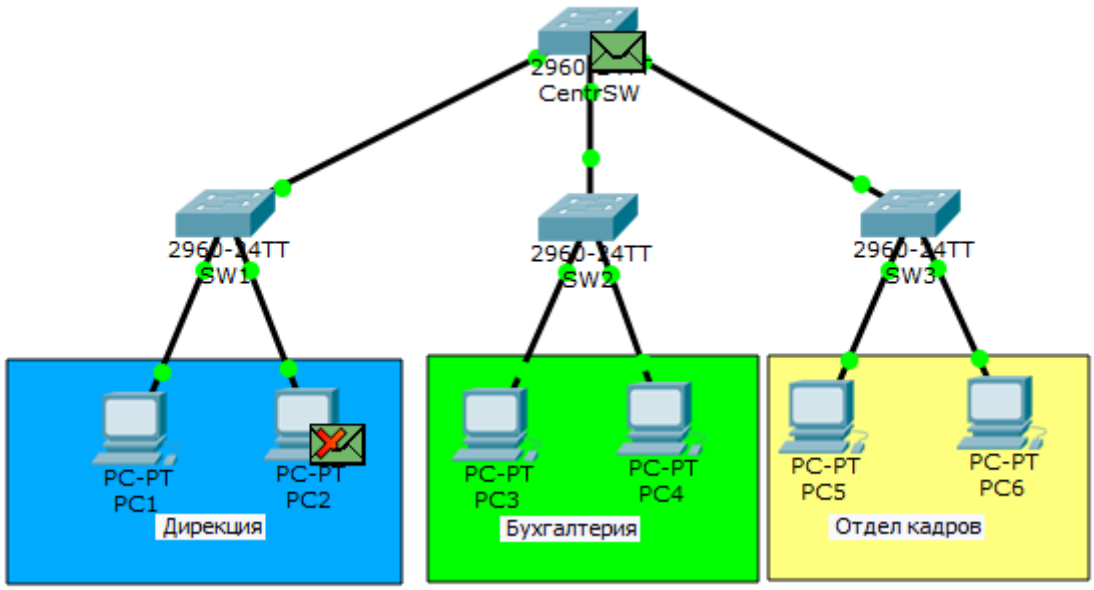
Йде в хід ARP, який нам і потрібний зараз. Відкриємо його.



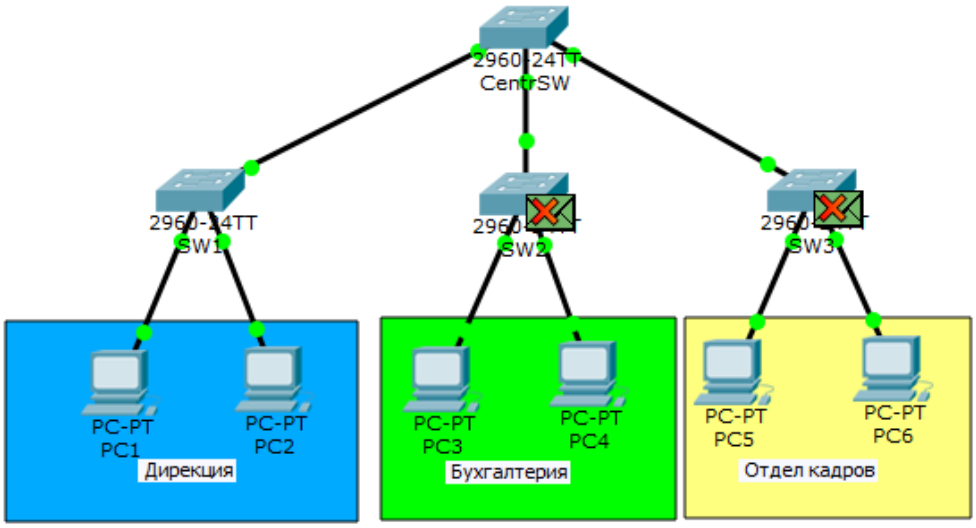
Поки що нічого нового. ARP інкапсульований у ethernet.



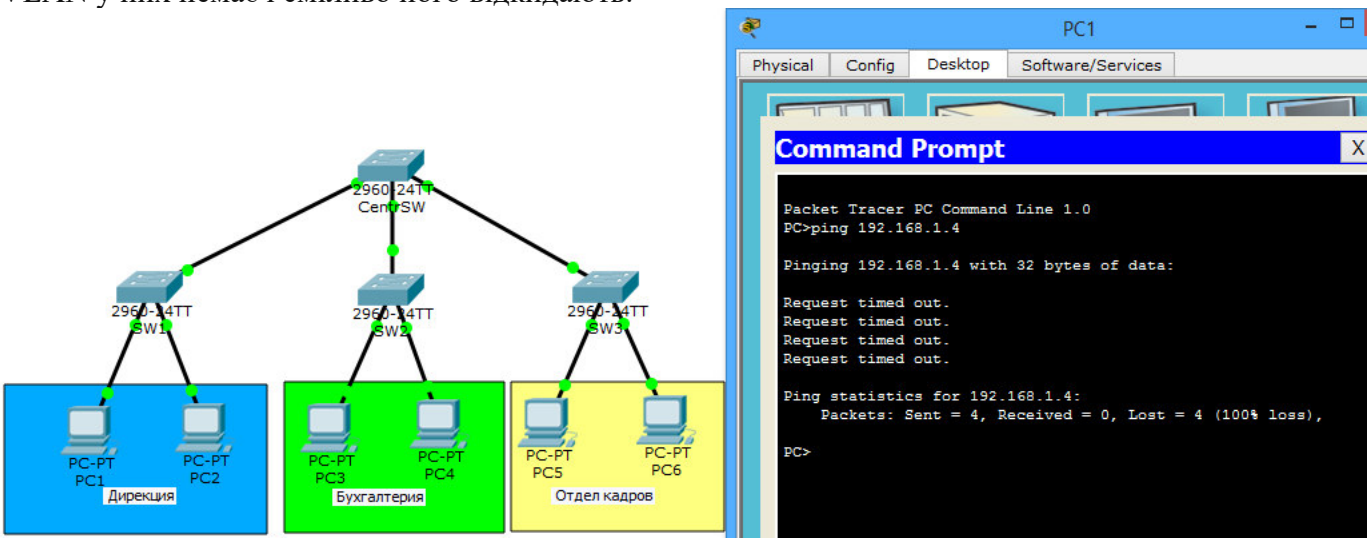
Кадр прилітає на комутатор та тегується. Тепер там не звичайний ethernet, а 802.1q. Додалися поля, про які писав раніше. Це **TPID**, який дорівнює 8100 і показує, що це 802.1q. Та **TCI**, який об'єднує 3 поля **PCP, CFI і VID**. Число, яке в цьому полі – це номер VLAN. Рухаємось далі.



Після тега він відправляє кадр на PC2 (оскільки він у тому ж VLAN) і на центральний комутатор по транковому порту.

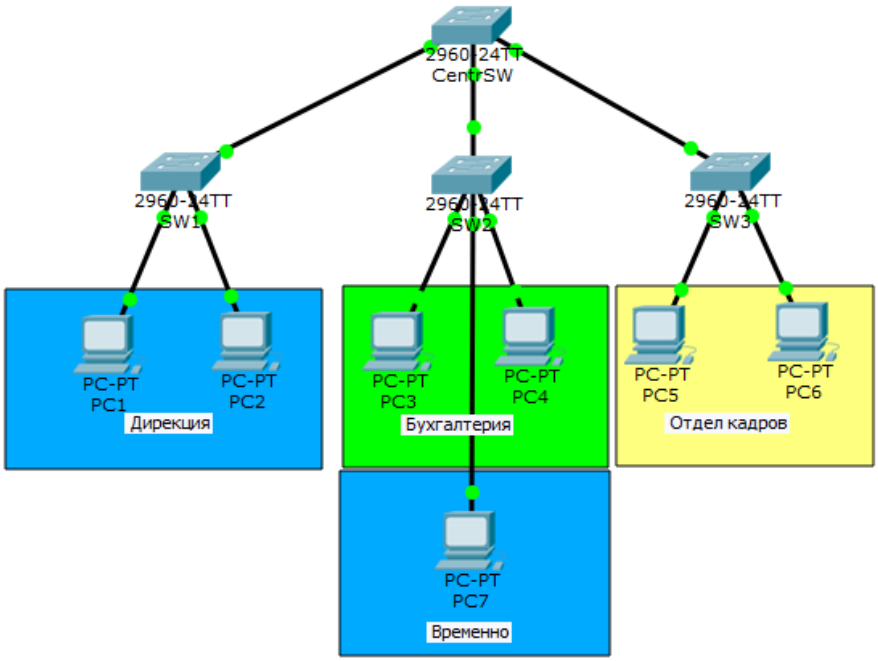


Так як жорстко не було прописано які типи VLAN пропускати по яких портах, він відправить на обидва комутатора. І ось тут комутатори, побачивши номер VLAN, розуміють, що пристроїв з таким VLAN у них немає і сміливо його відкидають.



PC1 очікує відповідь, яка так і не приходить.

Тепер така ситуація. До складу дирекції наймають ще одну людину, але в кабінеті дирекції немає місця і на якийсь час просять розмістити людину у відділі бухгалтерії. Вирішуємо цю проблему.



Подключили компьютер к порту FastEthernet 0/3 коммутатора и присвою IP-адрес 192.168.1.8/24. Теперь настрою коммутатор **SW2**. Так как компьютер должен находиться во 2-ом VLAN, о котором коммутатор не знает, то создам его на коммутаторе.

```
SW2(config)#vlan 2
SW2(config-vlan)#name Dir-ya
```

Далі налаштовуємо порт FastEthernet 0/3, який дивиться на PC7.

```
SW2(config)#interface fastEthernet 0/3
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 2
```

І останнє — налаштувати транковий порт.

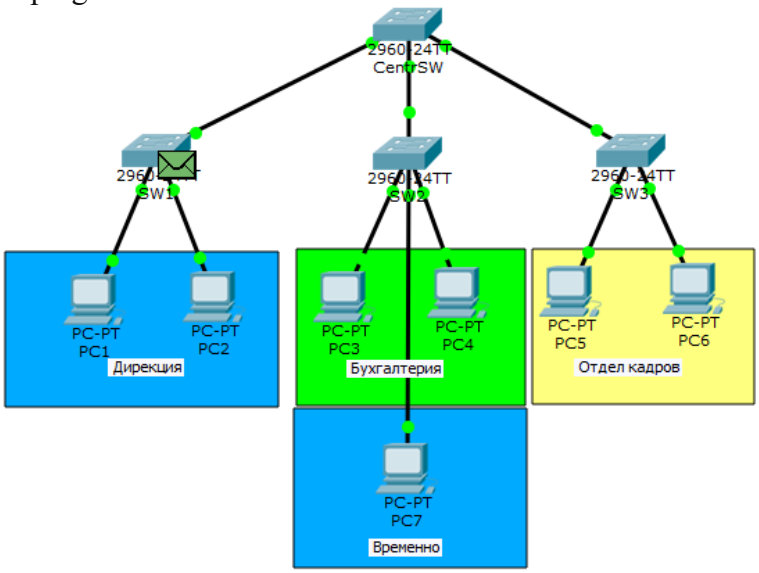
```
SW2(config)#interface fastEthernet 0/24
SW2(config-if)#switchport trunk allowed vlan add 2 – зверніть увагу на цю команду.
```

А саме на ключове слово **add**. Якщо не дописати це слово, ви зітрете всі інші дозволені для передачі VLAN на цьому порту. Тому якщо у вас вже було піднято транк на порту і передавалися інші VLAN, то треба додавати саме так.

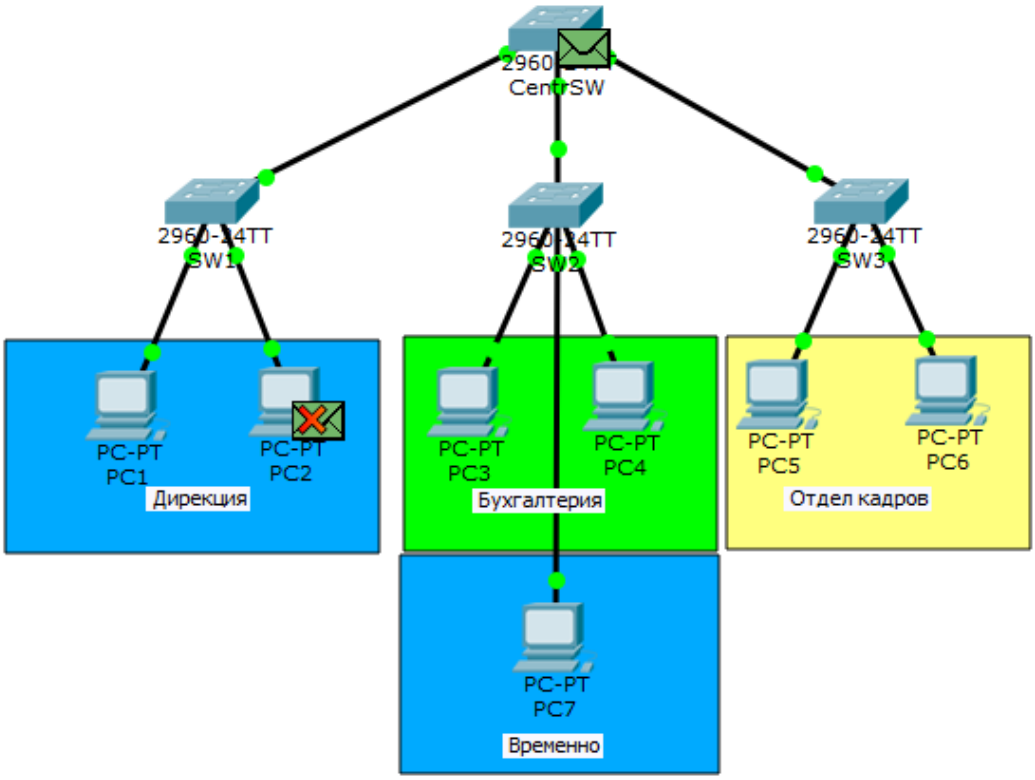
Щоб кадри ходили гарно, підкоригуємо центральний комутатор **CentrSW.**

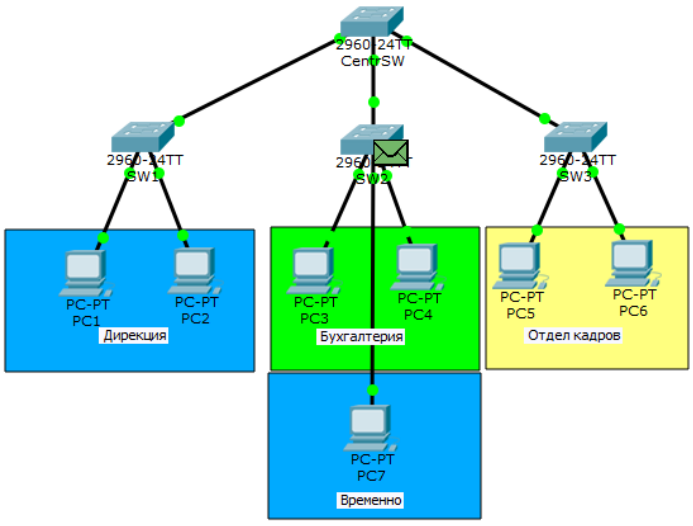
```
CentrSW(config)#interface fastEthernet 0/1
CentrSW(config-if)#switchport trunk allowed vlan 2
CentrSW(config)#interface fastEthernet 0/2
CentrSW(config-if)#switchport trunk allowed vlan 2,3
CentrSW(config)#interface fastEthernet 0/3
CentrSW(config-if)#switchport trunk allowed vlan 4
```

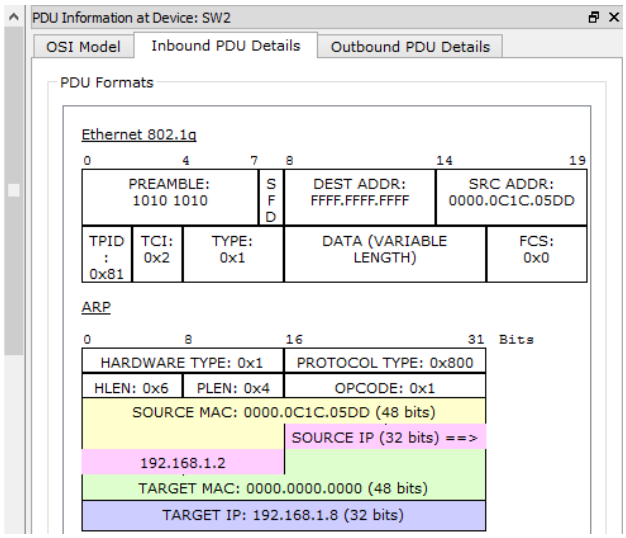
Перевірка. Відправляємо ping з PC1 на PC7.



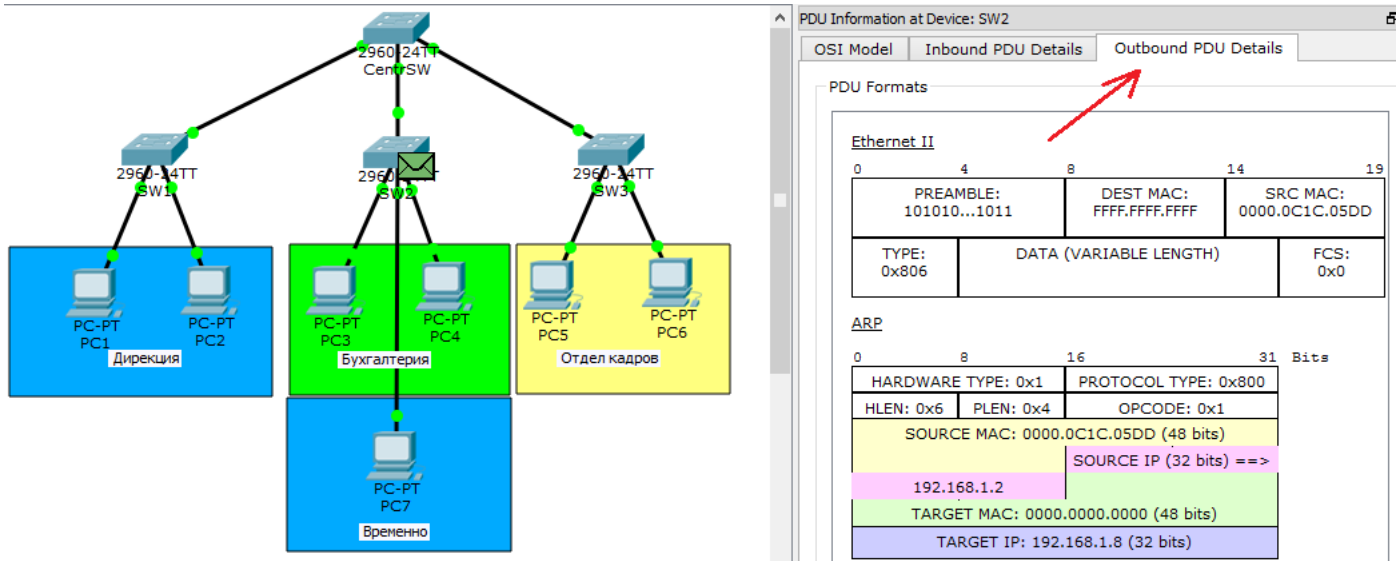
Поки що весь шлях аналогічний до попереднього. Але з цього моменту (з картинки нижче) центральний комутатор прийме інше рішення. Він отримує кадр і бачить, що той протегований другим VLAN-ом. Отже, відправляти його треба тільки туди, де це дозволено, тобто на порт fa0/2.





