Основы компьютерных сетей. Тема №6. Понятие VLAN, Trunk и протоколы VTP и DTP

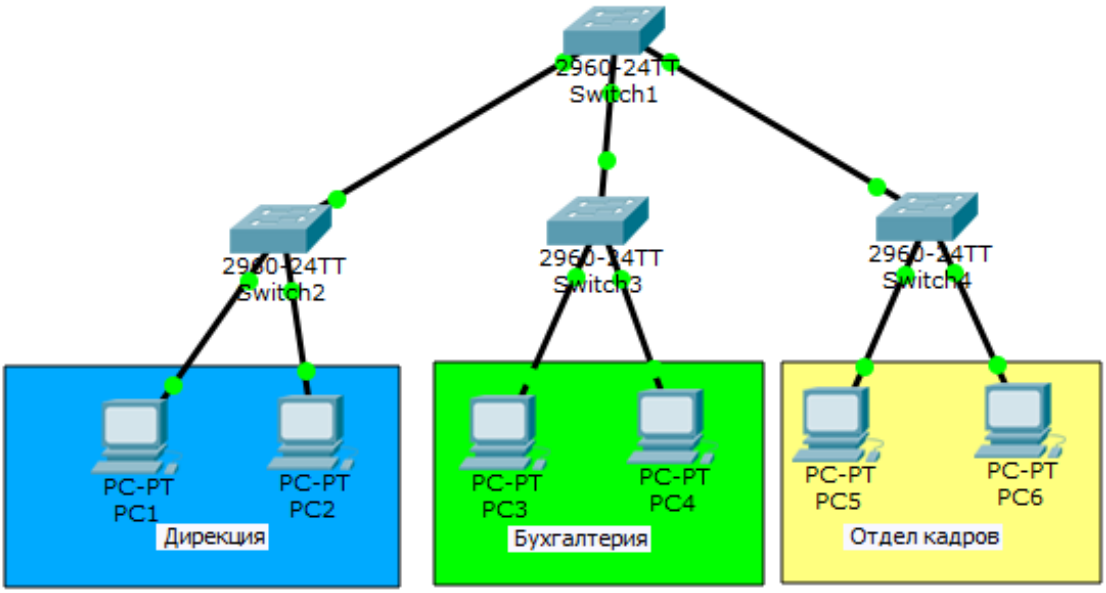
habr.com/ru/articles/319080

Денис 1 февраля 2017 г.

Всех с наступившим новым годом! Продолжаем разговор о сетях и сегодня затронем такую важную тему в мире коммутации, как VLAN. Посмотрим, что он из себя представляет и как с ним работать. А также разберем работающие с ним протоколы VTP и DTP.

Содержание

В предыдущих статьях мы уже работали с многими сетевыми устройствами, поняли, чем они друг от друга отличаются и рассмотрели из чего состоят кадры, пакеты и прочие PDU. В принципе с этими знаниями можно организовать простейшую локальную сеть и работать в ней. Но мир не стоит на месте. Появляется все больше устройств, которые нагружают сеть или что еще хуже — создают угрозу в безопасности. А, как правило, «опасность» появляется раньше «безопасности». Сейчас я на самом простом примере покажу это.