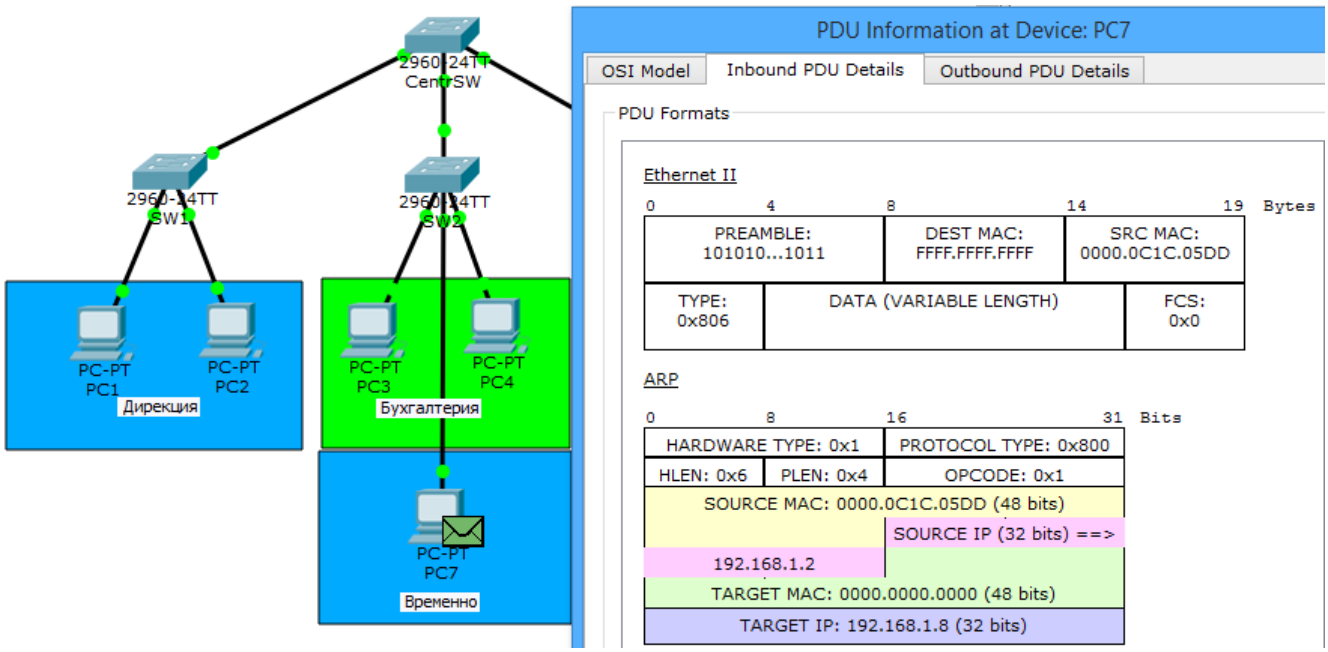


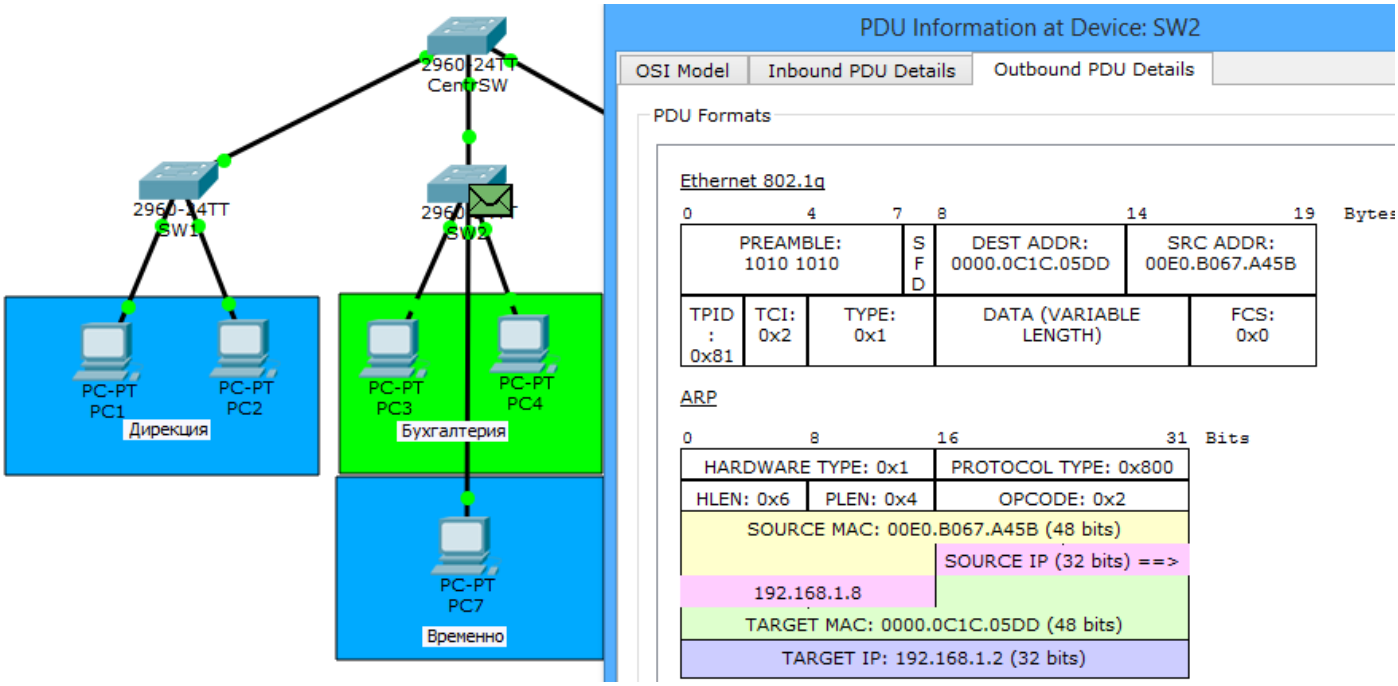
І ось він приходить на SW2. Відкриваємо та бачимо, що він ще тегований. Але наступним вузлом стоїть комп'ютер, і тег треба знімати. Натискаємо на **Outbound PDU Details**, щоб подивитися в якому вигляді кадр вилетить з комутатора.



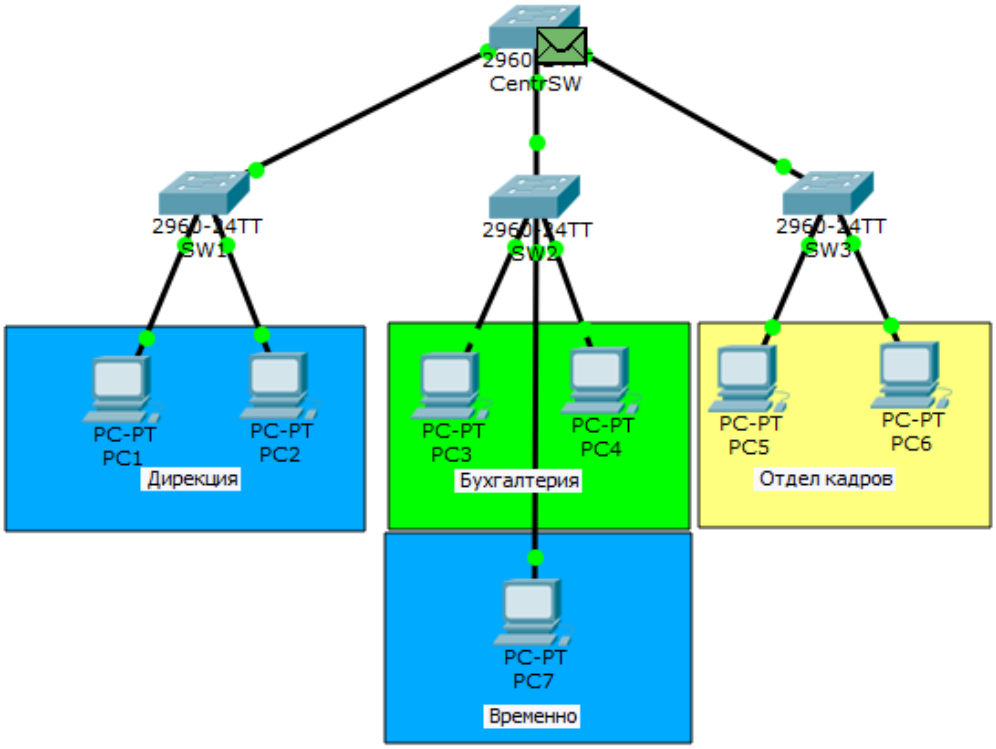
І дійсно. Комутатор відправить кадр у чистому вигляді, тобто без тегів.

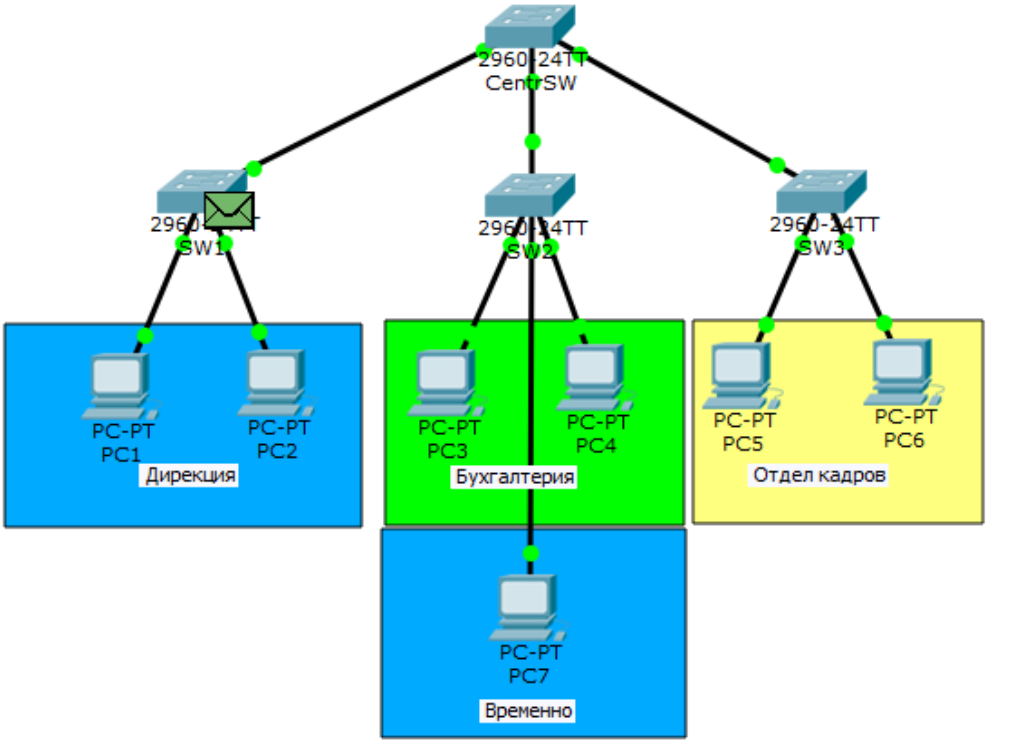
Доходить ARP до PC7. Відкриваємо його і переконуємося, що кадр не тегований PC7 дізнався про себе і надсилає відповідь.

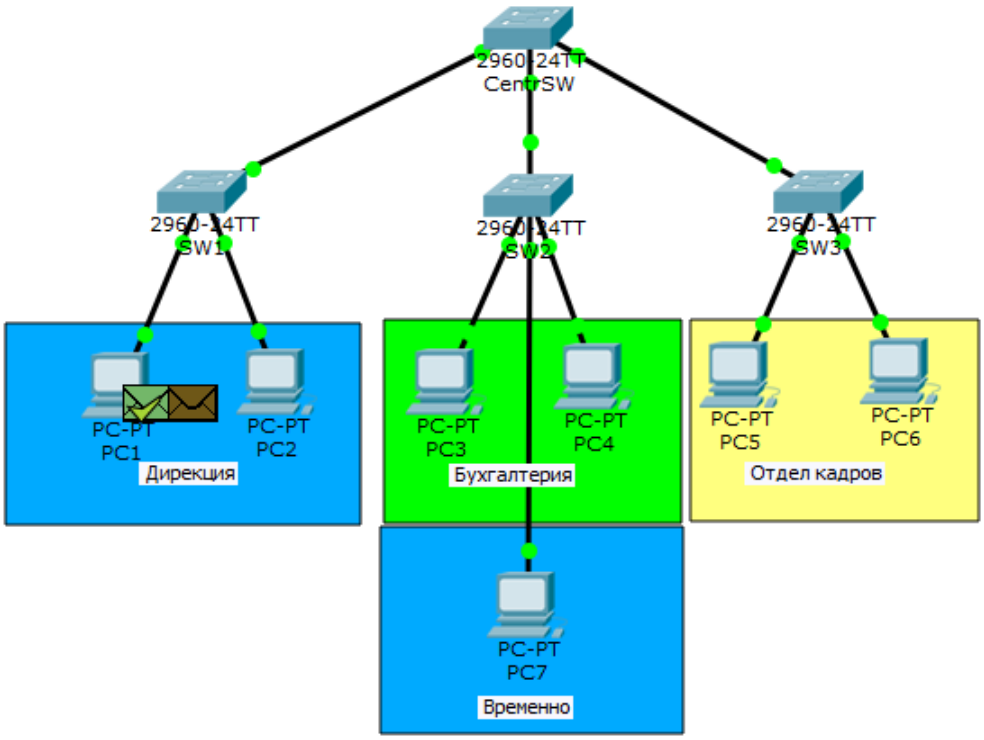




Відкриваємо кадр на комутаторі та бачимо, що на відправлення він піде тегованим. Далі кадр подорожуватиме тим самим шляхом, що й прийшов.

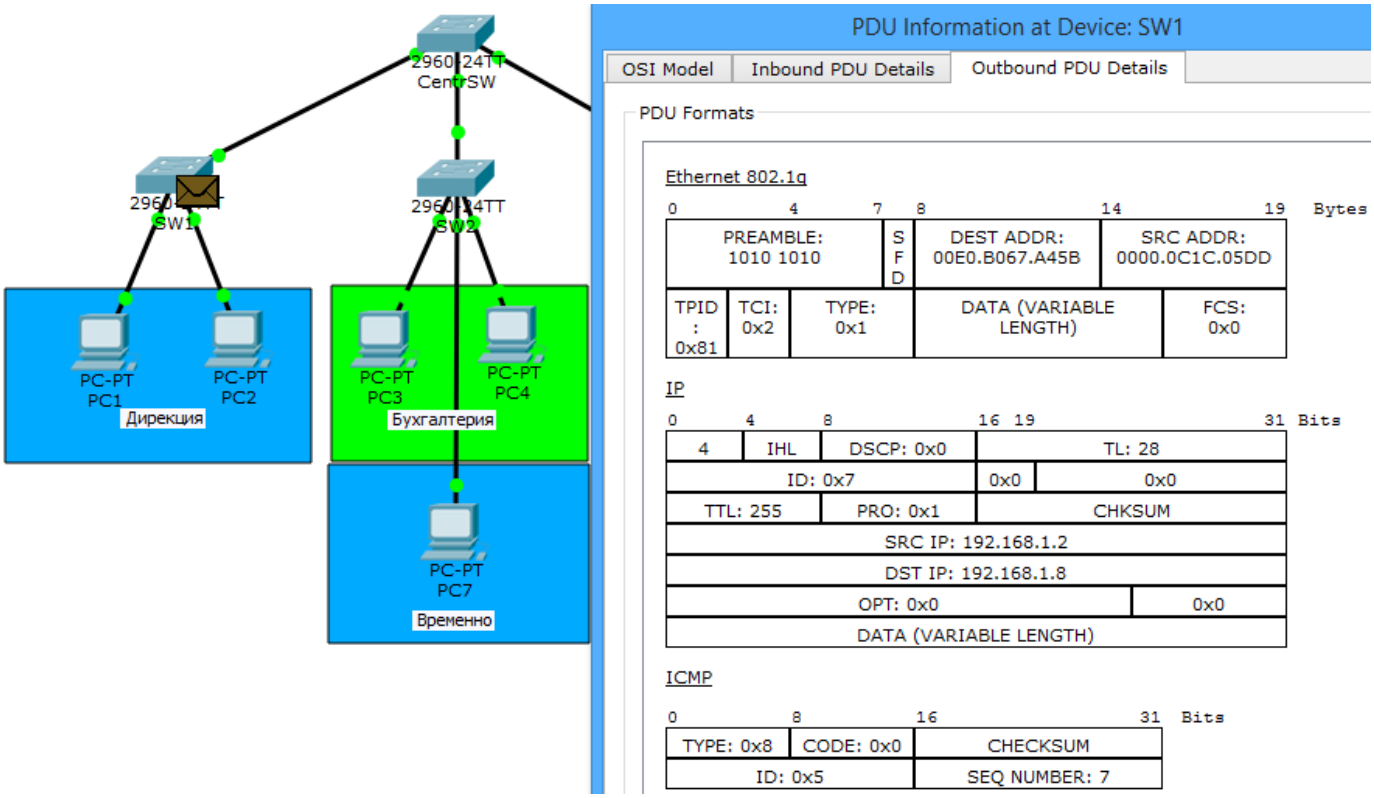




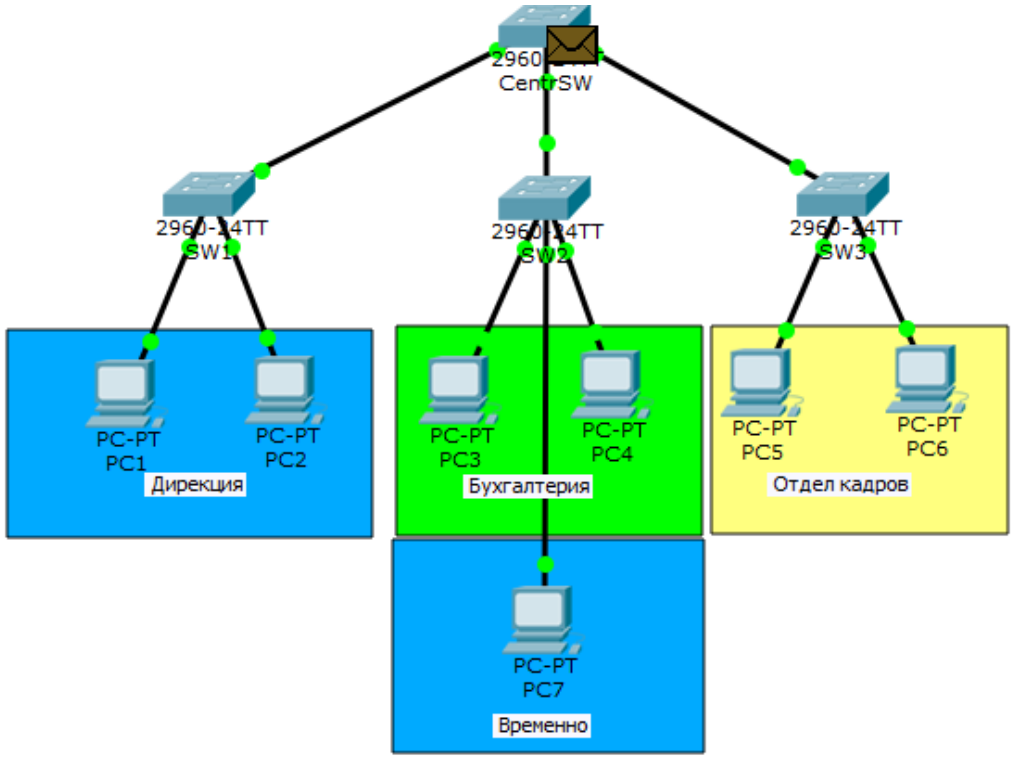


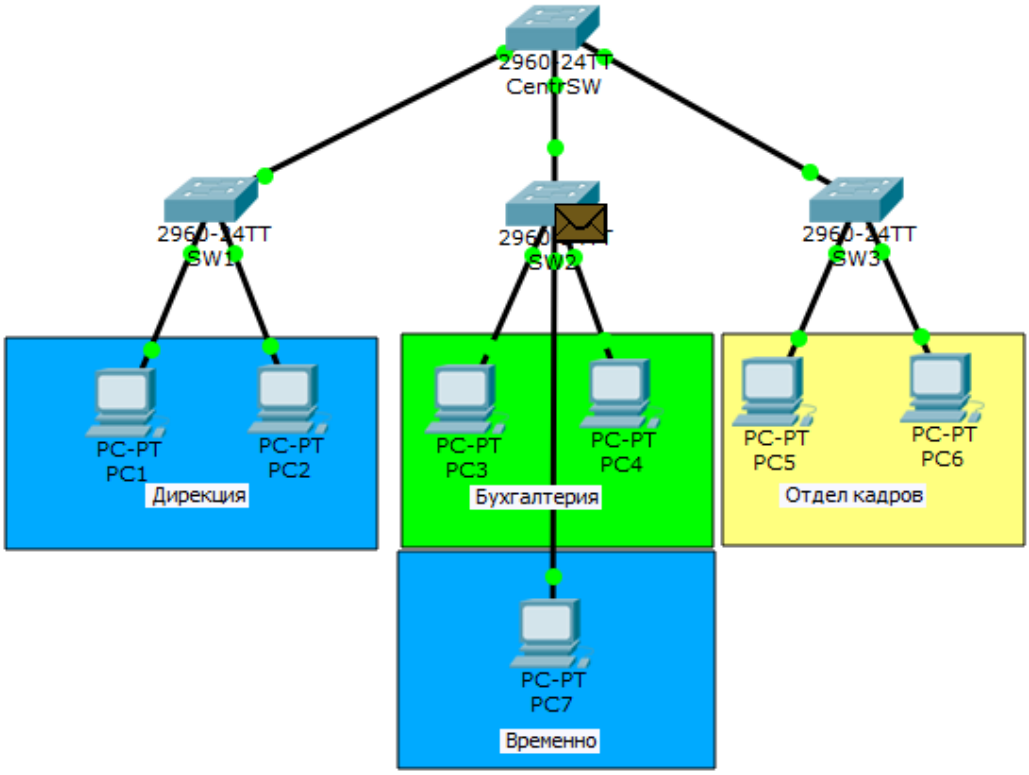
ARP доходить до PC1, що свідчить галочка на конверті. Тепер йому відома MAC-адреса і вона пускає в хід ICMP.

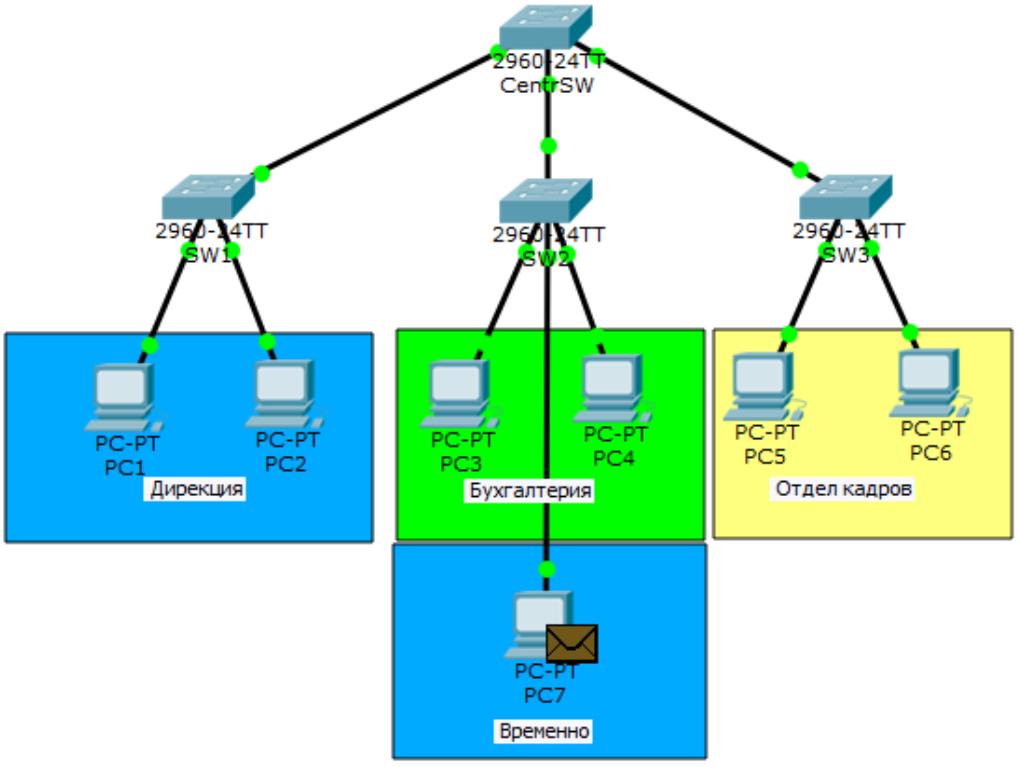
ICMP (англ. Internet Control Message Protocol - протокол міжмережевих керуючих повідомлень - мережевий протокол, що входить у стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки та інші виняткові ситуації, що виникли при передачі даних, наприклад, запитувана послуга недоступна або хост, або маршрутизатор не відповідають. Також ICMP покладаються деякі сервісні функції (services).



Відкриваємо пакет на комутаторі та спостерігаємо таку саму картину. На канальному рівні кадр тегується комутатором. Так буде з кожним повідомленням.







Бачимо, що пакет успішно сягає PC7. Зворотний шлях показувати не будемо, оскільки він аналогічний.

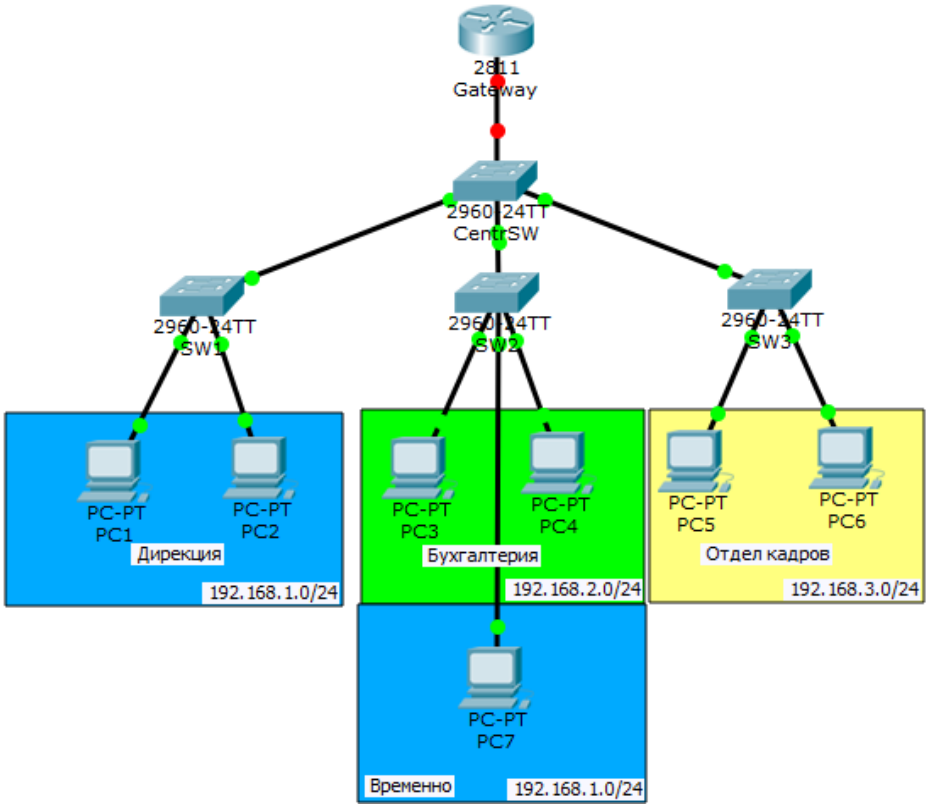
Логіка роботи VLAN
(наприклад на підприємстві)

Ось у принципі найпопулярніше застосування VLAN-ів. Незалежно від фізичного розташування, можна логічно об'єднувати вузли в групи, там ізолюючи їх від інших. Дуже зручно, коли працівники фізично працюють у різних місцях, але мають бути об'єднані. І звичайно з точки зору безпеки VLAN не замінні. Головне, щоб до мережних пристроїв мали доступ обмежене коло осіб.

Домоглися обмеження на канальному рівні. Трафік тепер не гуляє будь-де, а ходить строго за призначенням. Але тепер постає питання, що відділам між собою потрібно спілкуватися. Оскільки вони у різних канальних середовищах, то справа вступає маршрутизація. Але перед початком приведемо топологію в порядок. Найперше до чого прикладемо руку - це адресація вузлів.

Кожен відділ повинен бути у своїй підмережі. Разом отримуємо:

- Дирекція — 192.168.1.0/24
- Бухгалтерія — 192.168.2.0/24
- Відділ кадрів — 192.168.3.0/24



Якщо підмережі визначені, то відразу адресуємо вузли.

1. **PC1:**
   IP: 192.168.1.2
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.1.1
2. **PC2:**
   IP: 192.168.1.3
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.1.1
3. **PC3:**
   IP: 192.168.2.2

Маска: 255.255.255.0 или /24
Шлюз: 192.168.2.1

4. **PC4:**
   IP: 192.168.2.3
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.2.1

5. **PC5:**
   IP: 192.168.3.2
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.3.1
6. **PC6:**
   IP: 192.168.3.3
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.3.1
7. **PC7:**
   IP: 192.168.1.4
   Маска: 255.255.255.0 или /24
   Шлюз: 192.168.1.1

Тепер про зміни у топології. Бачимо, що додався маршрутизатор. Він якраз і перекидатиме трафік з одного VLAN на інший (тобто маршрутизувати). Спочатку з'єднання між ним та комутатором немає, тому що інтерфейси вимкнені.
У вузлів додався такий параметр, як адреса шлюзу. Цю адресу вони використовують, коли потрібно надіслати повідомлення вузлу, що знаходиться в іншій підмережі. Відповідно, у кожної підмережі свій шлюз.

Залишилося налаштувати маршрутизатор і я відкриваю його **CLI**. За традицією дамо осмислене ім'я.

```
Router(config)#hostname Gateway
Gateway(config)#
```

Далі переходимо до настроювання інтерфейсів.

```
Gateway(config)#interface fastEthernet 0/0 - переходимо до необхідного інтерфейсу.
Gateway(config-if)#no shutdown – вмикаємо його.
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Увага! Ми включили інтерфейс, але не повісили на нього IP-адресу. Справа в тому, що від фізичного інтерфейсу (fastethernet 0/0) потрібен лише лінк або канал. Роль шлюзів виконуватимуть віртуальні інтерфейси чи сабінтерфейси (англ. subinterface). На даний момент три типи VLAN. Значить і сабінтерфейсів буде 3. **Приступаємо до налаштування**.

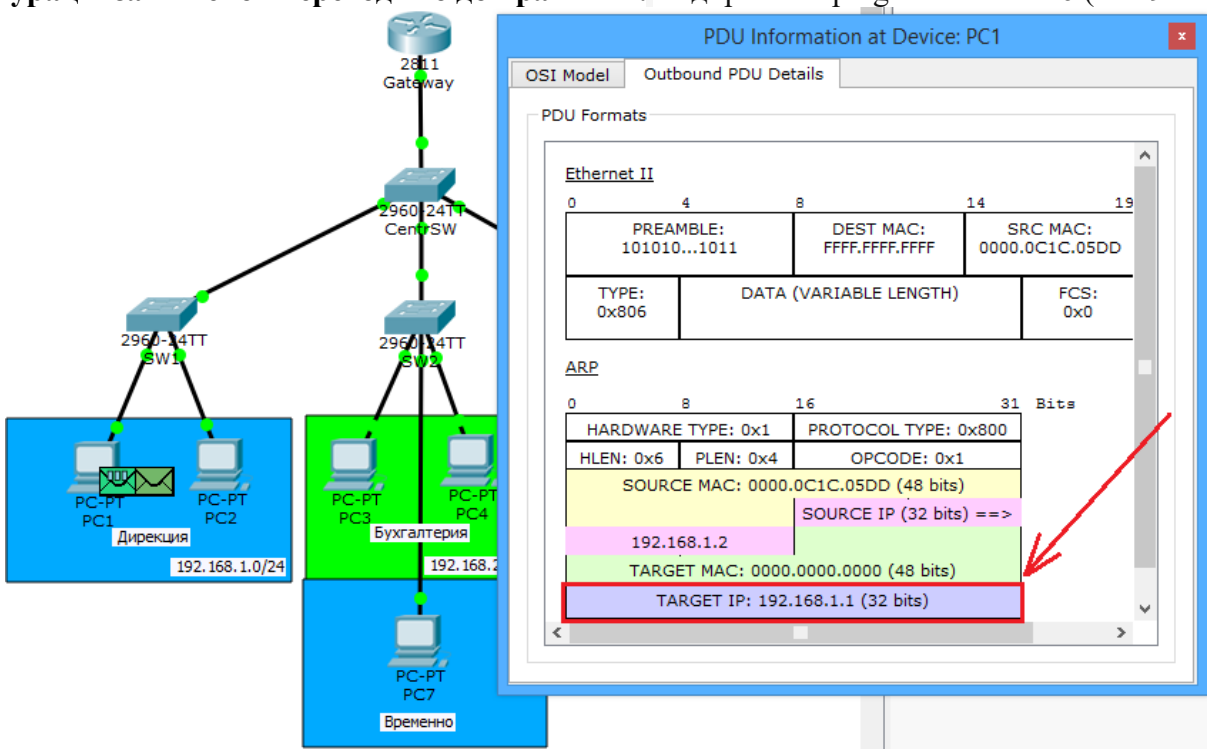
```
Gateway(config)#interface fastEthernet 0/0.2
Gateway(config-if)#encapsulation dot1Q 2
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config)#interface fastEthernet 0/0.3
```