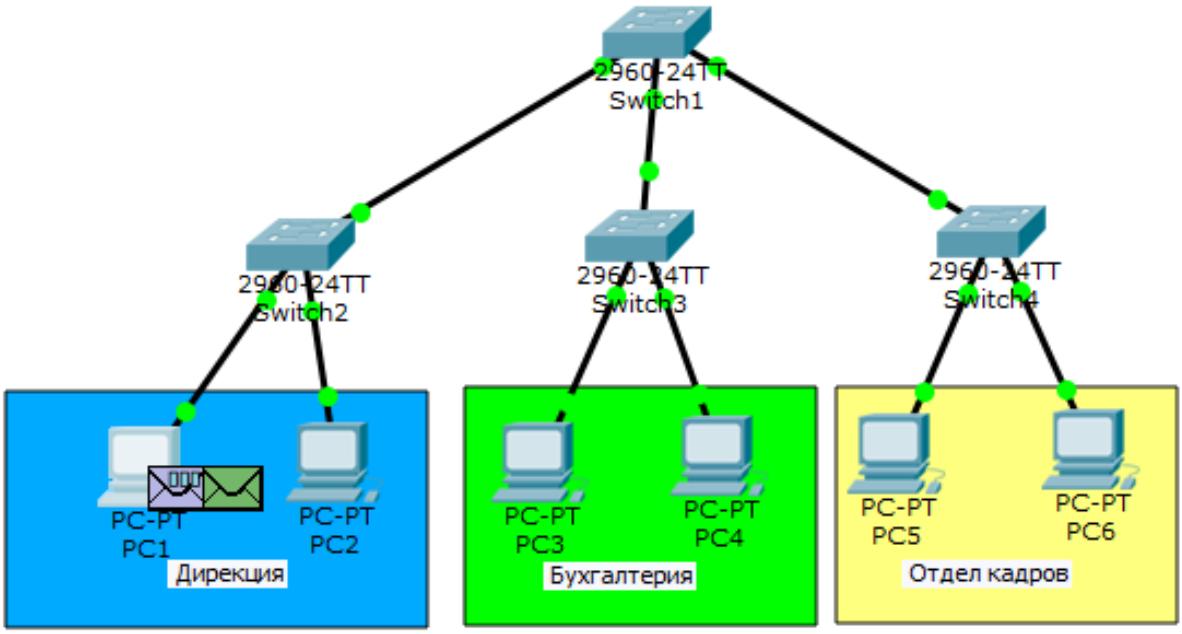


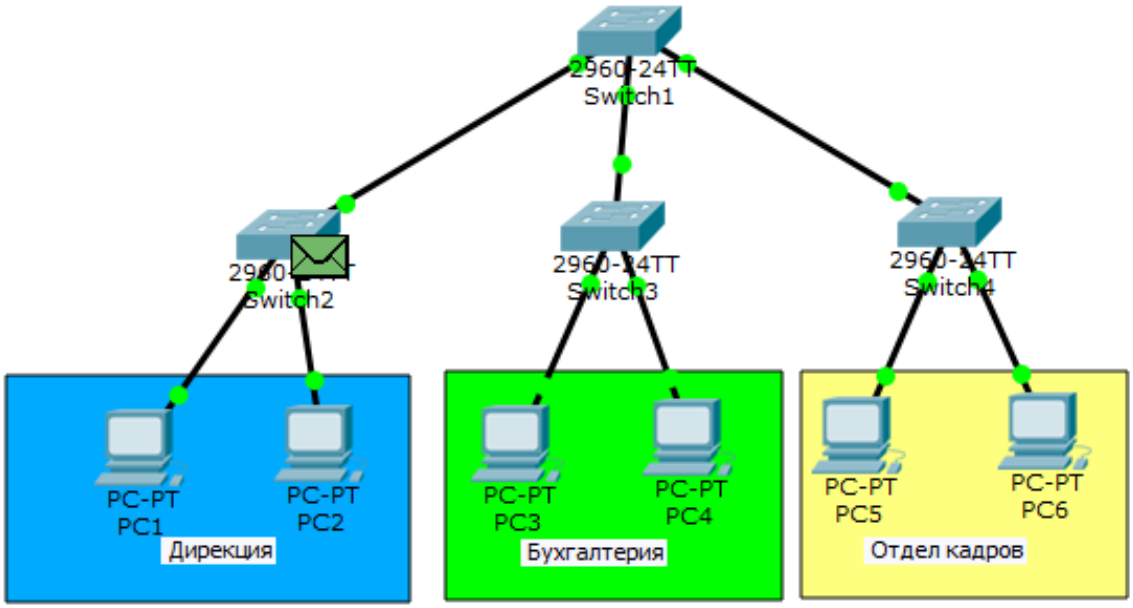
Мы пока не будем затрагивать маршрутизаторы и разные подсети. Допустим все узлы находятся в одной подсети.

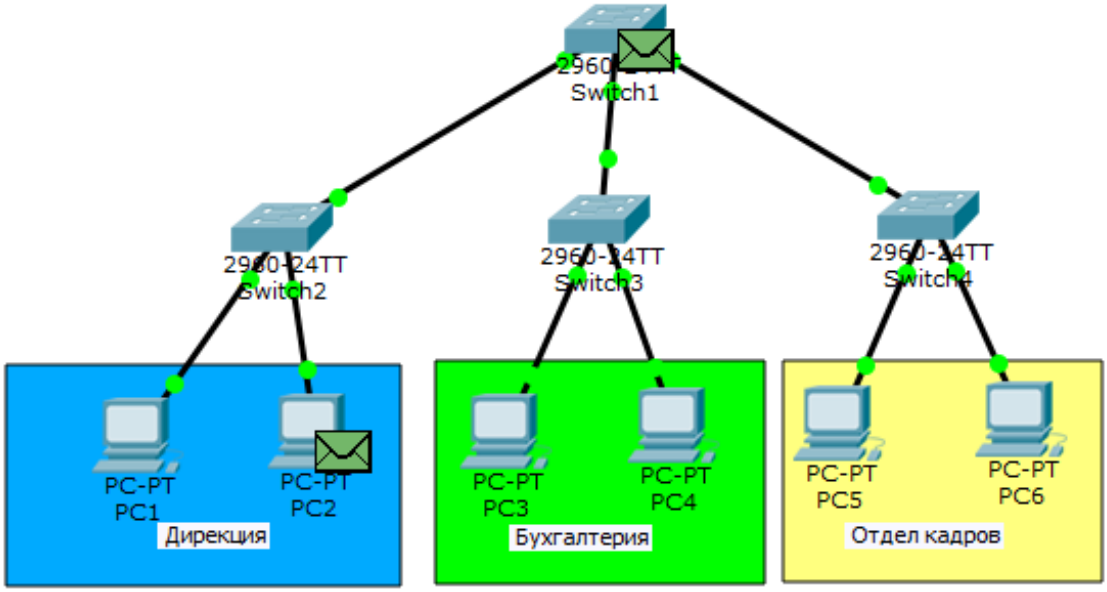
Сразу приведу список IP-адресов:

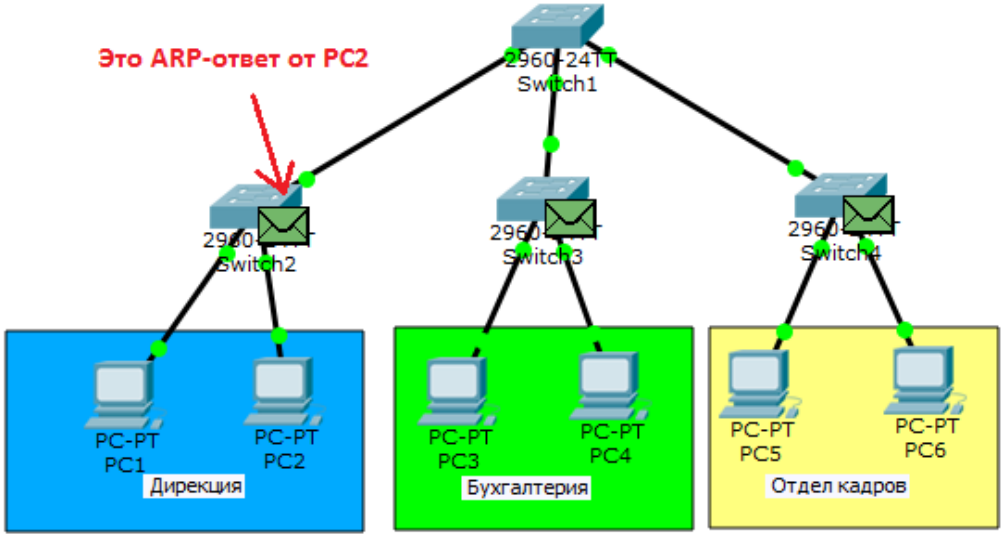
1. PC1 – 192.168.1.2/24
2. PC2 – 192.168.1.3/24
3. PC3 – 192.168.1.4/24
4. PC4 – 192.168.1.5/24
5. PC5 – 192.168.1.6/24
6. PC6 – 192.168.1.7/24

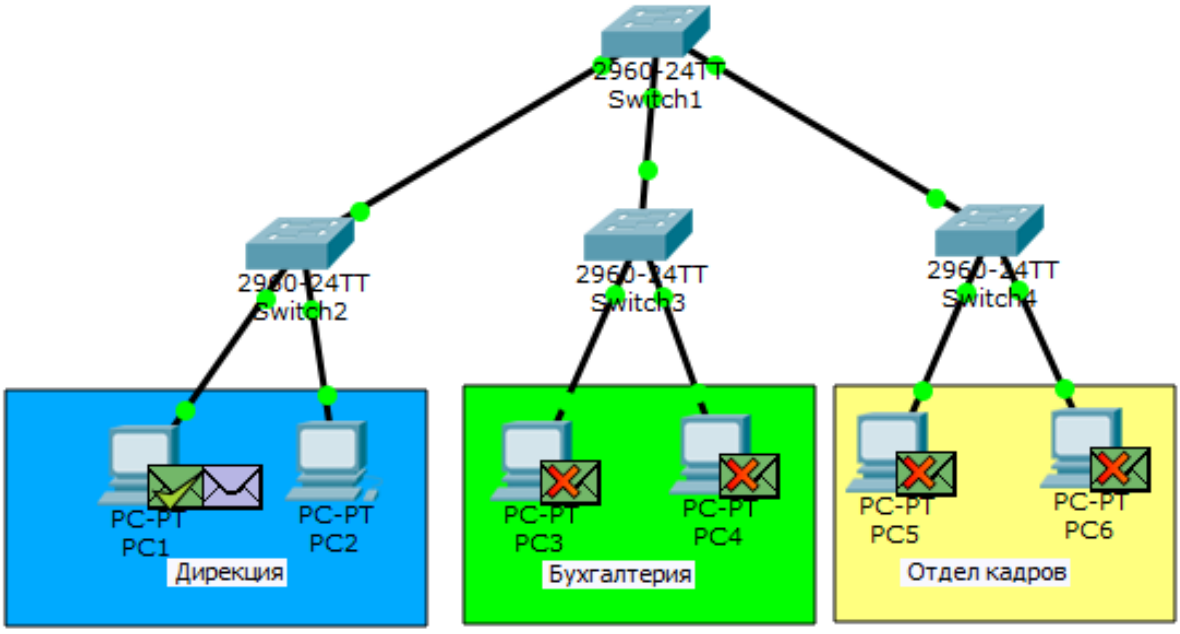
У нас 3 отдела: дирекция, бухгалтерия, отдел кадров. У каждого отдела свой коммутатор и соединены они через центральный верхний. И вот PC1 отправляет ping на компьютер PC2.


2960-24TT
Switch1
2960-24TT
Switch2
2960-24TT
Switch3
2960-24TT
Switch4
PC-PT
PC1
PC-PT
PC2
Дирекция
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
PC-PT
PC5
PC-PT
PC6
Отдел кадров


2960-24TT
Switch1
2960-24TT
Switch3
2960-24TT
Switch4
PC-PT
PC1
PC-PT
PC2
Дирекция
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
PC-PT
PC5
PC-PT
PC6
Отдел кадров


Switch1
Switch2
Switch3
Switch4
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
Дирекция
Бухгалтерия
Отдел кадров


Это ARP-ответ от PC2
Switch1
Switch2
Switch3
Switch4
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
Дирекция
Бухгалтерия
Отдел кадров



Кто хочет увидеть это в виде анимации, открывайте спойлер (там показан ping от PC1 до PC5).