```
Gateway(config-if)#encapsulation dot1Q 3
Gateway(config-if)#ip address 192.168.2.1 255.255.255.0
Gateway(config)#interface fastEthernet 0/0.4
Gateway(config-if)#encapsulation dot1Q 4
Gateway(config-if)#ip address 192.168.3.1 255.255.255.0
```

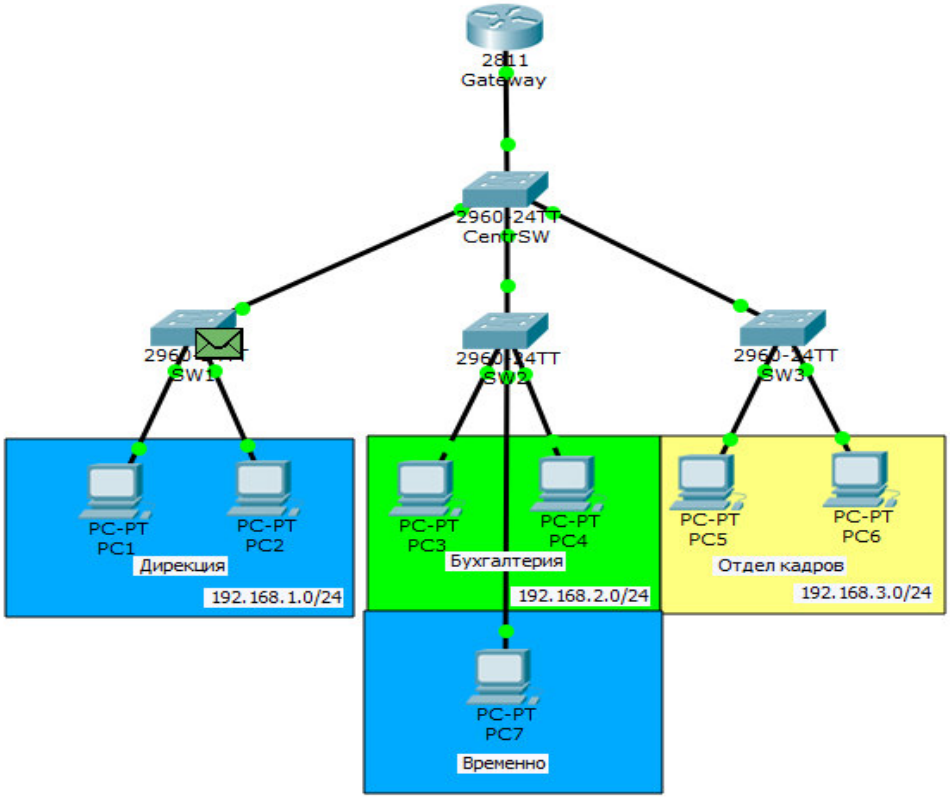
Маршрутизатор налаштовано. Переходимо до **центрального комутатора** і налаштуємо на ньому **транковий порт,** щоб **пропускав теговані кадри на маршрутизатор**.

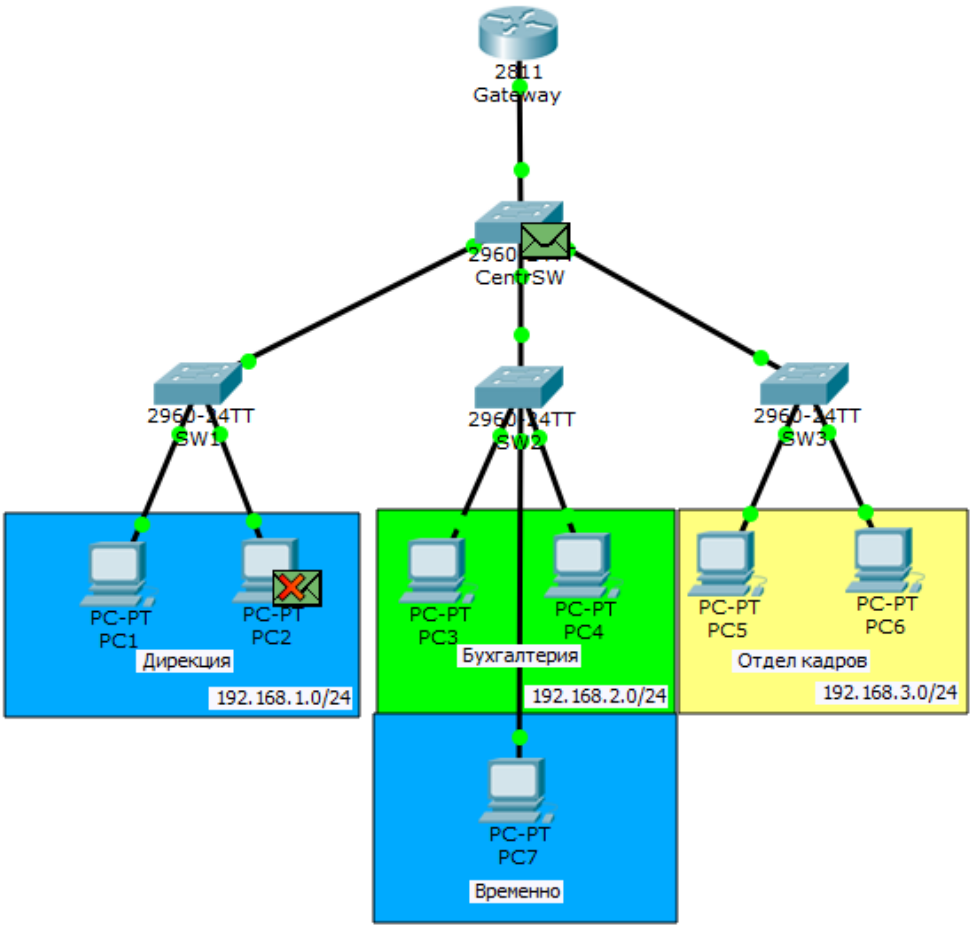
```
CentrSW(config)#interface fastEthernet 0/24
CentrSW(config-if)#switchport mode trunk
CentrSW(config-if)#switchport trunk allowed vlan 2,3,4
```

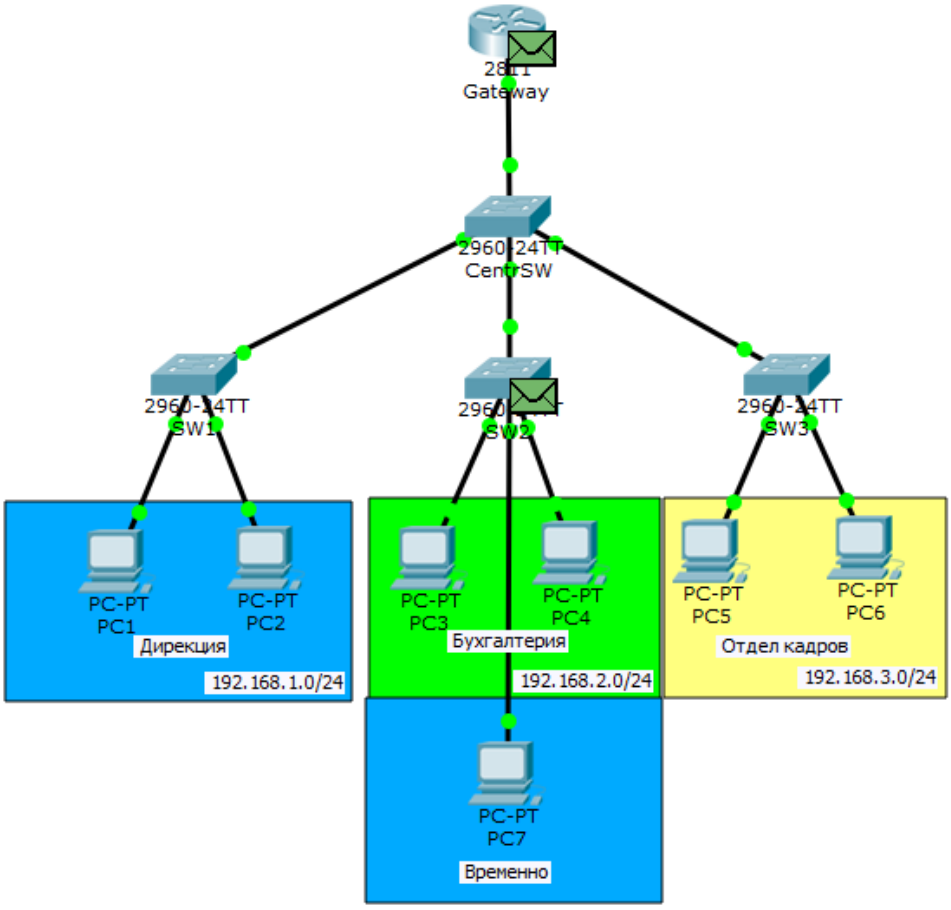
Конфігурація закінчено і переходимо до практики. Відправляю ping з PC1 на PC6 (на 192.168.3.3).



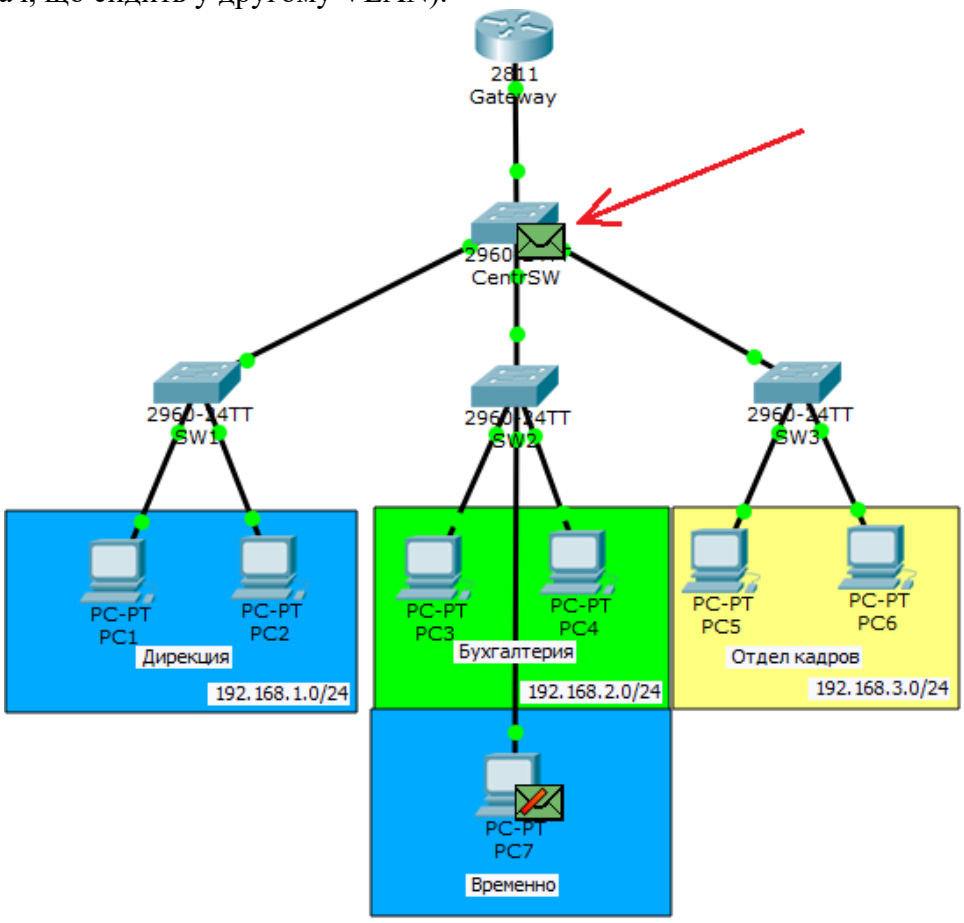
PC1 не має, хто такий PC6 або 192.168.3.3, але знає, що вони знаходяться в різних підмережах. Тому він надішле повідомлення через основний шлюз, адресу якого вказано у його налаштуваннях. І хоч PC1 знає IP-адресу основного шлюзу, не вистачає MAC-адреси. І він пускає у хід ARP.


2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

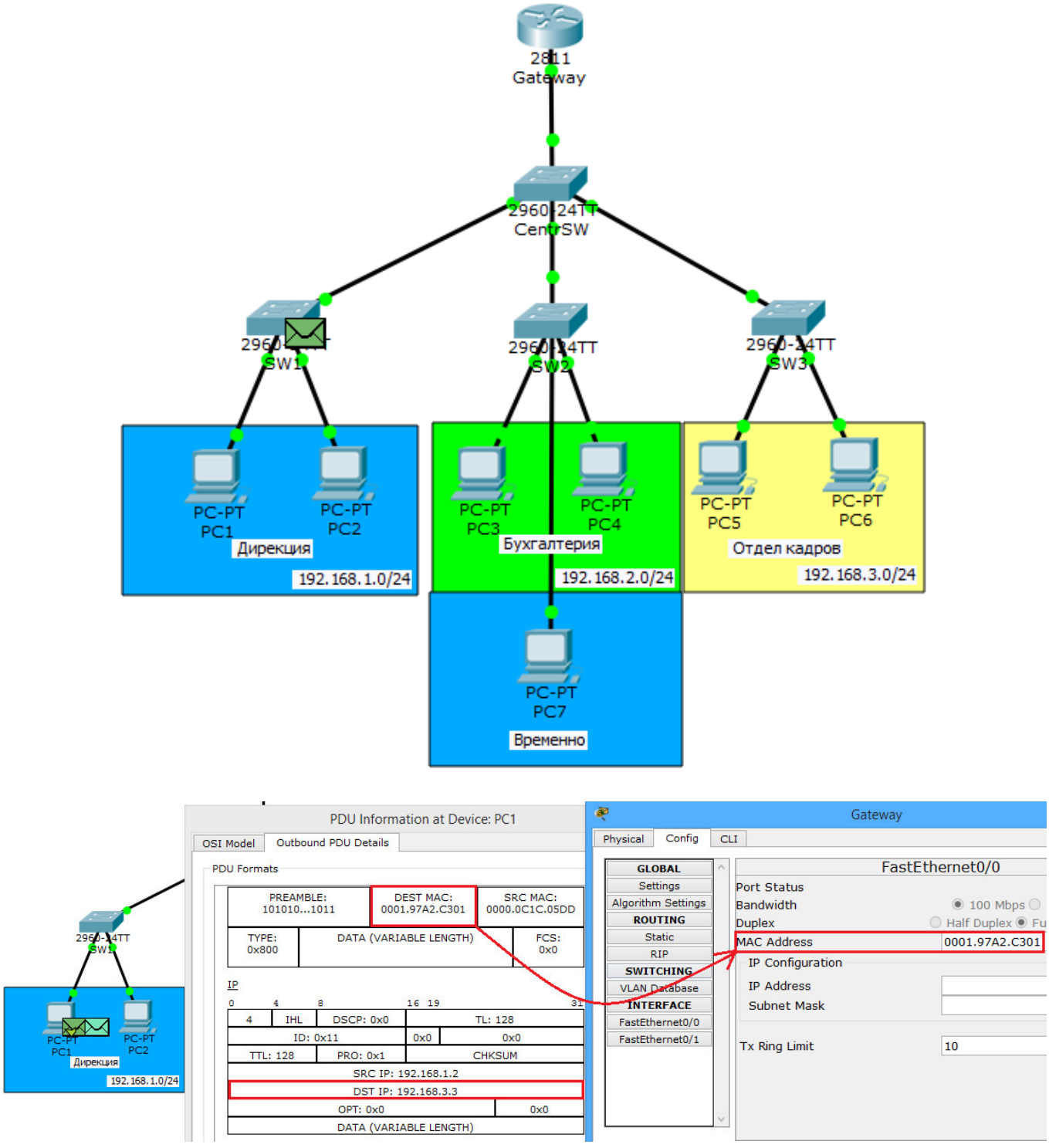

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно



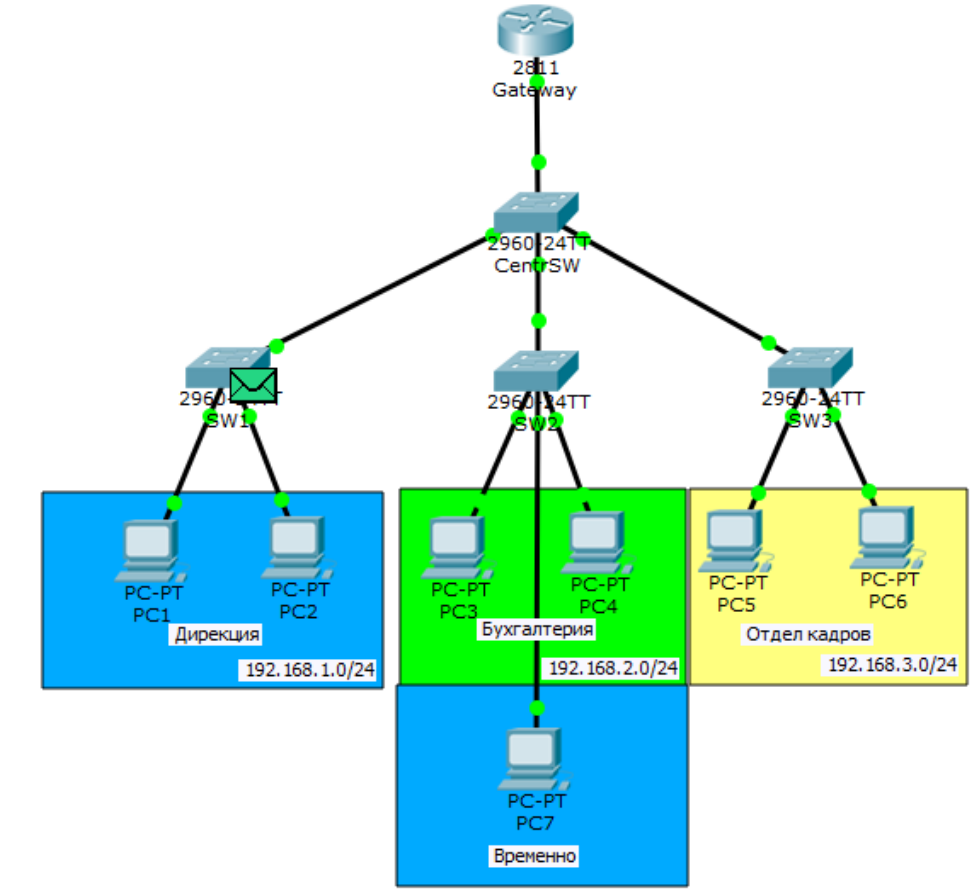
Зверніть увагу. Як тільки кадр прибуває на **CentrSW**, комутатор не розсилає його будь-кому. Він розсилає лише на ті порти, де дозволено пропуск 2-го VLAN. Тобто на маршрутизатор і на SW2 (там є користувач, що сидить у другому VLAN).

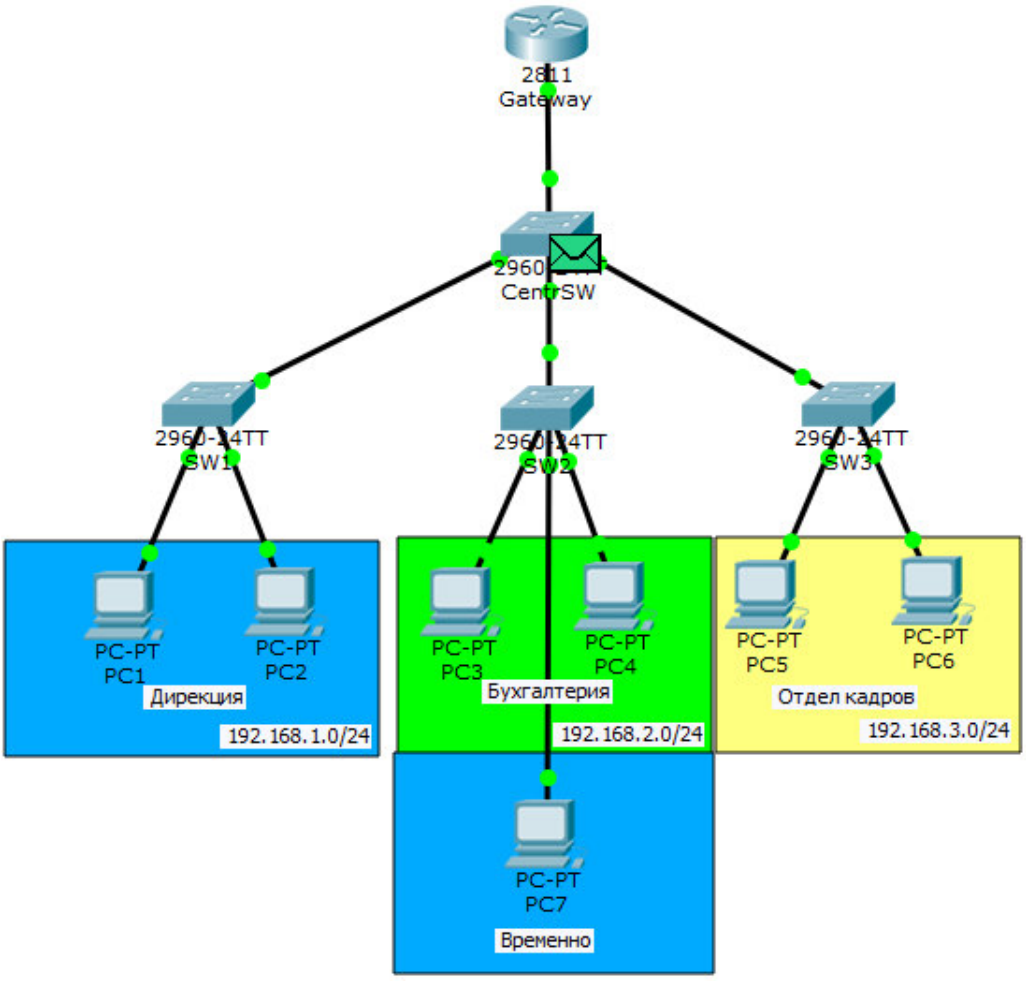


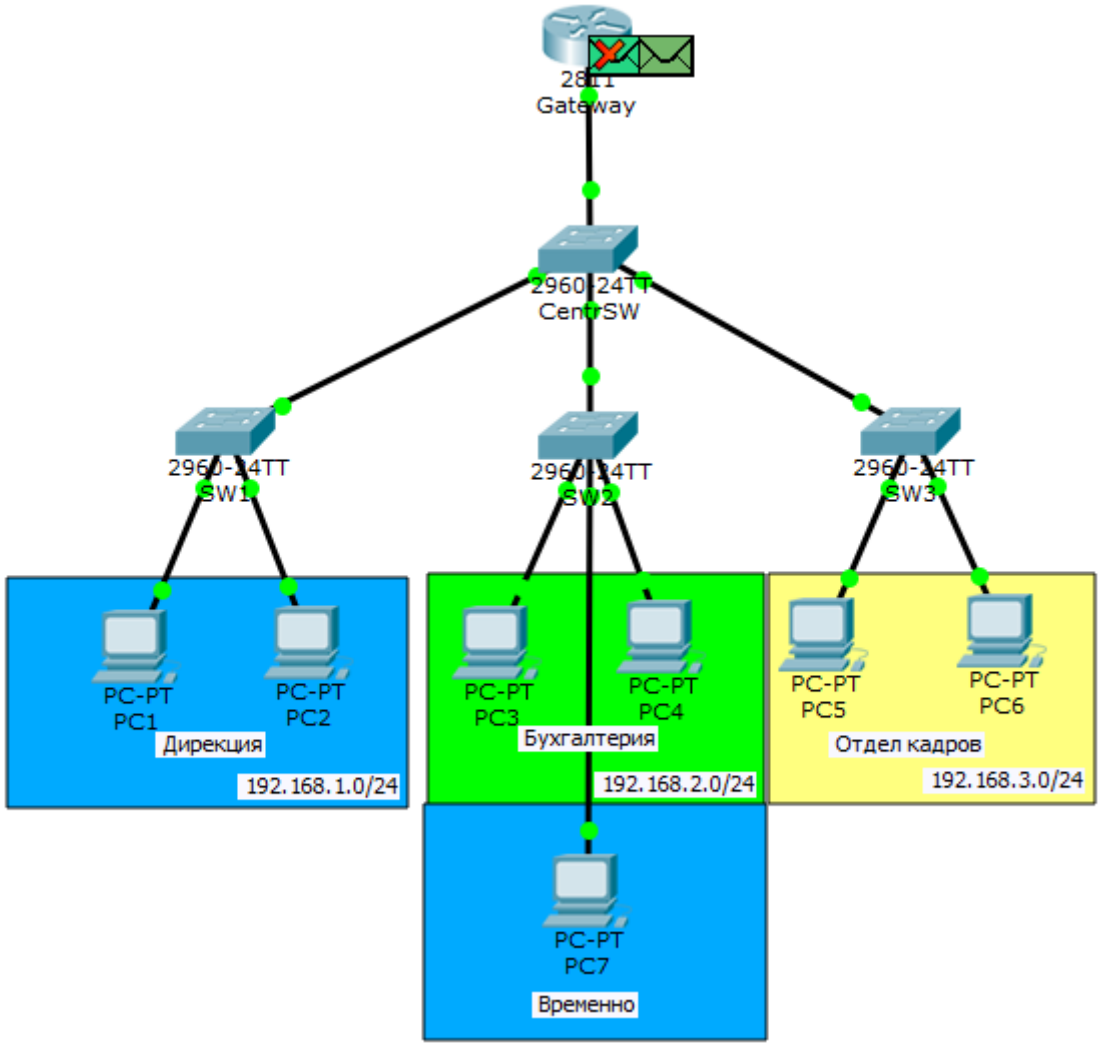
Маршрутизатор впізнає себе і відправляє відповідь (показаний стрілочкою). І зверніть увагу на нижній кадр. Коли **SW2** отримав ARP від центрального комутатора, він аналогічно не став розсилати його на всі комп'ютери, а **відправив лише PC7**, який сидить у **другому VLAN**. Але PC7 його відкидає, оскільки він не для нього. Дивимося далі.



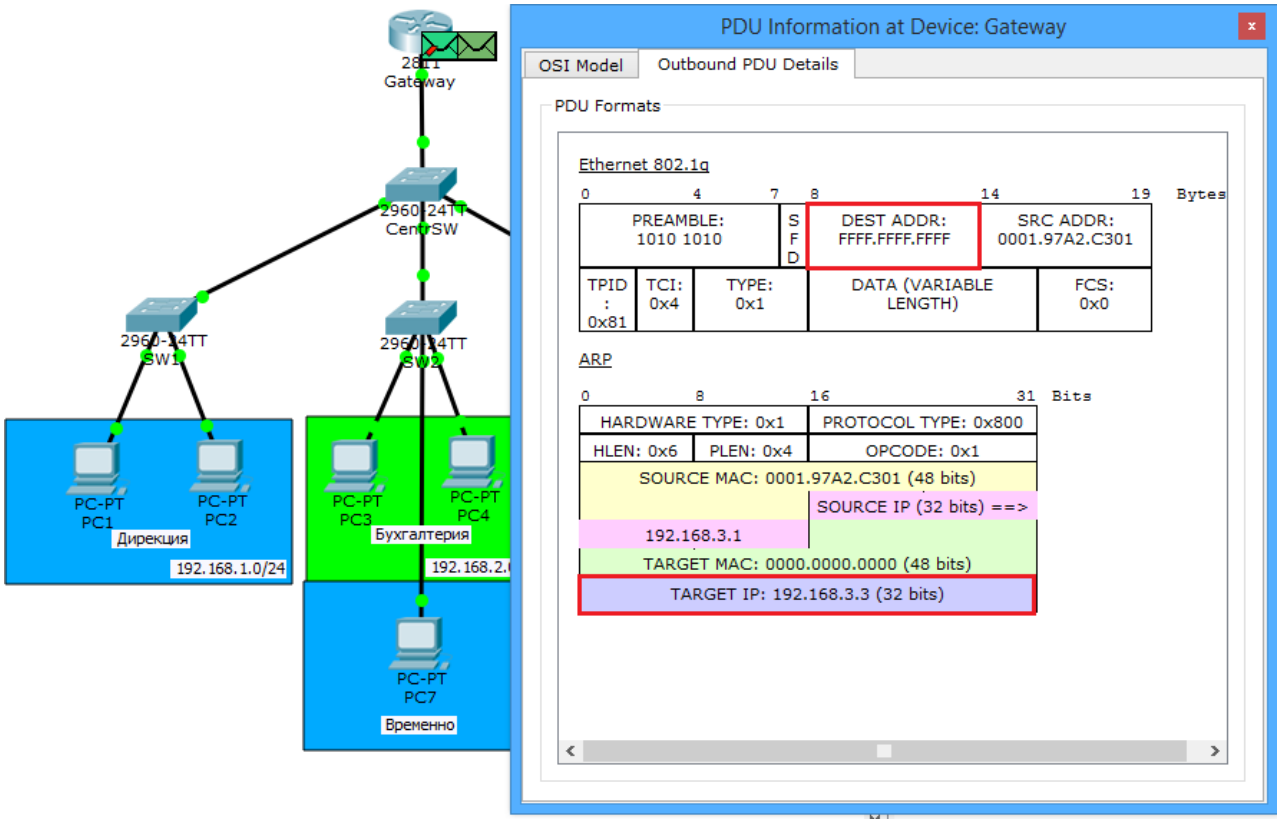
ARP дійшов PC1. Тепер йому все відомо і можна надсилати ICMP. Ще раз зверну увагу на те, що як MAC-адреса призначення (канальний рівень), буде адреса маршрутизатора, а як IP-адреса призначення (мережевий рівень), адреса PC6.

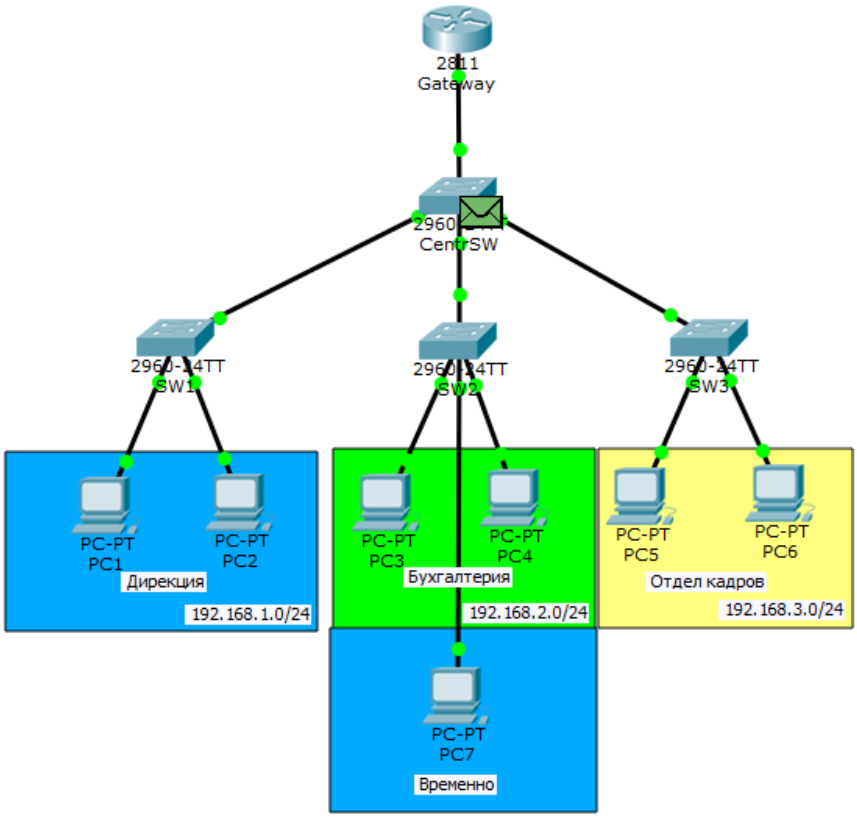

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

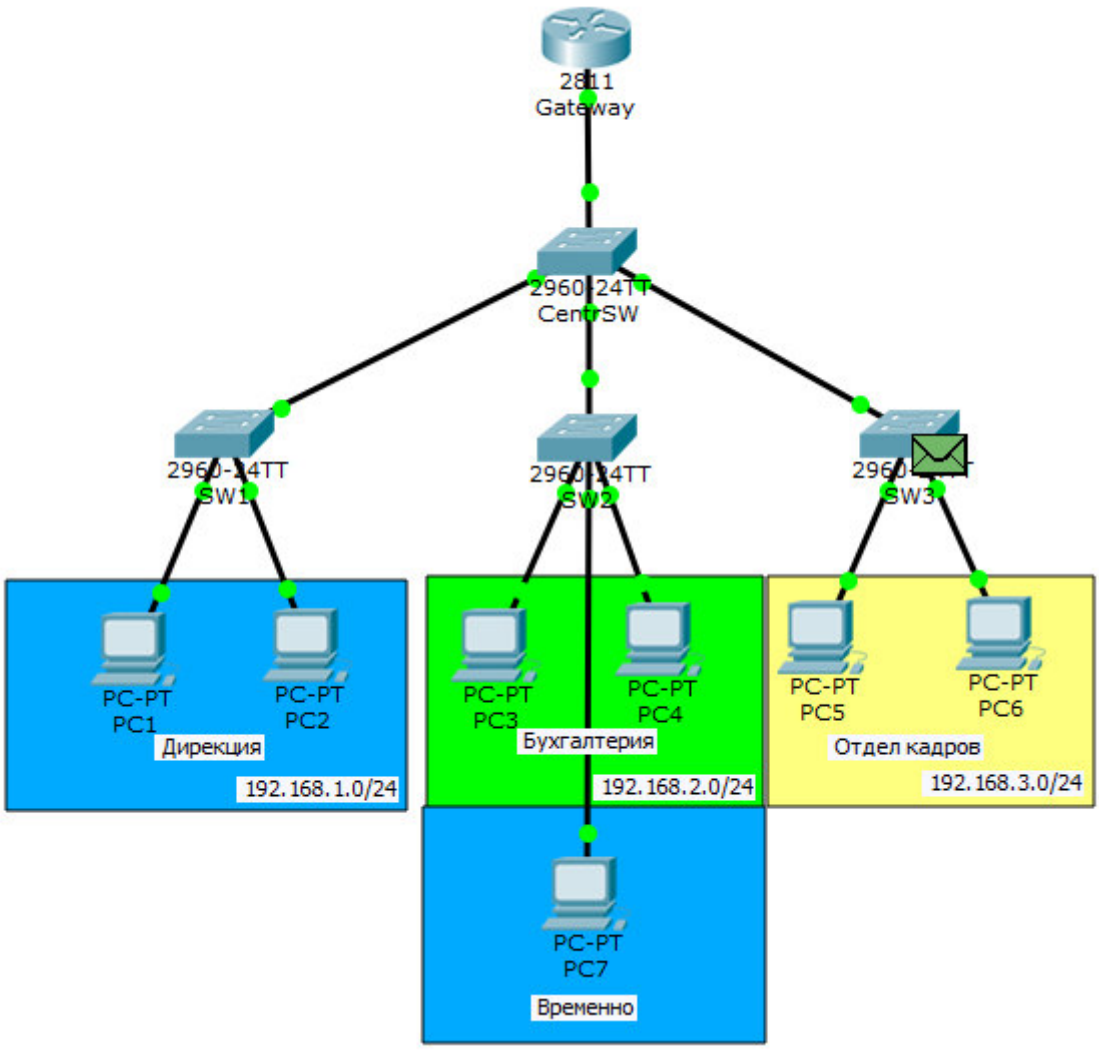

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

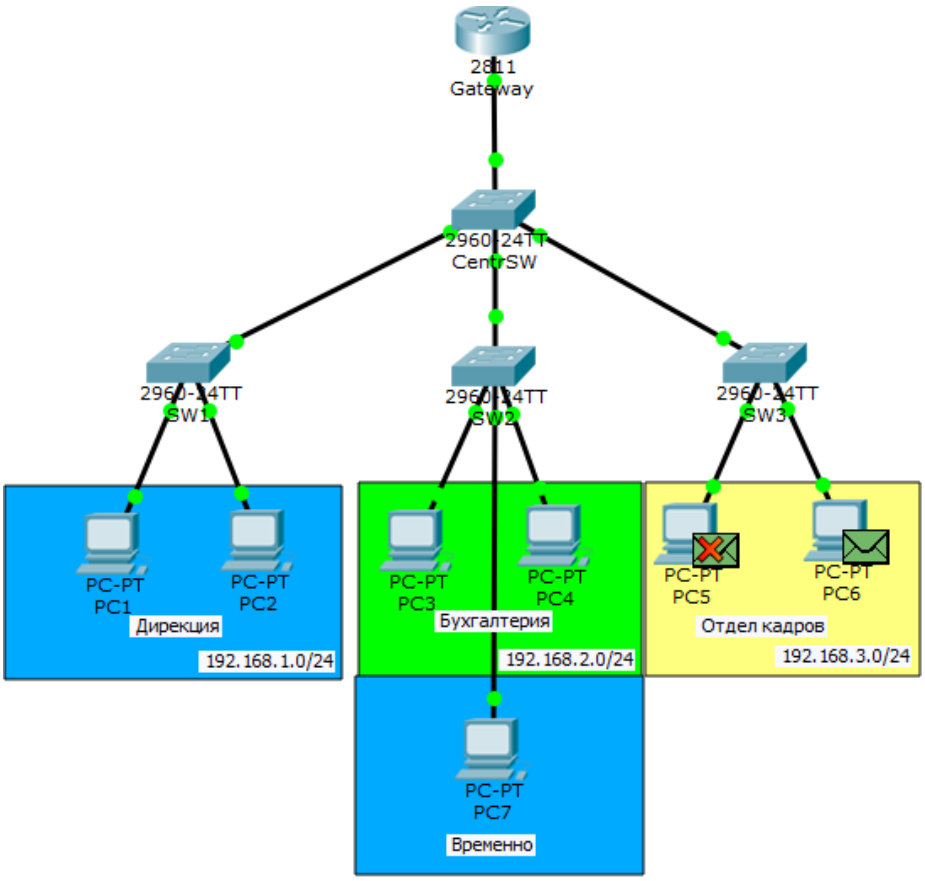


Доходить ICMP до маршрутизатора. Він дивиться у свою таблицю і розуміє, що нікого не знає за адресою 192.168.3.3. Відкидає ICMP, що прибув, і пускає розвідати ARP.

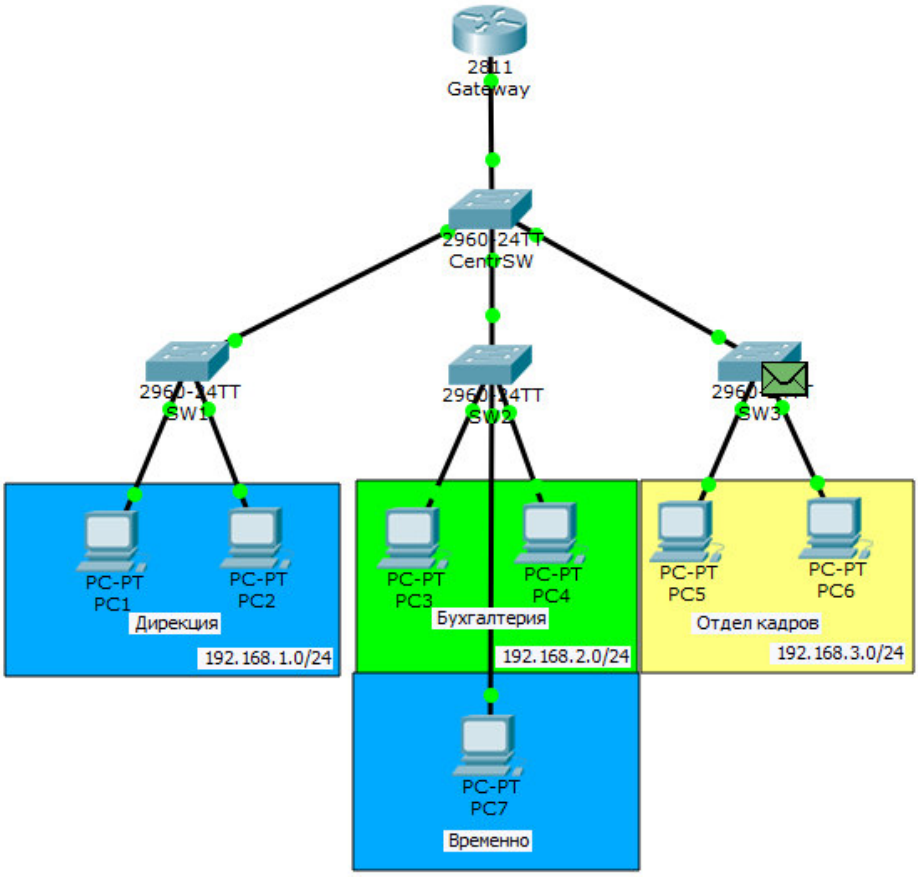


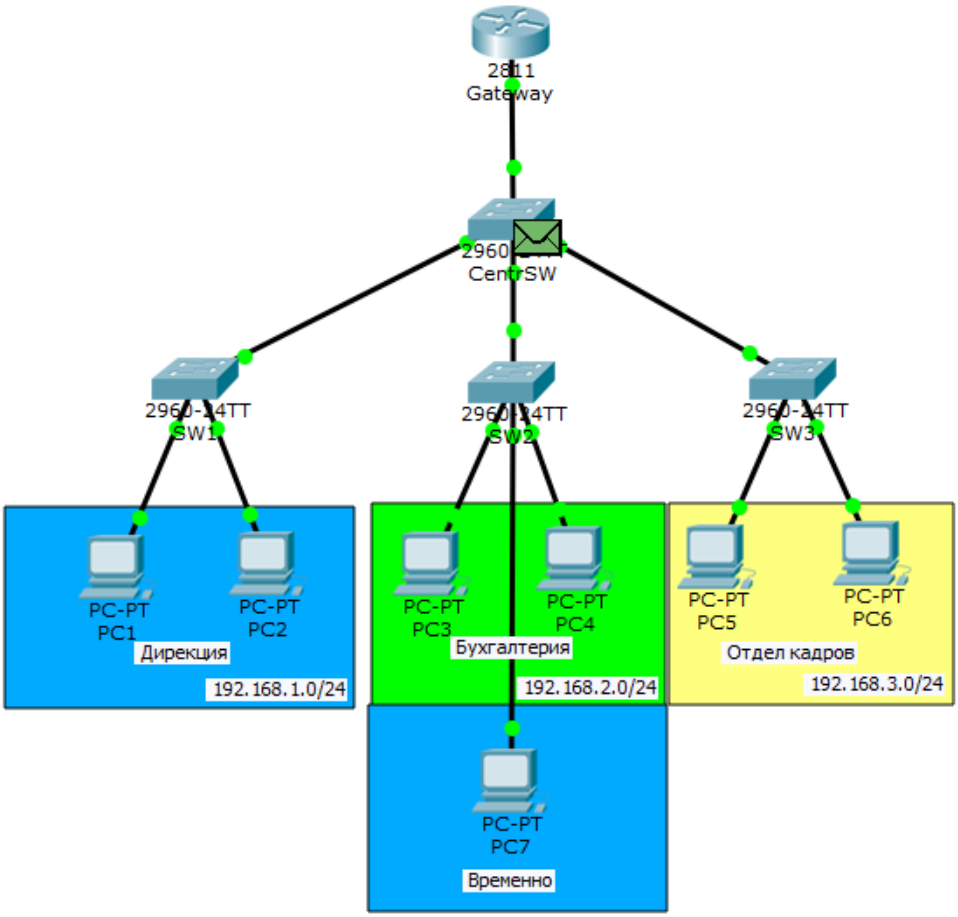

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

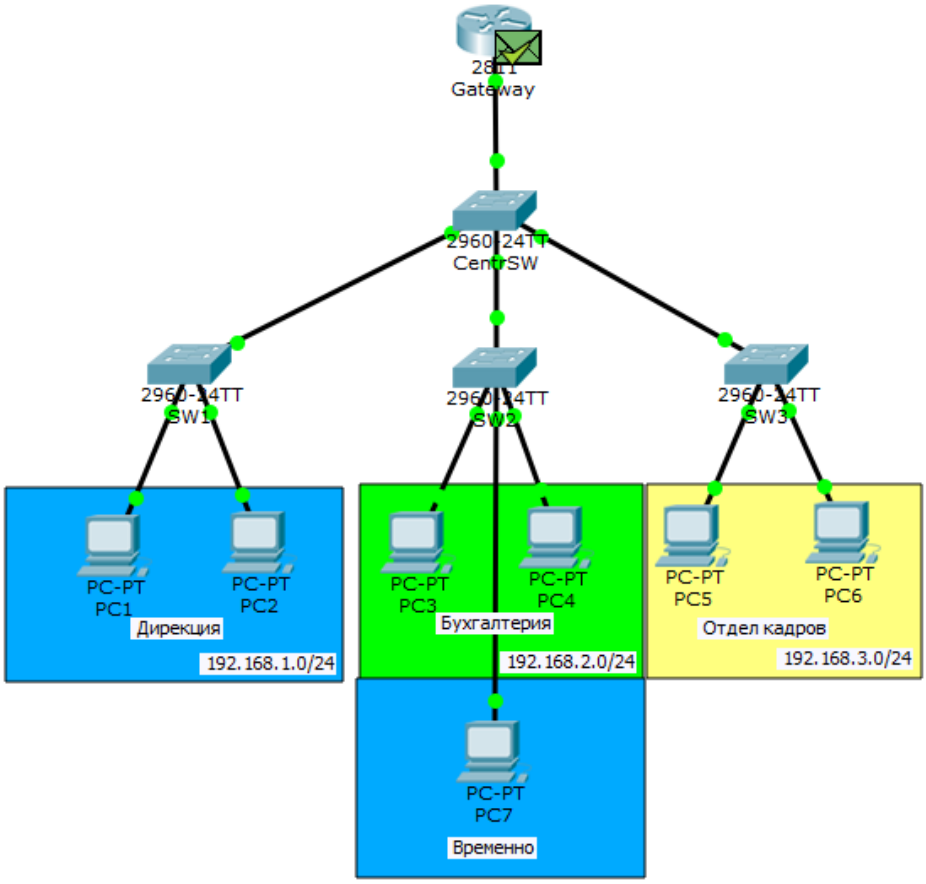

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно



PC6 впізнає себя і відправляє відповідь.



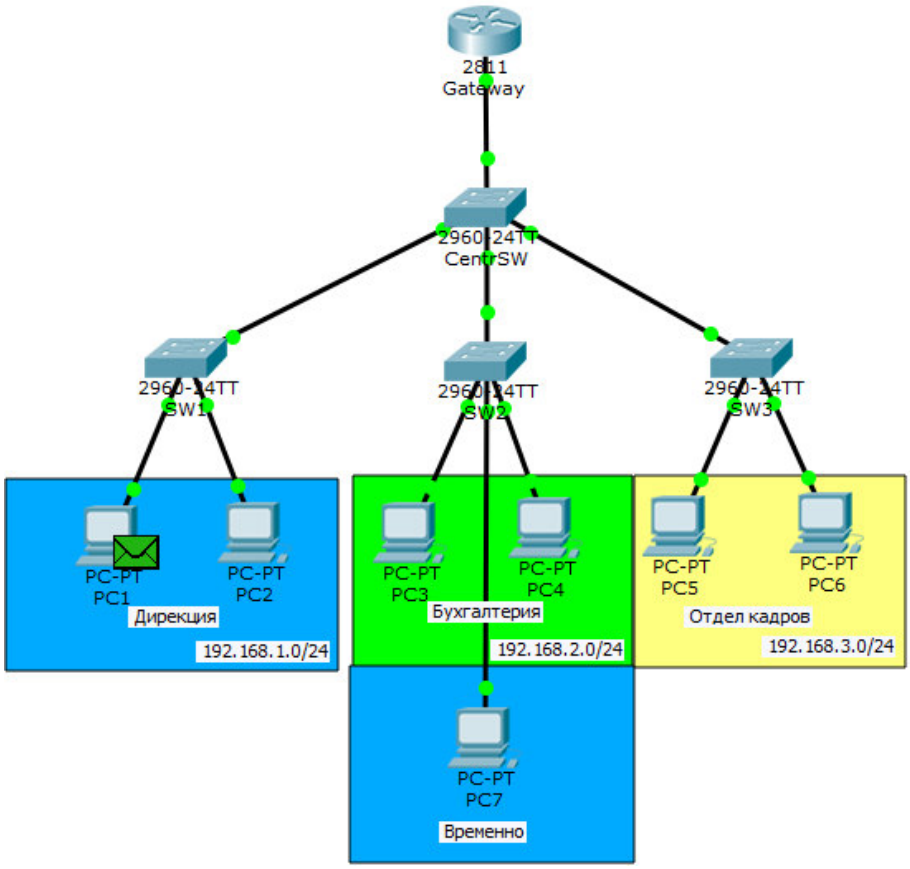


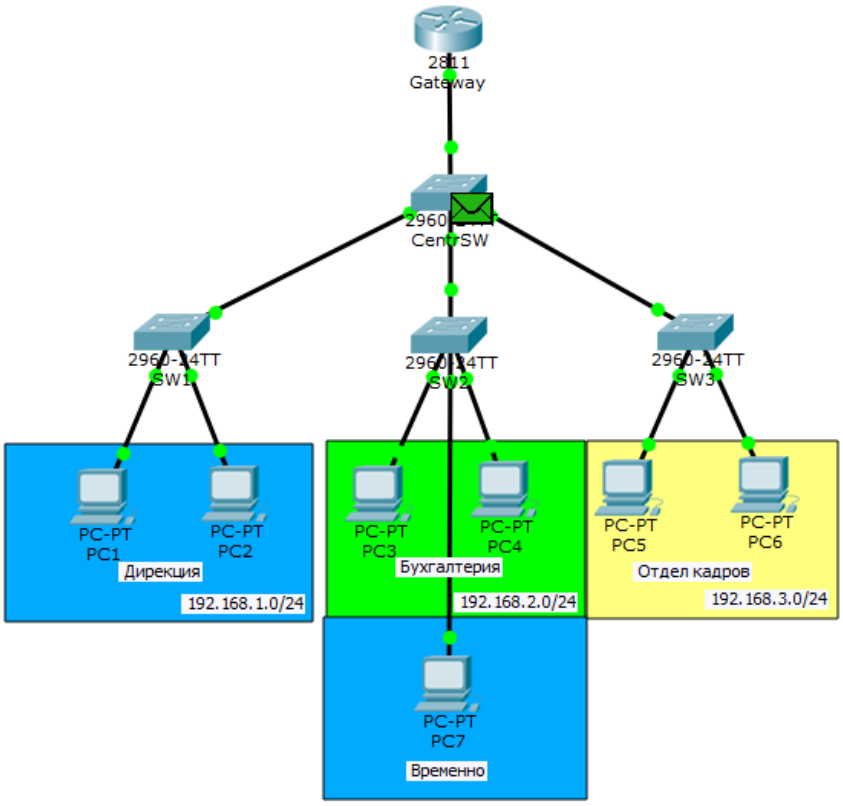


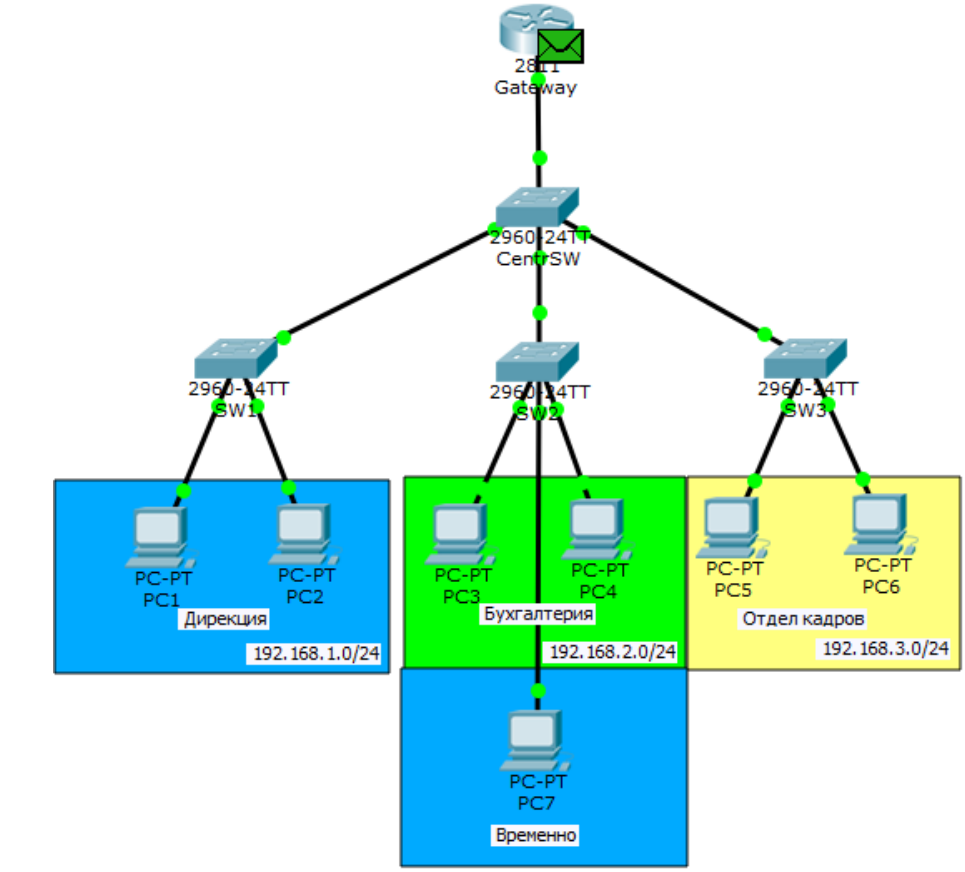
Доходить до маршрутизатора відповідь і він додає запис у таблиці. Переглянути таблицю ARP можна командою **show arp**.

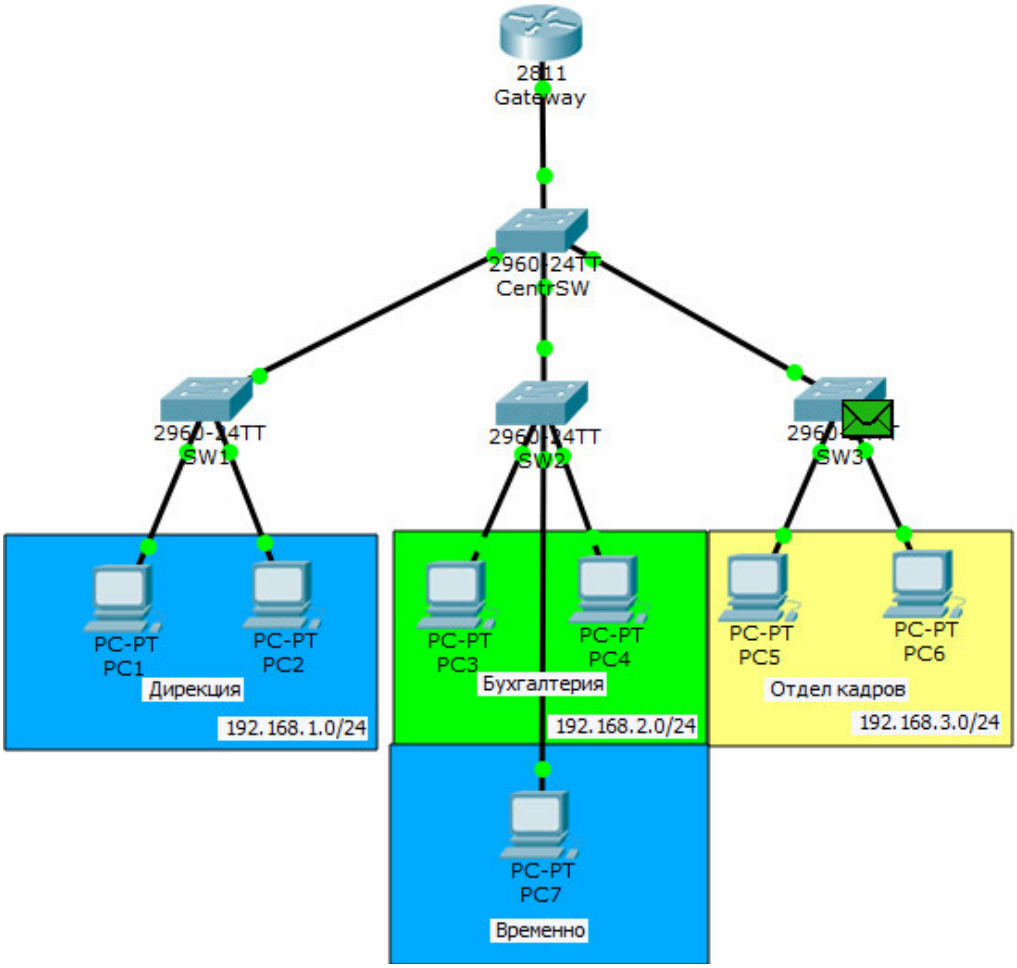
```
Gateway#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.2              0  0000.0C1C.05DD  ARPA   FastEthernet0/0.2
Internet  192.168.3.3              0  0002.17A5.D5B4  ARPA   FastEthernet0/0.4
```

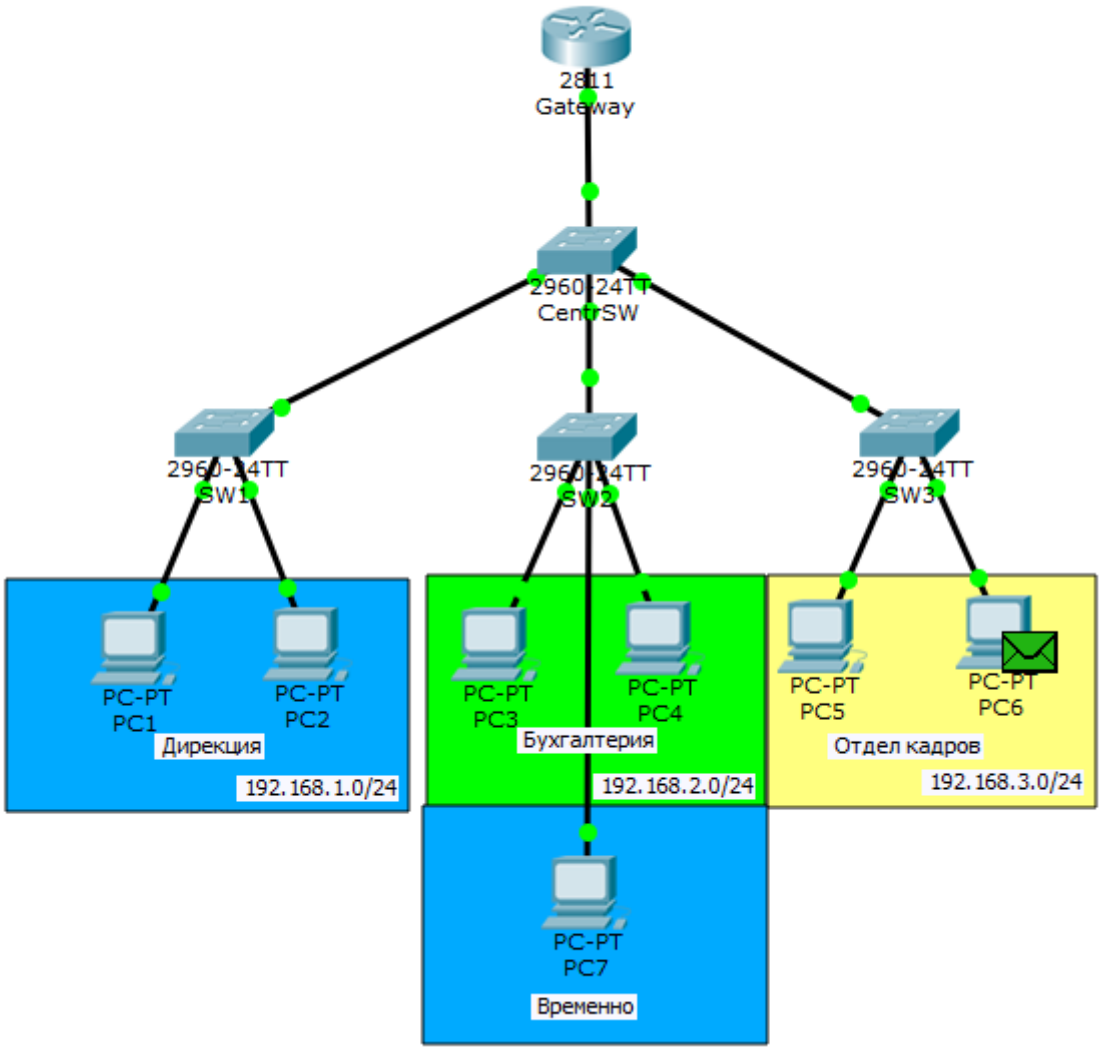
Рухаємось далі. PC1 незадоволений, що ніхто не відповідає і надсилає наступне ICMP-повідомлення.



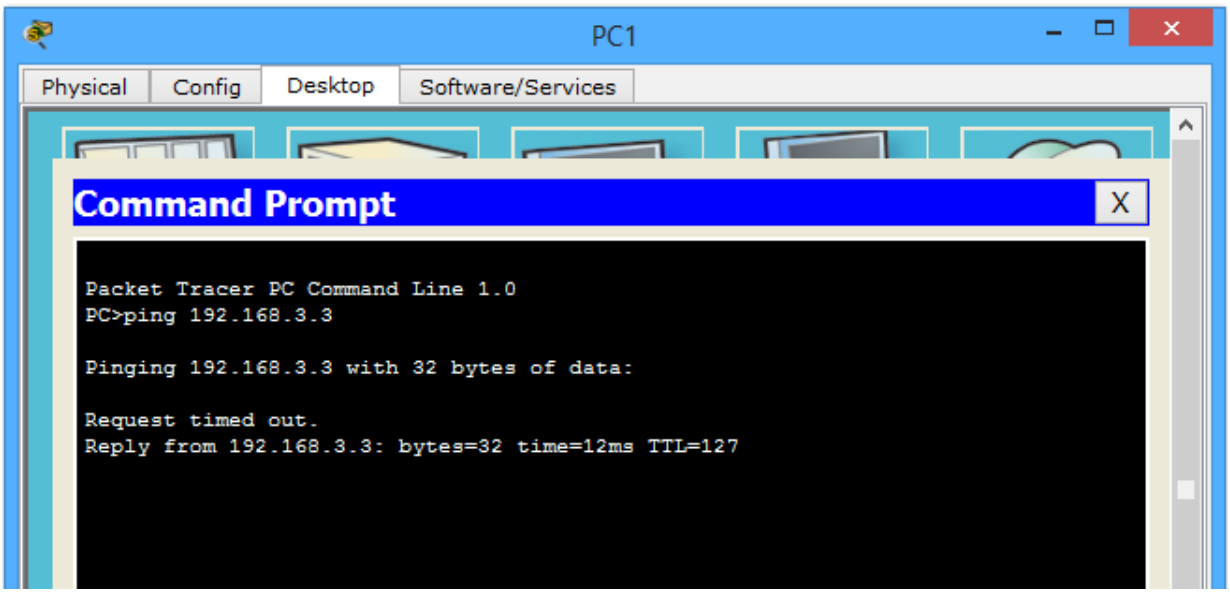



2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

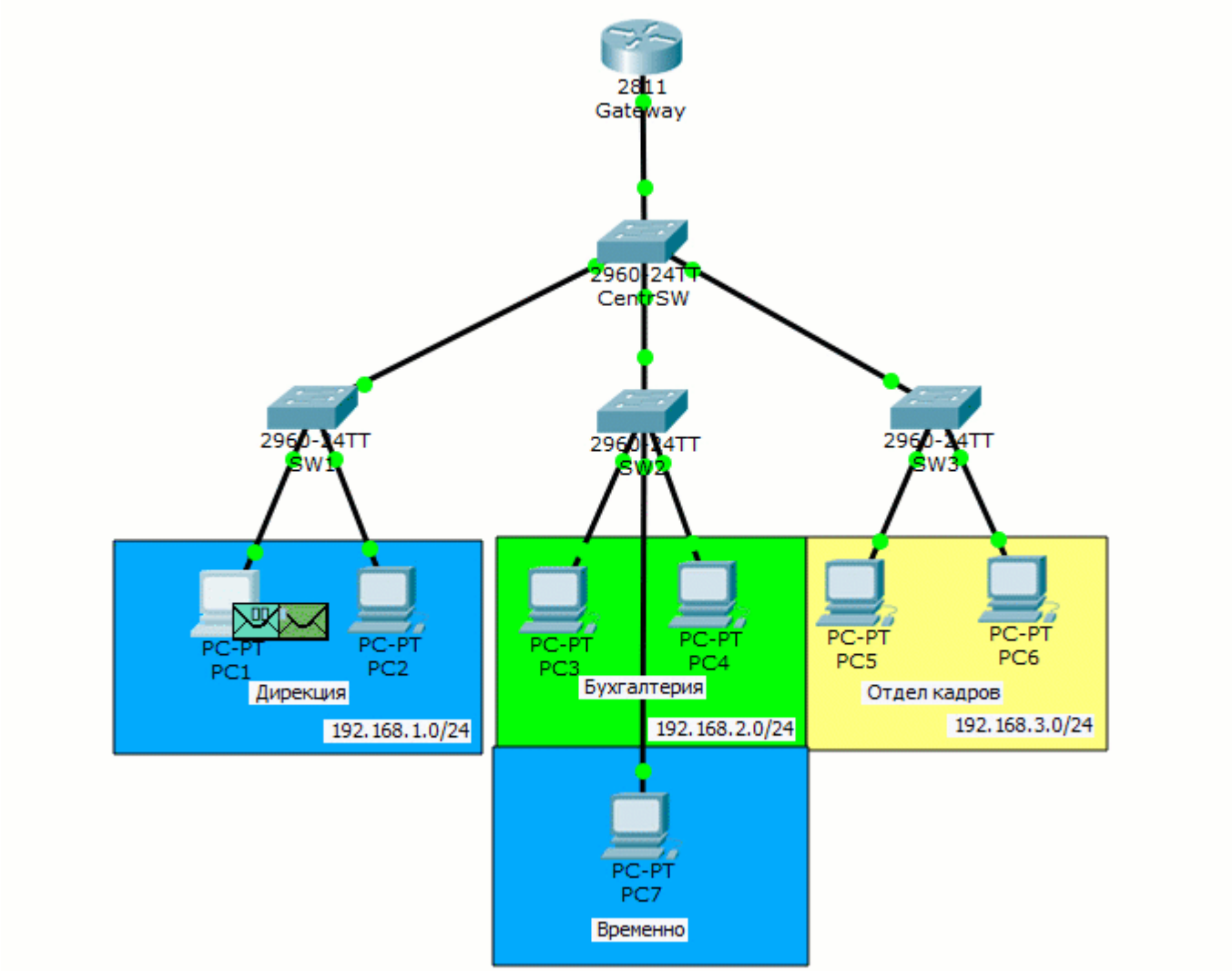

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно



На цей раз ICMP доходить без проблем. Назад він пройде тим самим маршрутом. Покажемо кінцевий результат.



Перший пакет загубився (в результаті роботи ARP), а другий дійшов без проблем.



Отже. Ми домоглися того, що якщо вузли знаходяться в одній підмережі та в одному VLAN, то вони будуть ходити безпосередньо через комутатори. У випадку, коли потрібно передати повідомлення в іншу підмережу та VLAN, то передаватимуться через роутер **Gateway**, який здійснює «**міжланову**» **маршрутизацію.** Ця топологія отримала назву **"router on a stick**" або "**роутер на паличці"**. Як ви зрозуміли, вона дуже зручна.

Ми створили **3 віртуальні інтерфейси** і по одному дроту ганяли різні теговані кадри. Без використання сабінтерфейсів та VLAN-ів, довелося б для кожної підмережі задіяти окремий фізичний інтерфейс, що зовсім не вигідно.

Розібралися з VLAN і переходимо до одного з протоколів, що працює з ним.

DTP (англ. Dynamic Trunking Protocol)

Динамічний транковий протокол – пропрієтарний протокол компанії **Cisco**, який служить для реалізації trunk режиму між комутаторами. Хоча залежно від стану, вони можуть узгоджуватися і в режимі access.

В DTP есть 4 режима: Dynamic auto, Dynamic desirable, Trunk, Access.

Розглянемо як вони узгоджуються.

Режими	**Dynamic auto**	**Dynamic desirable**	**Trunk**	**Access**
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Відсутність з'єднання
Access	Access	Access	Відсутність з'єднання	Access

Тобто колонка ліворуч – це перший пристрій, а верхній рядок другий пристрій. За замовчуванням комутатори перебувають у режимі "dynamic auto". Якщо подивитися таблицю зіставлення, то два комутатора в режимі "dynamic auto" узгоджуються в режим "access". Давайте це й перевіримо. Створимо нову лабораторну роботу і додамо 2 комутатора.

З'єднувати їх поки що не будемо. Потрібно переконатися, що обидва комутатори в режимі "dynamic auto". Перевіряти будемо командою **show interfaces switchport**.