Работа сети в одном широковещательном домене

Красиво да? Мы в прошлых статьях уже не раз говорили о работе протокола ARP, но это было еще в прошлом году, поэтому вкратце объясню. Так как PC1 не знает MAC-адрес (или адрес канального уровня) PC2, то он отправляет в разведку ARP, чтобы тот ему сообщил. Он приходит на коммутатор, откуда ретранслируется на все активные порты, то есть к PC2 и на центральный коммутатор. Из центрального коммутатора вылетит на соседние коммутаторы и так далее, пока не дойдет до всех. Вот такой не маленький трафик вызвало одно ARP-сообщение. Его получили все участники сети. Большой и не нужный трафик — это первая проблема. Вторая проблема — это безопасность. Думаю, заметили, что сообщение дошло даже до бухгалтерии, компьютеры которой вообще не участвовали в этом. Любой злоумышленник, подключившись к любому из коммутаторов, будет иметь доступ ко всей сети. В принципе сети раньше так и работали. Компьютеры находились в одной канальной среде и разделялись только при помощи маршрутизаторов. Но время шло и нужно было решать эту проблему на канальном уровне. Cisco, как пионер, придумала свой протокол, который тегировал кадры и определял принадлежность к определенной канальной среде. Назывался он **ISL (Inter-Switch Link)**. Идея эта понравилась всем и IEEE решили разработать аналогичный открытый стандарт. Стандарт получил название **802.1q**. Получил он огромное распространение и Cisco решила тоже перейти на него.
И вот как раз технология VLAN основывается на работе протокола 802.1q. Давайте уже начнем говорить про нее.

В 3-ей части я показал, как выглядит ethernet-кадр. Посмотрите на него и освежите в памяти. Вот так выглядит не тегированный кадр.

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

Теперь взглянем на тегированный.

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)

Как видим, отличие в том, что появляется некий **Тег**. Это то, что нам и интересно. Копнем глубже. Состоит он из 4-х частей.

1) **TPID (англ. Tag Protocol ID) или Идентификатор тегированного протокола** — состоит из 2-х байт и для VLAN всегда равен 0x8100.
2) **PCP (англ. Priority Code Point) или значение приоритета** — состоит из 3-х бит. Используется для приоритезации трафика. Крутые и бородатые сисадмины знают, как правильно им управлять и оперирует им, когда в сети гуляет разный трафик (голос, видео, данные и т.д.)
3) **CFI (англ. Canonical Format Indicator) или индикатор каноничного формата** — простое поле, состоящее из одного бита. Если стоит 0, то это стандартный формат MAC-адреса.
4) **VID (англ. VLAN ID) или идентификатор VLAN** — состоит из 12 бит и показывает, в каком VLAN находится кадр.

Хочу заострить внимание на том, что тегирование кадров осуществляется между сетевыми устройствами (коммутаторы, маршрутизаторы и т.д.), а между конечным узлом (компьютер, ноутбук) и сетевым устройством кадры не тегируются. Поэтому порт сетевого устройства может находиться в 2-х состояниях: **access** или **trunk**.

- **Access port или порт доступа** — порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство.
- **Trunk port или магистральный порт** — порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами.

Сейчас я покажу это на практике. Открываю ту же лабу. Картинку повторять не буду, а сразу открою коммутатор и посмотрю, что у него с VLAN.

Набираю 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
------- --------- ----------------- ------------------------------------------
```

Выстраиваются несколько таблиц. Нам по сути важна только самая первая. Теперь покажу как ее читать.

1 столбец — это номер VLAN. Здесь изначально присутствует номер 1 — это стандартный VLAN, который изначально есть на каждом коммутаторе. Он выполняет еще одну функцию, о которой чуть ниже напишу. Также присутствуют зарезервированные с 1002-1005. Это для других канальных сред, которые вряд ли сейчас используются. Удалить их тоже нельзя.

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

При удалении Cisco выводит сообщение, что этот VLAN удалить нельзя. Поэтому живем и эти 4 VLANa не трогаем.

2 столбец — это имя VLAN. При создании VLAN, вы можете на свое усмотрение придумывать им осмысленные имена, чтобы потом их идентифицировать. Тут уже есть default, fddi-default, token-ring-default, fddinet-default, trnet-default.

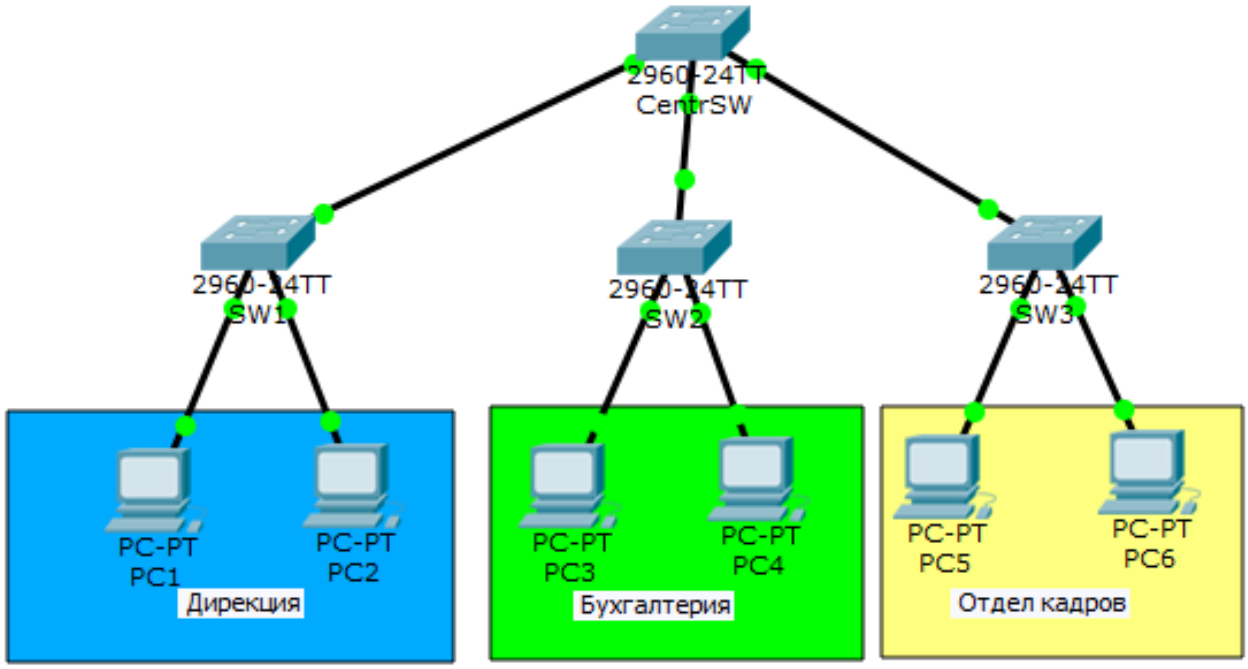
3 столбец — статус. Здесь показывается в каком состоянии находится VLAN. На данный момент VLAN 1 или default в состоянии active, а 4 следующих act/unsup (хоть и активные, но не поддерживаются).

4 столбец — порты. Здесь показано к каким VLAN-ам принадлежат порты. Сейчас, когда мы еще ничего не трогали, они находятся в default.

Приступаем к настройке коммутаторов. Правилом хорошего тона будет дать коммутаторам осмысленные имена. Чем и займемся. Привожу команду.

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

Остальные настраиваются аналогично, поэтому покажу обновленную схему топологии.



Начнем настройку с коммутатора SW1. Для начала создадим VLAN на коммутаторе.

```
SW1(config)#vlan 2 -  создаем VLAN 2 (VLAN 1 по умолчанию зарезервирован, поэтому берем следующий).
SW1(config-vlan)#name Dir-ya - попадаем в настройки VLAN и задаем ему имя.
```

VLAN создан. Теперь переходим к портам. Интерфейс FastEthernet0/1 смотрит на PC1, а FastEthernet0/2 на PC2. Как говорилось ранее, кадры между ними должны передаваться не тегированными, поэтому переведем их в состояние Access.

```
SW1(config)#interface fastEthernet 0/1 - переходим к настройке 1-ого порта.
SW1(config-if)#switchport mode access - переводим порт в режим access.
SW1(config-if)#switchport access vlan 2 - закрепляем за портом 2-ой VLAN.
SW1(config)#interface fastEthernet 0/2 - переходим к настройке 2-ого порта.
SW1(config-if)#switchport mode access - переводим порт в режим access.
SW1(config-if)#switchport access vlan 2 - закрепляем за портом 2-ой VLAN.
```

Так как оба порта закрепляются под одинаковым VLAN-ом, то их еще можно было настроить группой.

```
SW1(config)#interface range fastEthernet 0/1-2 - то есть выбираем пул и далее
настройка аналогичная.
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 2
```

Настроили access порты. Теперь настроим trunk между SW1 и CentrSW.

```
SW1(config)#interface fastEthernet 0/24 - переходим к настройке 24-ого порта.
SW1(config-if)#switchport mode trunk - переводим 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
```

Сразу видим, что порт перенастроился. В принципе для работы этого достаточно. Но с точки зрения безопасности разрешать для передачи нужно только те VLAN, которые действительно нужны. Приступим.

```
SW1(config-if)#switchport trunk allowed vlan 2 - разрешаем передавать только 2-ой
VLAN.
```

Без этой команды передаваться будут все имеющиеся VLAN. Посмотрим, как изменилась таблица командой **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
------- --------- ----------------- ------------------------------------------
```

Появился 2-ой VLAN с именем Dir-ya и видим принадлежащие ему порты fa0/1 и fa0/2.

Чтобы вывести только верхнюю таблицу, можно воспользоваться командой **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
```

Можно еще укоротить вывод, если указать определенный ID VLANa.

```
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
```

Или его имя.

```
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 информациях о VLAN хранится в flash памяти в файле 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)
```

Как вы заметили, ни в одной из команд, нет информации о trunk. Ее можно посмотреть другой командой **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
```

Здесь есть информация и о trunk портах, и о том какие VLAN они передают. Еще тут есть столбец **Native vlan**. Это как раз тот трафик, который не должен тегироваться. Если на коммутатор приходит не тегированный кадр, то он автоматически

причисляется к Native Vlan (по умолчанию и в нашем случае это VLAN 1). Native VLAN можно, а многие говорят, что нужно менять в целях безопасности. Для этого в режиме настройки транкового порта нужно применить команду — **switchport trunk native vlan X**, где **X** — номер присваиваемого VLAN. В этой топологии мы менять не будем, но знать, как это делать полезно.

Осталось настроить остальные устройства.

CentrSW:
Центральный коммутатор является связующим звеном, а значит он должен знать обо всех VLAN-ах. Поэтому сначала создаем их, а потом переводим все интерфейсы в транковый 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 забываем сохранять конфиг. Команда **copy running-config startup-config.**

SW2:

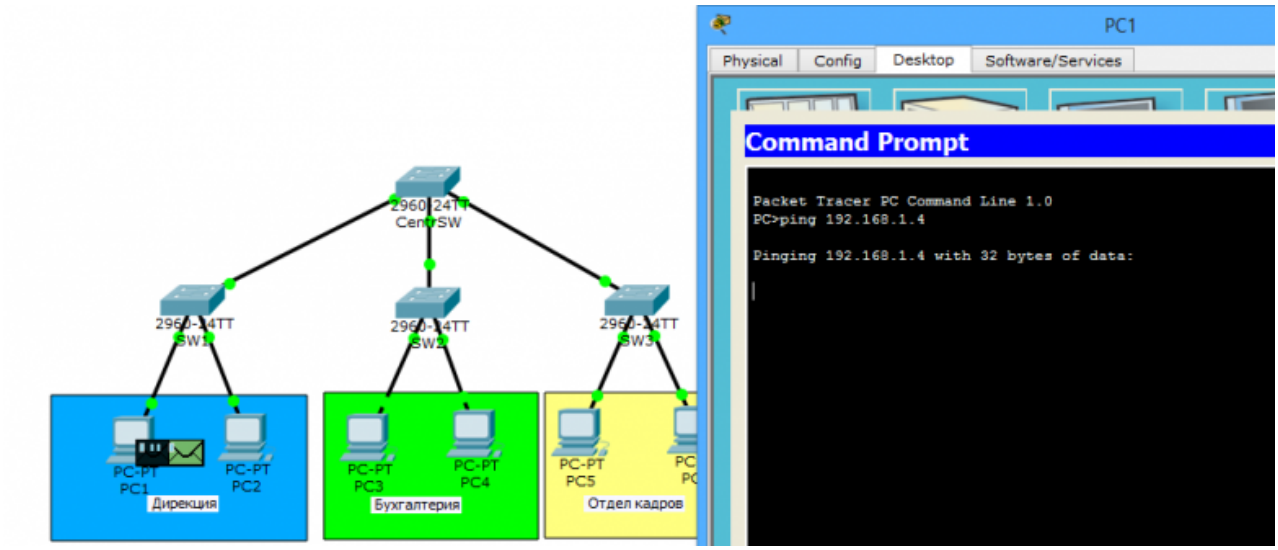
```
SW2(config)#vlan 3
SW2(config-vlan)#name buhgalter
SW2(config)#interface range fastEthernet 0/1-2
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 3
SW2(config)#interface fastEthernet 0/24
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk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

SW3:

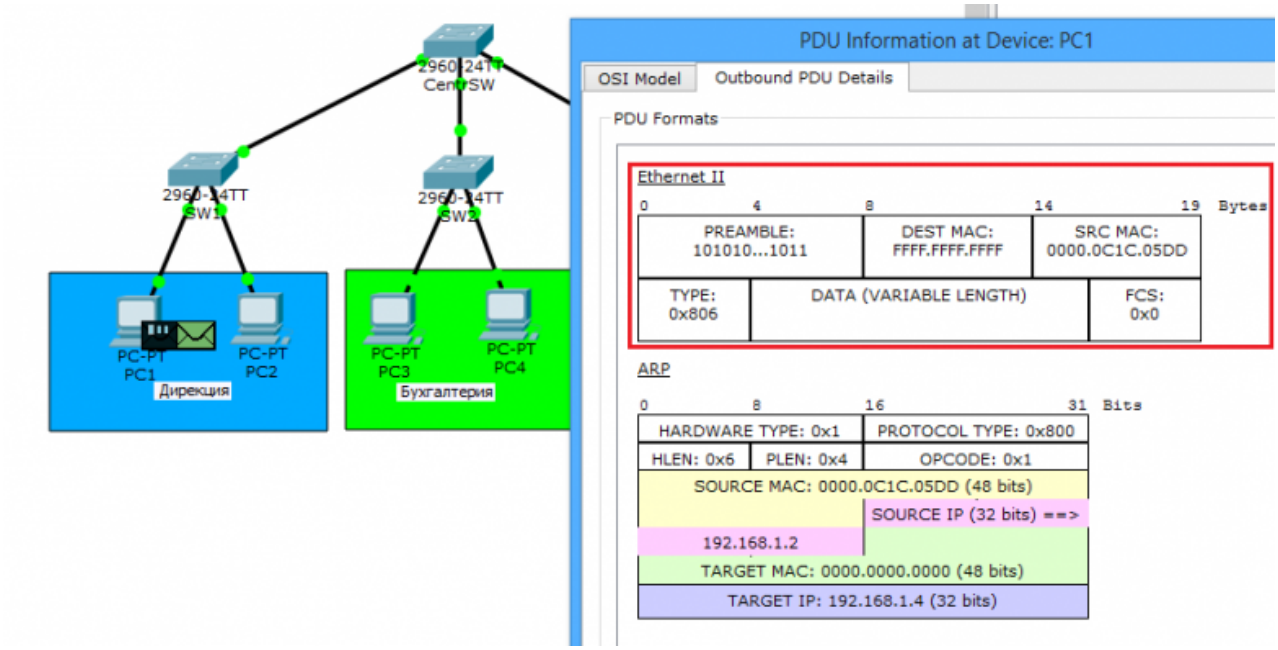
```
SW3(config)#vlan 4
SW3(config-vlan)#name otdel kadrov
SW3(config)#interface range fastEthernet 0/1-2
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 4
SW3(config)#interface fastEthernet 0/24
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk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

Обратите внимание на то, что мы подняли и настроили VLAN, но адресацию узлов оставили такой же. То есть, фактически все узлы в одной подсети, но разделены VLAN-ами. Так делать нельзя. Каждому VLAN надо выделять отдельную подсеть. Я