```
SW1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

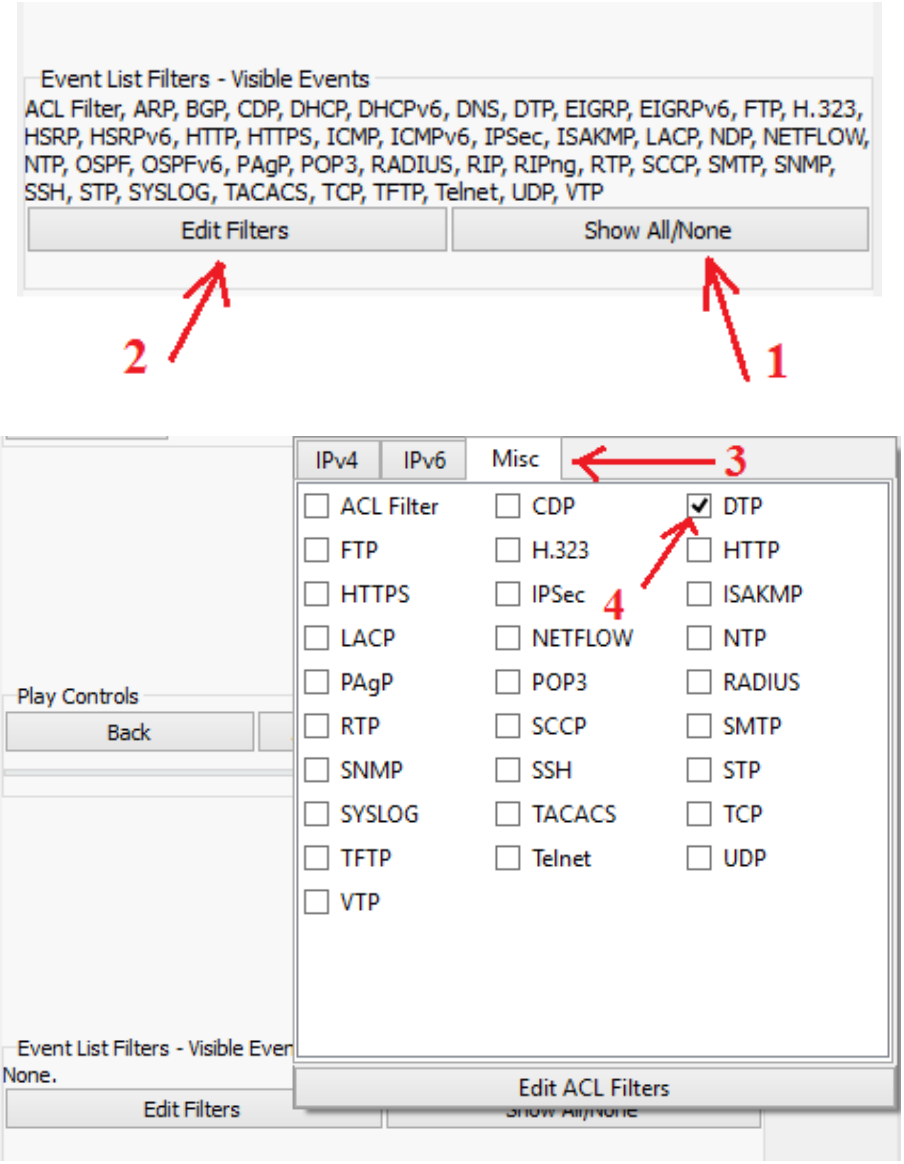
```
SW2#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Результат цієї команди дуже великий, тому я його обрізав і виділив пункти, що цікавлять. Почнемо з **Administrative Mode**. Цей рядок показує, у якому з 4-режимів працює цей порт на комутаторі. Переконуємось, що на обох комутаторах порти в режимі "Dynamic auto".

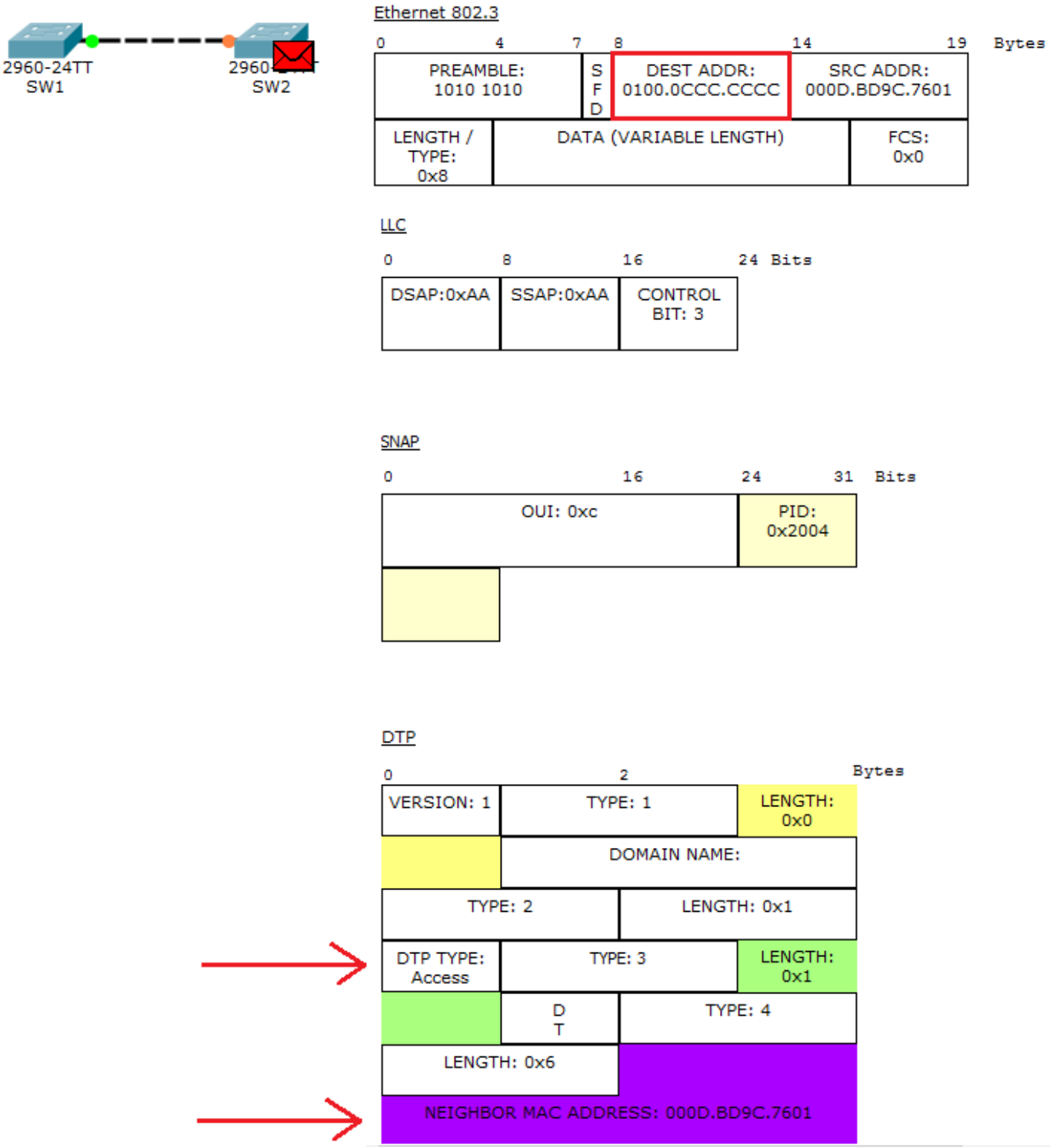
А рядок **Operational Mode** вказує, в якому режимі роботи вони узгодили роботу. Ми поки що їх не з'єднували, тому вони в стані «down».

При тестуванні будь-якого протоколу користуйтеся фільтрами. Вимкніть показ роботи всіх непотрібних вам протоколів.

Переводимо CPT в режим simulation і відфільтровуємо всі протоколи, крім DTP.



Думаю, тут все зрозуміло. З'єдную комутатор кабелем і, при піднятті лінків, один з комутаторів генерує DTP-повідомлення.

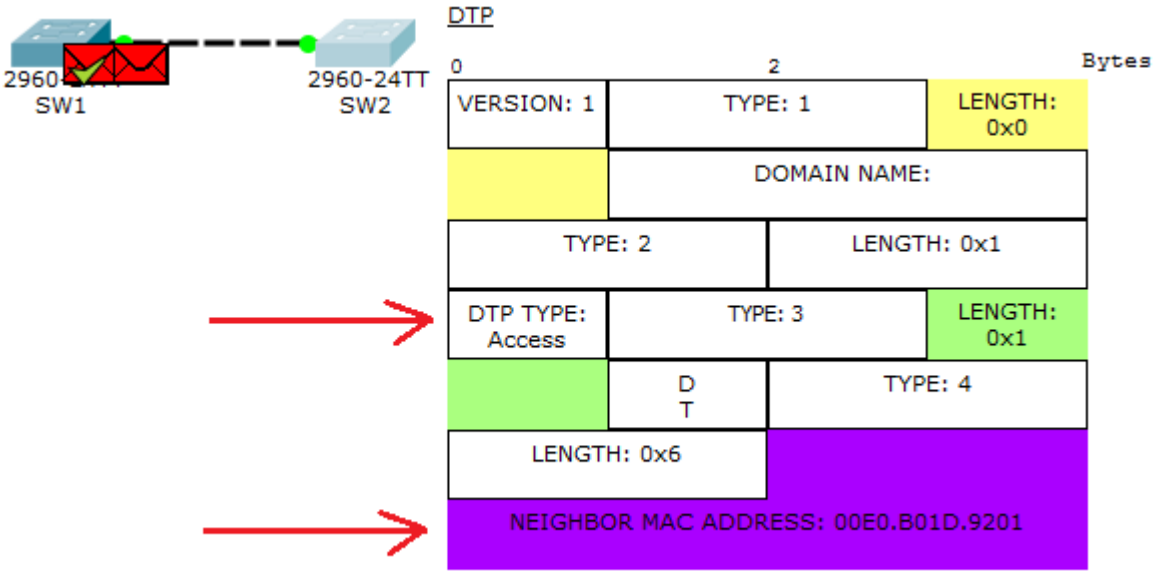


Відкриваю та бачу, що це DTP інкапсульований у Ethernet-кадр. Відправляє він його на мультикастовий адресу "**0100.0ccc.cccc**", який відноситься до протоколів DTP, VTP, CDP. І зверну увагу на 2 поля у заголовку DTP.

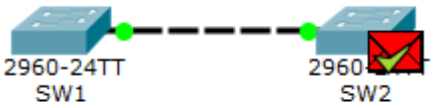
1) **DTP Type** – сюди відправляючий вставляє пропозицію. Тобто, у який режим він хоче погодитися. У нашому випадку він пропонує узгодити "access".

2) **Neighbor MAC-address** – в це поле він записує MAC-адресу свого порта.

Він відправляє і чекає на реакцію сусіда.



Доходить до SW1 повідомлення і він генерує у відповідь. Де також узгодить режим «access», вставляє свою MAC-адресу і відправляє в дорогу до SW2.



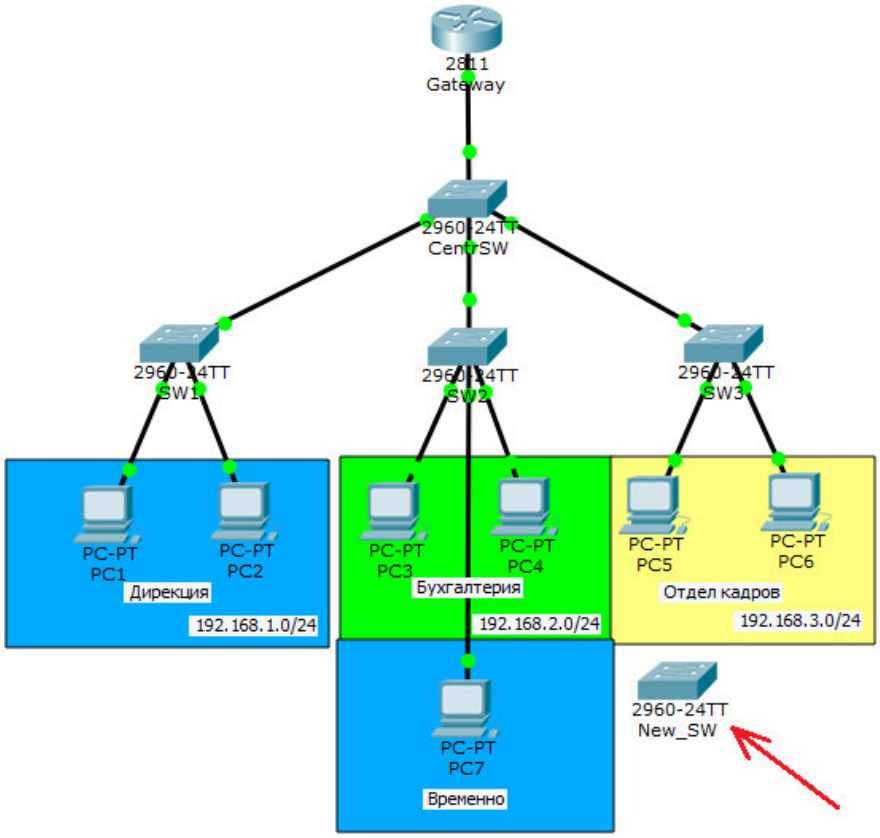
Успішно сягає DTP. За ідеєю вони мали погодитися у режимі «access». Перевірю.

```
SW1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

```
SW2#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Так стали в режим «access».

Але в цьому протоколі є проблеми з безпекою. Розглянемо попередню мережу з додатковим комутатором **New_SW**.



Тепер зайду в налаштування нового комутатора і жорстко пропишу роботу в режимі trunk.

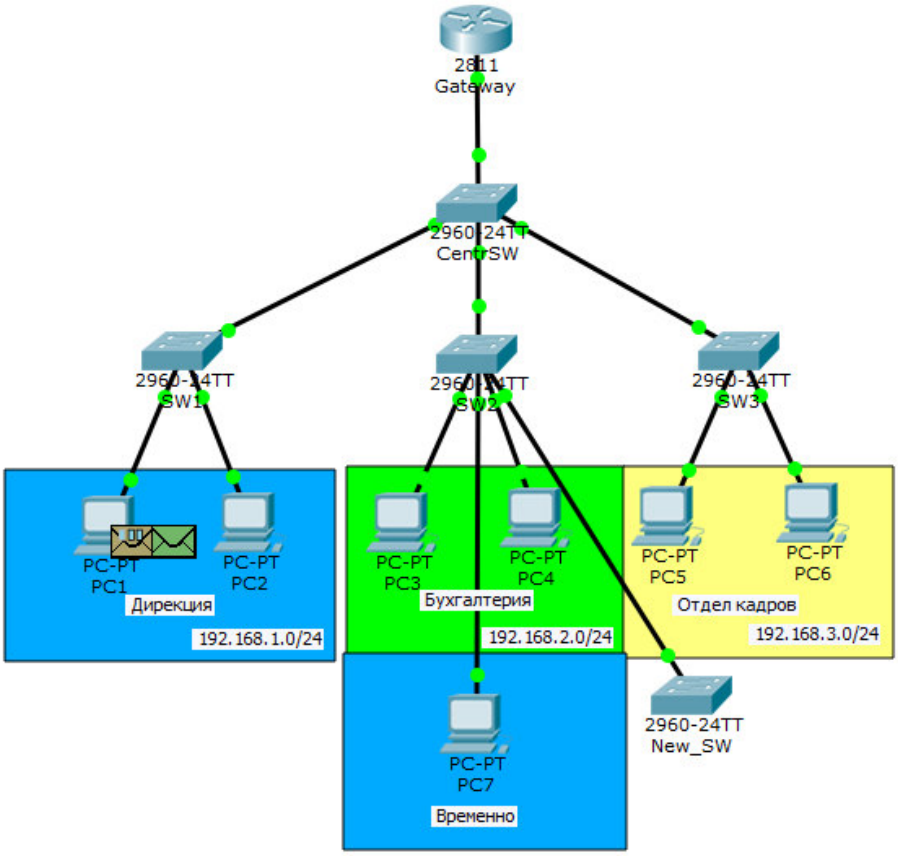
```
New_SW(config)#interface fastEthernet 0/1
New_SW(config-if)#switchport mode trunk
```

З'єдную їх і дивлюся, як вони узгодились.

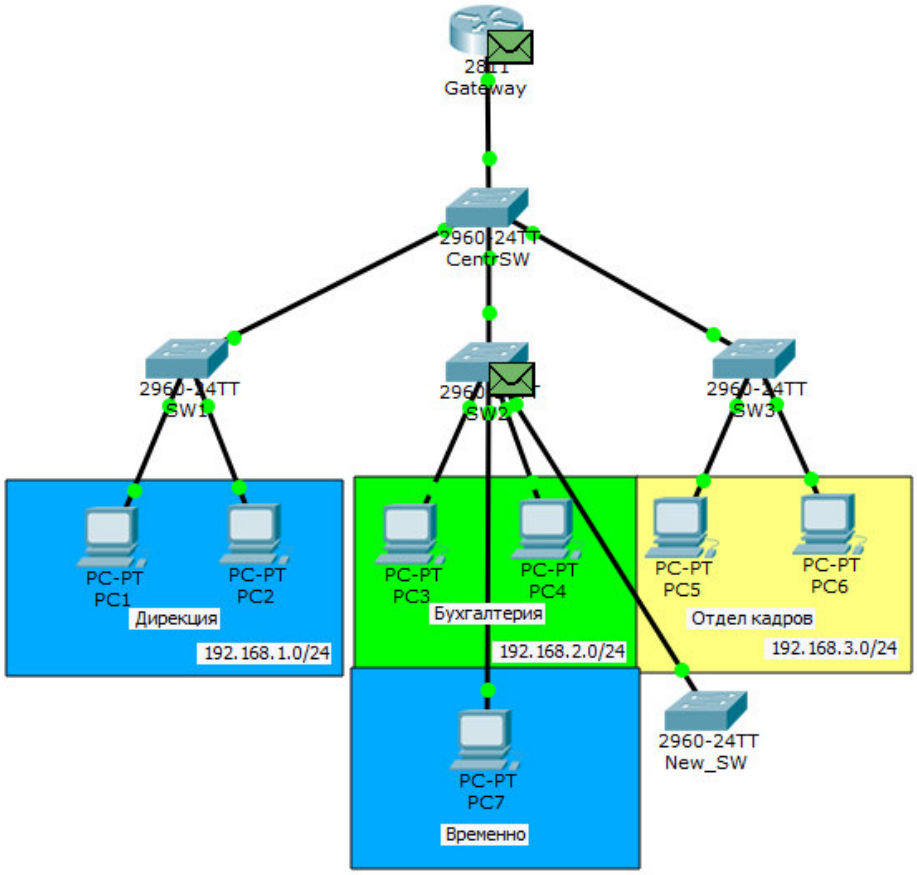
```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

```
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

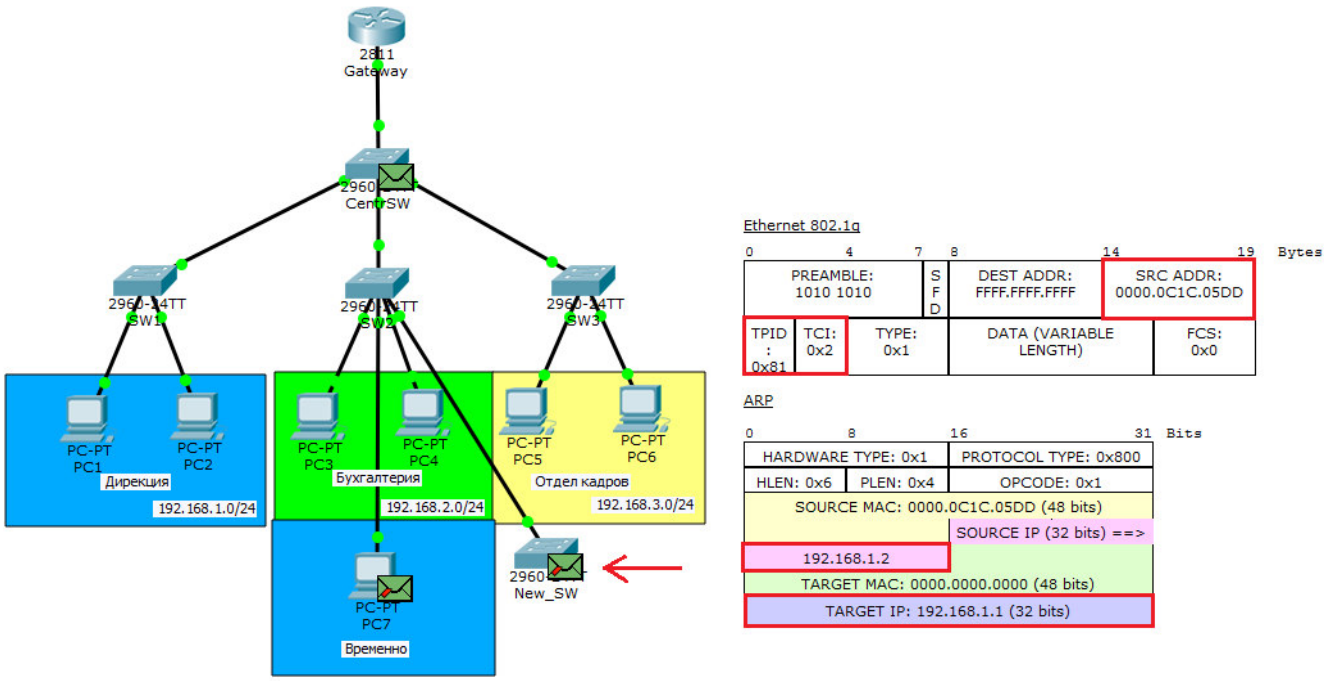
Все вірно. Режими "dynamic auto" та "trunk" узгоджуються в режим trunk. Тепер чекаємо, коли хтось почне виявляти активність. Допустимо PC1 вирішив комусь відправити повідомлення. Формує ARP та випускає в мережу.



Пропустимо його шлях до того моменту, коли він потрапить до SW2.



И от цікаве.

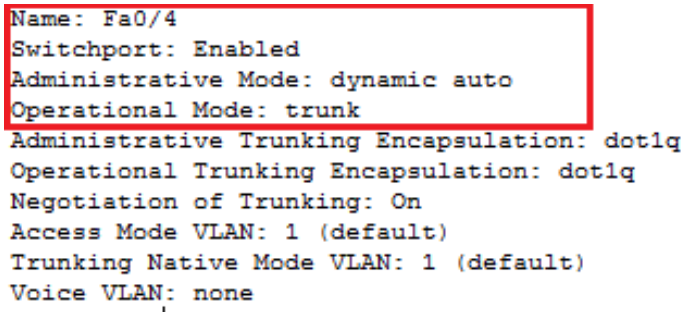


Він відправляє його на знову підключений комутатор. Пояснюю, що сталося. Як тільки ми погодили з ним trunk, він починає відправляти йому всі кадри. Хоча на схемі і показано, що комутатор відкидає кадри, це нічого не означає. До комутатора або замість комутатора можна підключити будь-який перехоплюючий пристрій (sniffer) і спокійно переглядати, що відбувається в мережі.

Начебто перехопив він невинний ARP. Але якщо поглянути глибше, то можна побачити, що вже відома MAC-адреса «0000.0C1C.05DD» та IP-адреса «192.168.1.2». Тобто PC1 не думаючи видав себе. Тепер зловмисник знає про такий комп'ютер. Також він знає, що він сидить у другому VLAN. Далі він може наробити багато чого. Найбанальне – це підмінити свою MAC-адресу, IP-адресу, погодитися швидко в Access і видавати себе за PC1. Але найцікавіше. Адже одразу можна цього не зрозуміти. Зазвичай, коли ми прописуємо режим роботи порту, він відразу відображається в конфігурації. Вводжу **show running-config**.

```
interface FastEthernet0/1
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
```

Але тут налаштування порта пусті. Ввожу **show interfaces switchport** і проматую до fa0/4.



А ось тут бачимо, що узгоджено trunk. Не завжди show running-config дає вичерпну інформацію. Тому запам'ятовуйте інші команди.

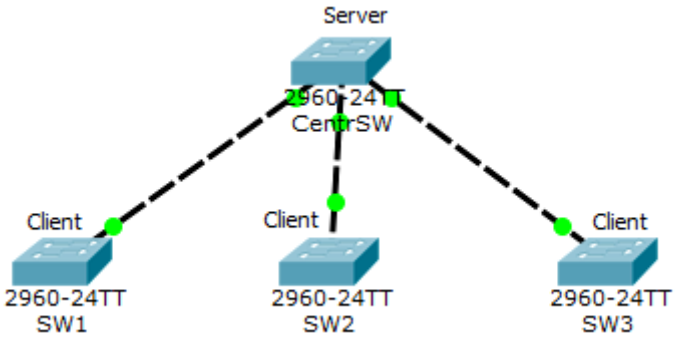
Думаю, зрозуміло чому не можна довіряти цьому протоколу. Він начебто полегшує життя, але водночас може створити величезну проблему. Тому покладайтеся на ручний спосіб. При налаштуванні відразу ж позначте собі, які порти будуть працювати в режимі trunk, а які в access. І найголовніше – завжди відключайте узгодження. Щоби комутатори не намагалися ні з ким погодитися. Робиться це командою "switchport nonegotiate".

Переходимо до наступного протоколу.

VTP (англ. VLAN Trunking Protocol)

пропрієтарний протокол компанії Cisco, що служить для обміну інформацією про VLAN-и.

Уявіть ситуацію, що у вас 40 комутаторів та 70 VLAN-ів. По хорошому потрібно вручну на кожному комутаторі їх створити і прописати на яких trunk портах дозволяти передачу. Справа ця нудна і довга. Тому це завдання може взяти на себе VTP. Ви створюєте VLAN на одному комутаторі, а решта синхронізуються з його базою. Подивіться на наступну топологію.



Тут присутні 4 комутатори. Один із них є VTP-сервером, а 3 інших клієнтами. Ті VLAN, які будуть створені на сервері, автоматично синхронізуються на клієнтах. Поясню як працює VTP і що він уміє.

Отже. VTP може створювати, змінювати та видаляти VLAN. Кожна така дія тягне за собою, що збільшується номер ревізії (кожна дія збільшує номер на +1). Після цього він розсилає оголошення, де вказаний номер ревізії. Клієнти, які отримали це оголошення, порівнюють свій номер ревізії з тим, що прийшов. І якщо номер співпадає, вони синхронізують свою базу з нею (ревізією). Інакше оголошення ігнорується.

Але це ще не все. VTP має ролі. За замовчуванням усі комутатори працюють у ролі сервера. Розповім про них.

1. **VTP Server**. Вміє все. Тобто створює, змінює, видаляє VLAN. Якщо отримує оголошення, в яких ревізія старша за нього, то синхронізується. Постійно розсилає оголошення та ретранслює від сусідів.
2. **VTP Client** – Ця роль обмежена. Не можна створювати, змінювати та видаляти VLAN. Усі VLAN отримує та синхронізує від сервера. Періодично повідомляє сусідів про свою базу VLAN-ів.
3. **VTP Transparent** – ця така незалежна роль. Може створювати, змінювати та видаляти VLAN лише у своїй базі. Нікому нічого не нав'язує і ні від кого не сприймає. Якщо отримує якесь оголошення, передає далі, але зі своєю базою не синхронізує. Якщо попередніх ролях, при кожному зміні збільшувався номер ревізії, то цьому режимі номер ревізії завжди дорівнює 0.

Це все, що стосується VTP версії 2. У VTP третьої версії додалася ще одна роль – **VTP Off**. Він не передає жодних оголошень. В іншому робота аналогічна режиму Transparent.

Начиталися теорії та переходимо до практики. Перевіримо, що центральний комутатор у режимі Server. Вводимо команду **show vtp status**.