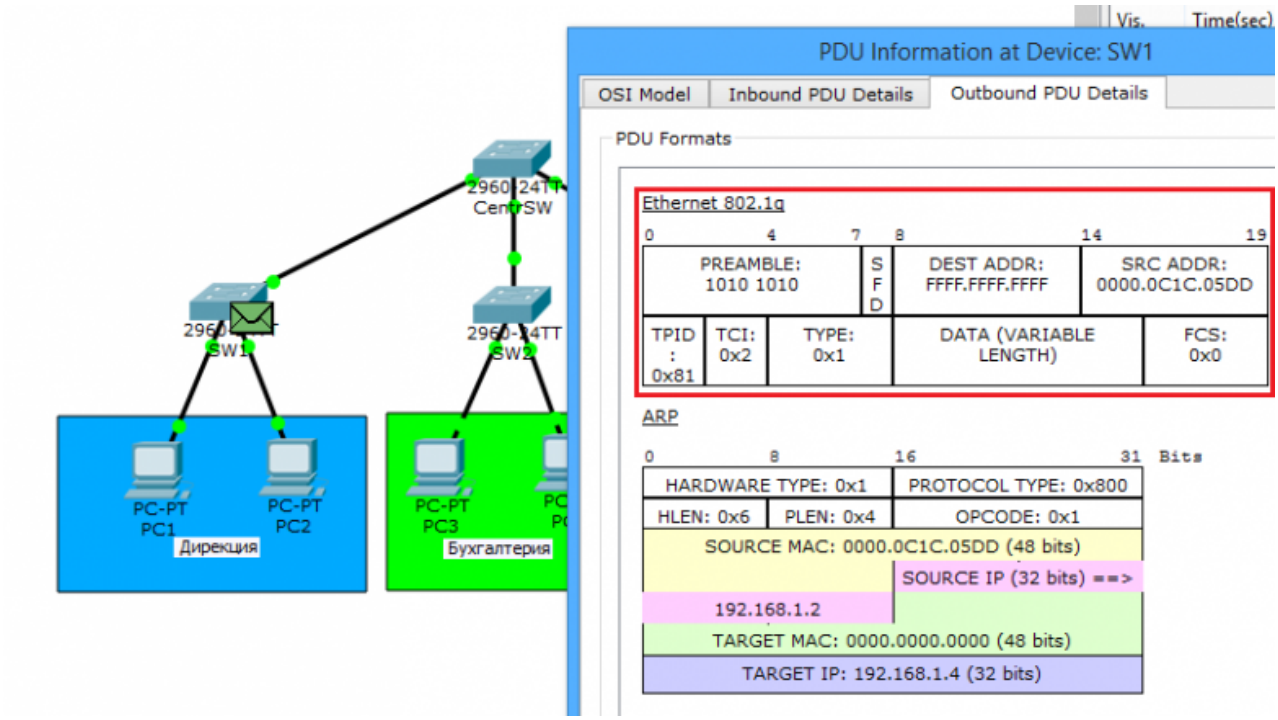
это сделал исключительно в учебных целях. Если бы каждый отдел сидел в своей подсети, то они бы априори были ограничены, так как коммутатор не умеет маршрутизировать трафик из одной подсети в другую (плюс это уже ограничение на сетевом уровне). А нам нужно ограничить отделы на канальном уровне.
Снова отправляю ping с PC1 к PC3.



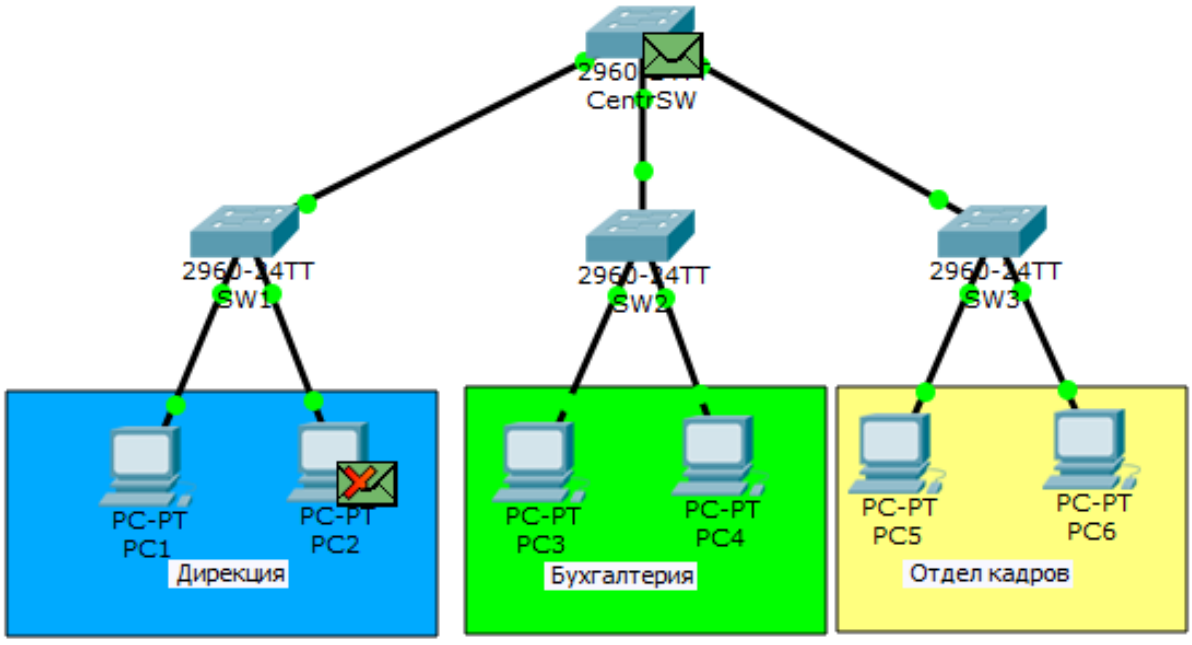
Идет в ход ARP, который нам и нужен сейчас. Откроем его.