```
CentrSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Бачимо, що VTP Operating Mode: Server. Також можна побачити, що версія VTP друга. На жаль, у CPT 3-я версія не підтримується. Версія ревізії нульова.
Тепер налаштуємо нижні комутатори.

```
SW1(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

Бачимо повідомлення, що пристрій перейшов у режим клієнта. Інші налаштовуються так само.

Щоб обмінюватись оголошеннями, вони повинні перебувати в одному домені. Причому тут є особливість. Якщо пристрій (в режимі Server або Client) не перебуває в жодному домені, то при першому отриманому оголошенні перейде в оголошений домен. Якщо ж клієнт полягає в якомусь домені, то приймати оголошення від інших доменів не буде. Відкриємо SW1 і переконаємося, що він не перебуває в жодному домені.

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Бачимо, що тут пусто.

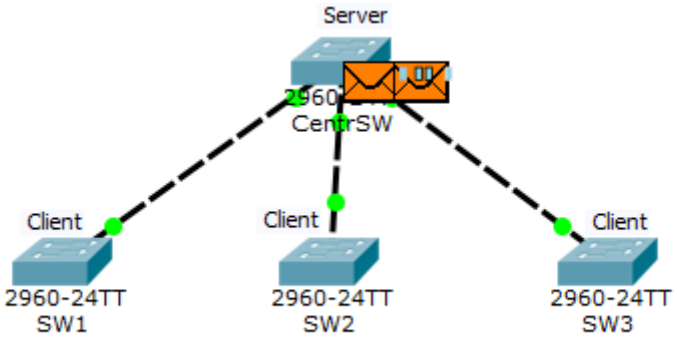
Тепер переходимо до центрального комутатора і переведемо його в домен.

```
CentrSW(config)#vtp domain cisadmin.ua
Changing VTP domain name from NULL to cisadmin.ua
```

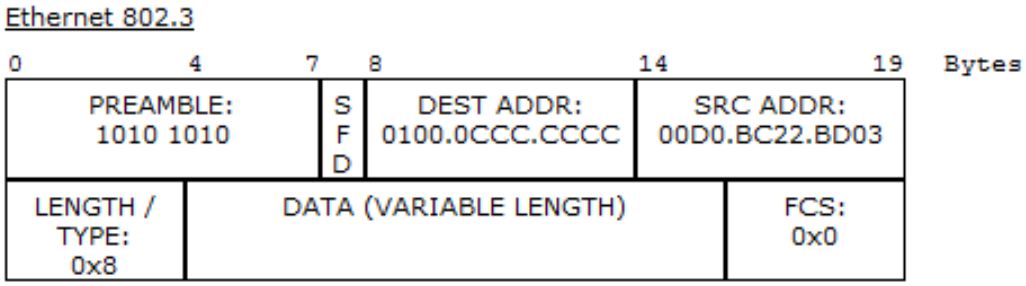
Бачимо повідомлення, що він переклався на домен **cisadmin.ua**.
Перевіримо статус.

```
CentrSW#sh
CentrSW#show vtp s
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisadmin.ua
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA4 0xF7 0xDE 0x24 0x07 0x3D 0x91 0xD2
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

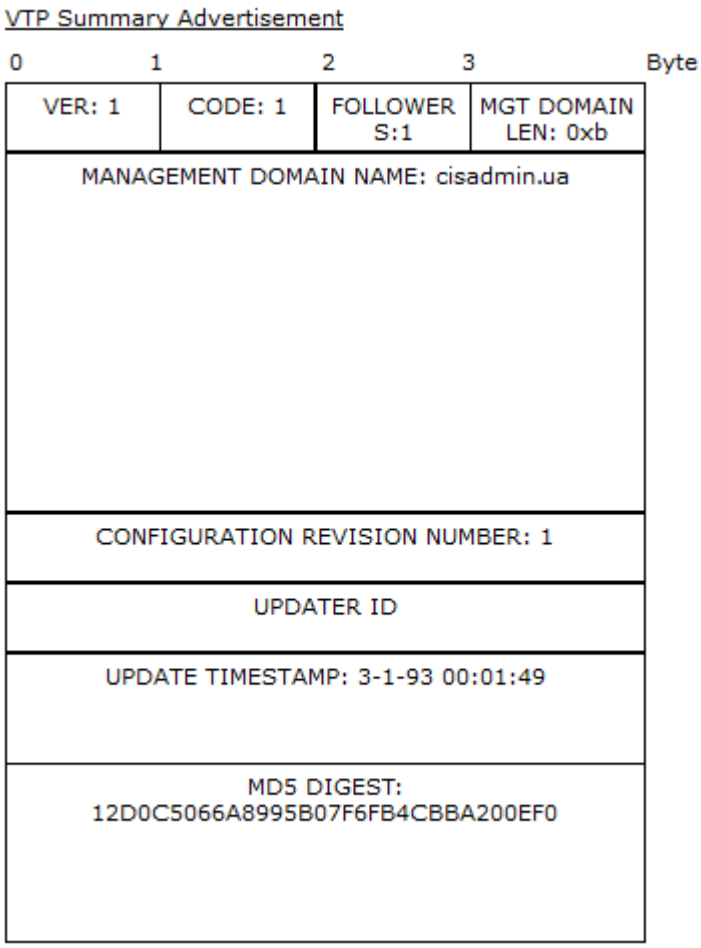
І дійсно. Ім'я домену змінилося. Зверніть увагу, що номер ревізії поки що нульовий. Він зміниться, коли ми створимо на ньому VLAN. Але перед створенням треба перевести симулятор у режим simulation, щоб побачити, як він згенерує оголошення. Створюємо 20-ий VLAN і бачимо наступну картинку.



Щойно створено VLAN та збільшився номер ревізії, сервер генерує оголошення. У нього їх два. Спочатку відкриємо той, що лівіше. Це оголошення називається "Summary Advertisement" або російською "зведене оголошення". Це оголошення генерується комутатором раз на 5 хвилин, де він розповідає про ім'я домену та поточну ревізію. Дивимось як виглядає.



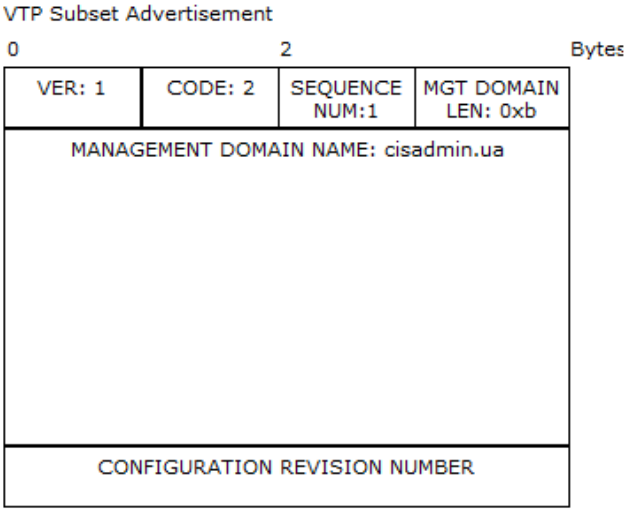
В Ethernet-кадрі зверніть увагу на Destination MAC-адресу. Він такий самий, як і вище, коли генерувався DTP. Тобто в нашому випадку на нього відреагують лише ті, у кого запущено VTP. Тепер подивимося на поле.



Тут якраз вся інформація. Пройдуся найважливішими полями.

• **Management Domain Name** – ім'я домену (в даному випадку cisadmin.ua).
• **Updater Identity** – це ідентифікатор того, хто оновлює. Тут, як правило, записується IP-адреса. Але оскільки адресу комутатору не надавали, то поле порожнє
• **Update Timestamp** – час оновлення. Час на комутаторі не мінявся, тому там стоїть заводський.
• **MD5 Digest** – хеш MD5. Воно використовується для перевірки повноважень.

Тобто якщо на VTP стоїть пароль. Ми пароль не змінювали, тому хеш за замовчуванням.
Тепер подивимося на наступне повідомлення, що генерується (те, що праворуч). Воно називається "Subset Advertisement" або "Детальне оголошення". Це така докладна інформація про кожен переданий VLAN.



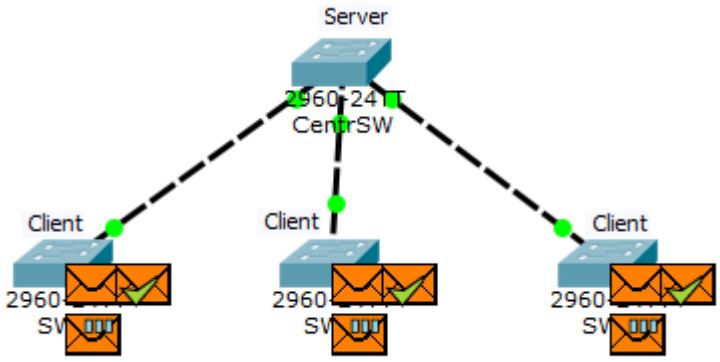
VTP VLAN Information

0		2	Bytes
VLAN INFO LEN	STATUS: 0	VLAN TYPE: 1	VLAN NAME LEN: 0x7
VLAN ID: 0x1		MTU SIZE: 0x13	
802.10 INDEX			
VLAN NAME: default			

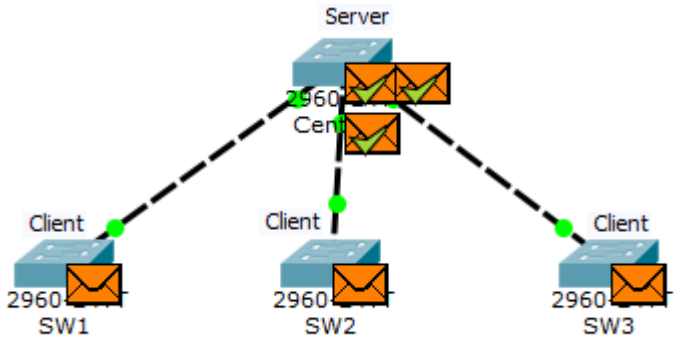
VTP VLAN Information

0		2	Bytes
VLAN INFO LEN	STATUS: 0	VLAN TYPE: 1	VLAN NAME LEN: 0x8
VLAN ID: 0x14		MTU SIZE: 0x14	
802.10 INDEX			
VLAN NAME: VLAN0020			

Тут зрозуміло. Окремий заголовок кожного типу VLAN. Список такий довгий, що не помістився в екран. Але вони такі, крім назв. Розглядати, що означає кожен код не будемо і в CPT вони тут більші за умовність. Дивимося, що відбувається далі.



Отримують клієнти оголошення. Бачать, що номер ревізії вище, ніж і синхронізують базу. І надсилають повідомлення серверу про те, що база VLAN змінилася.



Отак у принципі працює протокол VTP. Але він має дуже великі мінуси. І мінуси ці щодо безпеки. Поясню з прикладу. У нас є центральний комутатор, на якому створюються VLAN, а потім за мультикастом він їх синхронізує з усіма комутаторами. У нашому випадку він розповідає про VLAN 20. Пропоную ще раз глянути на його конфігурацію.

```
CentrSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : cisadmin.ru
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF6 0x6B 0x63 0xA2 0xD2 0x4F 0x30 0xAA
```

```
CentrSW#show vlan

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
                                                 Fa0/24, Gig0/1, Gig0/2
20   VLAN0020                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

І тут до мережі ми додаємо новий комутатор. У нього немає нових VLAN-ів, крім стандартних і він не перебуває в жодному VTP-домені, але підкручено номер ревізії.

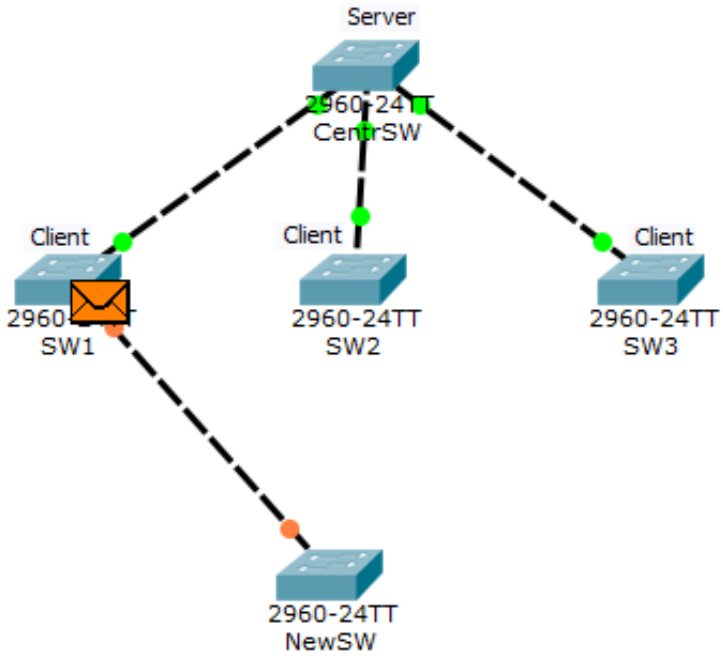
```
NewSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x64 0x4E 0x6D 0x14 0xA8 0xEC 0x2F 0xD3
```

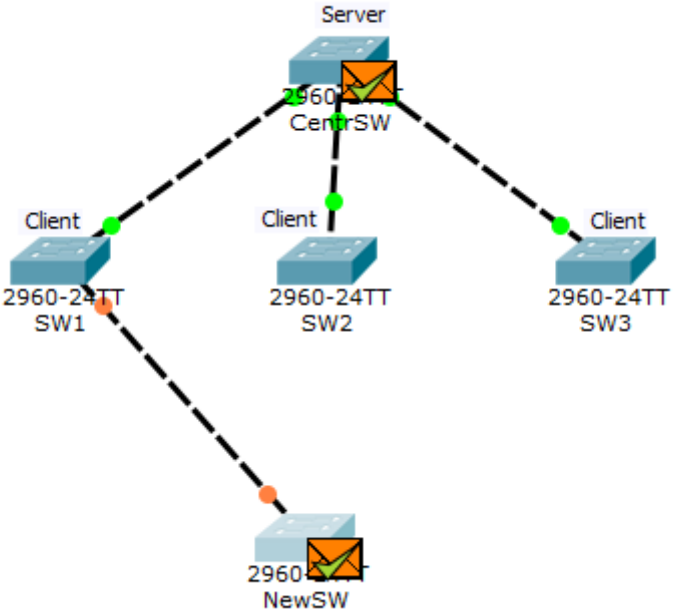
```
NewSW#show vlan

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
                                                 Gig0/1, Gig0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

І перед тим як його встромити в мережу, переводимо порт у режим **trunk**.

```
NewSW#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Тепер перемикаю CPT у «Simulation Mode» і відфільтровую все, крім VTP. Підключаюсь і дивлюся, що відбувається.

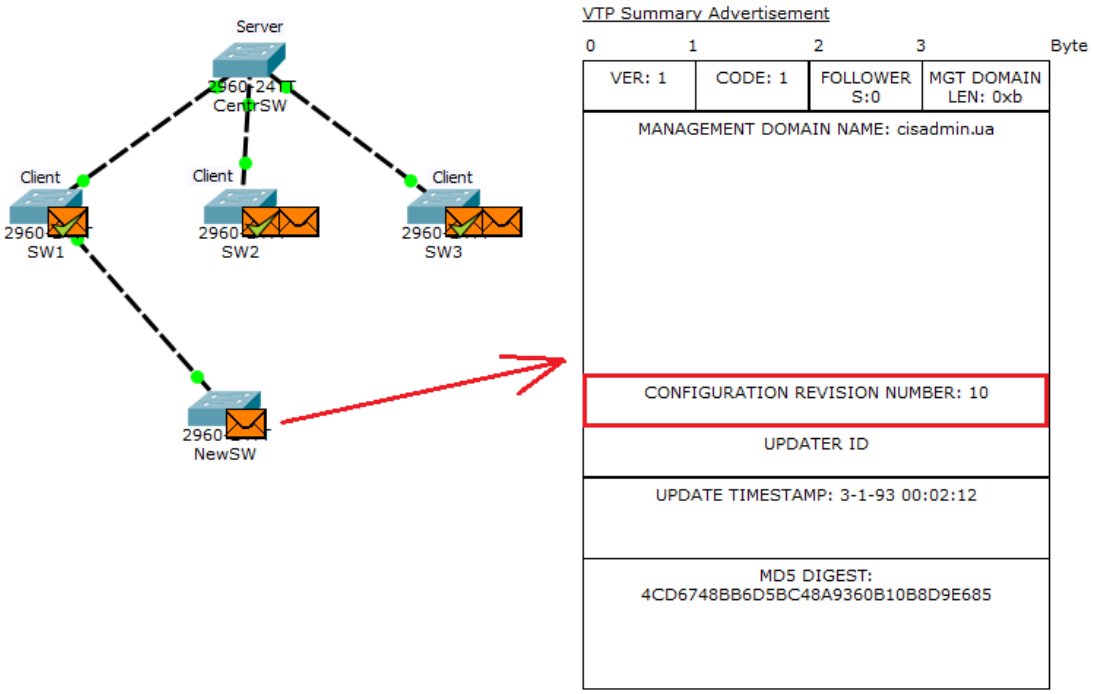




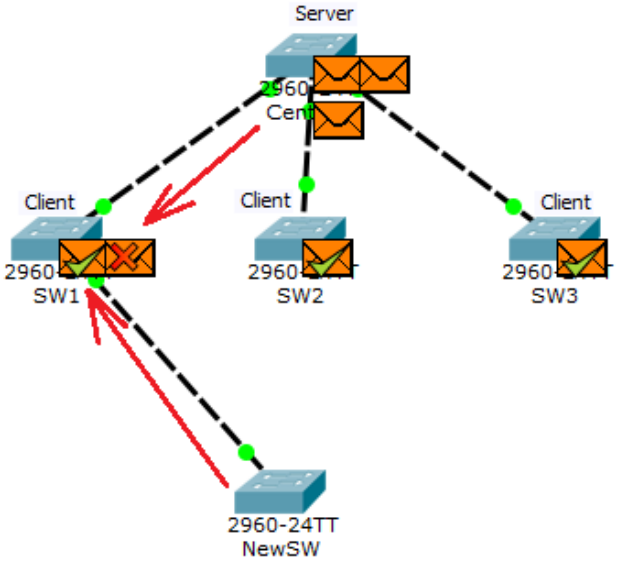
Через якийсь час до NewSW доходить VTP повідомлення, звідки він дізнається, що мережа має VTP-домен «cisadmin.ua». Так як він не був раніше в іншому домені, він автоматично в нього переходить. **Перевіримо.**

```
NewSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisadmin.ua
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4C 0xD6 0x74 0x8B 0xB6 0xD5 0xBC 0x48
```

Тепер він у тому ж домені, але має номер ревізії вище. Він формує VTP-повідомлення, де розповідає про це.



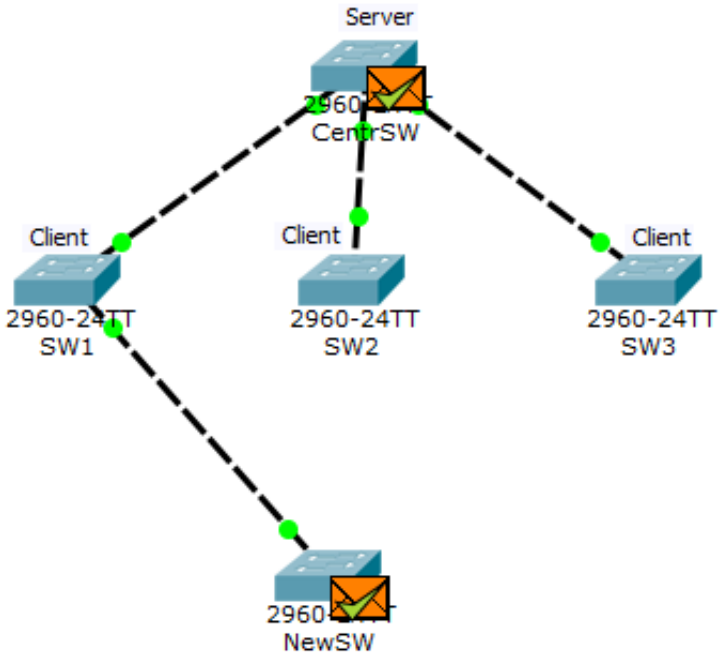
Першим під роздачу потрапляє SW1.



Зауважте, що на SW1 приходять одразу 2 VTP-повідомлення (від NewSW та від CentrSW). У повідомленні від NewSW він бачить, що номер ревізії вищий, ніж його синхронізує свою базу. А ось повідомлення від CentrSW для нього вже застаріло і він відкидає його.

Перевіримо, що змінилося на SW1.

Обновився номер ревізії та, що найцікавіше, база VLAN. Тепер вона пуста. Дивимося далі.



Зверніть увагу. До сервера доходить VTP-повідомлення, де номер ревізії вищий, ніж у нього. Він розуміє, що мережа змінилася і треба під неї підлаштуватися. Перевіримо конфігурацію.

```
CentrSW>show vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisadmin.ua
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4C 0xD6 0x74 0x8B 0xB6 0xD5 0xBC 0x48
```

```
CentrSW>show vlan

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
                                                 Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Конфігурація центрального сервера змінилася і тепер він мовитиме саме її. А тепер уявіть, що ми не один VLAN, а сотні. Ось у такий простий спосіб можна покласти мережу. Звичайно, домен може бути запаролений і зловмиснику буде важче завдати шкоди. А уявіть, що у вас зламався комутатор і терміново треба його замінити. Ви чи ваш колега біжіть на склад за старим комутатором та забуваєте перевірити номер ревізії. Він виявляється вищим ніж в інших. Що буде далі, ви вже бачили. Тому рекомендую не використовувати цей протокол. Особливо у великих корпоративних мережах. Якщо Ви використовуєте VTP 3-ї версії, то сміливо переводіть комутатори в режим «**Off**». Якщо ж використовується друга версія, то переводьте в режим «**Transparent**».