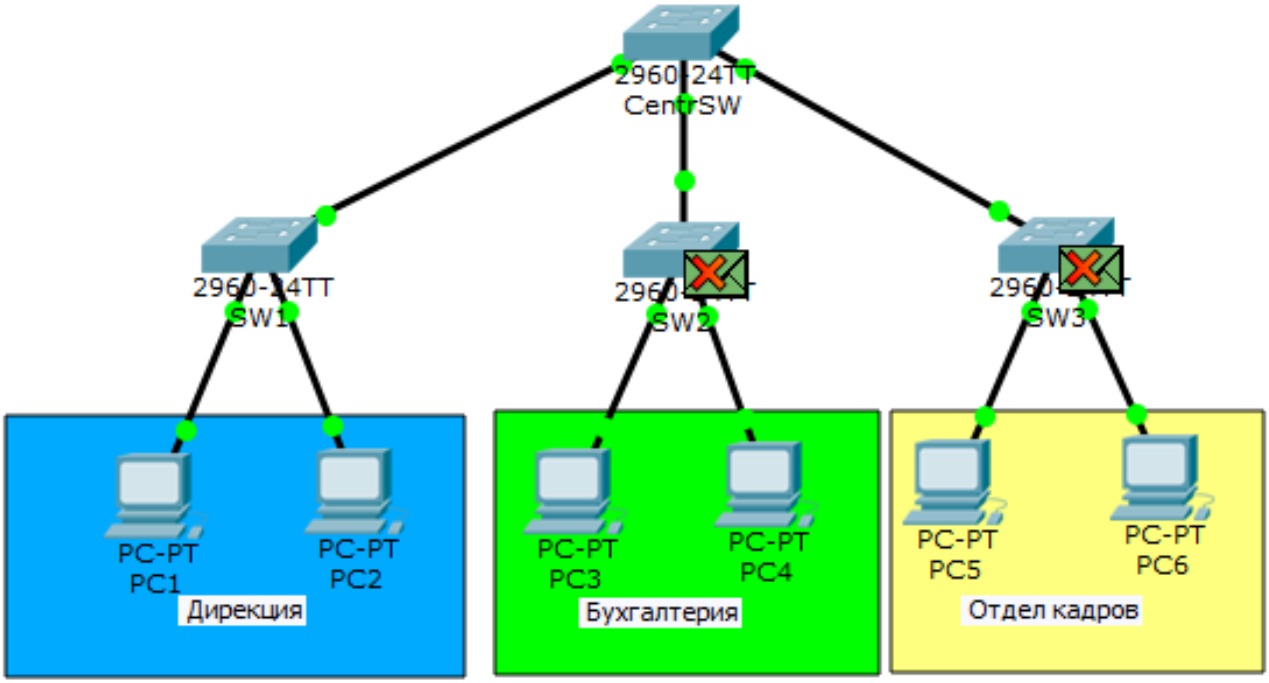
Пока что ничего нового. ARP инкапсулирован в ethernet.



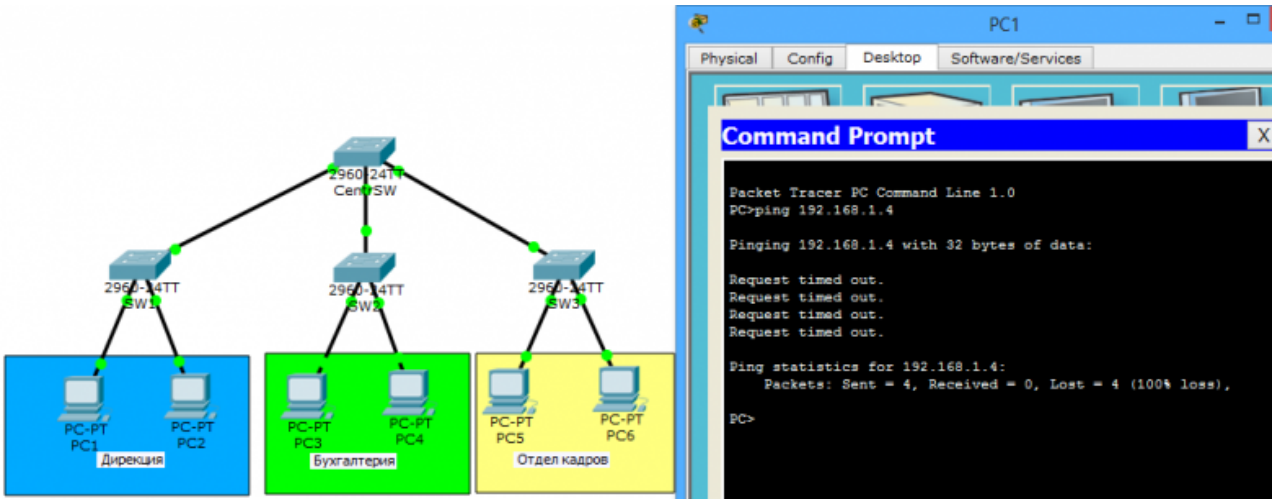
Кадр прилетает на коммутатор и тегируется. Теперь там не обычный ethernet, а 802.1q. Добавились поля, о которых я писал ранее. Это **TPID**, который равен 8100 и показывающий, что это 802.1q. И **TCI**, которое объединяет 3 поля **PCP, CFI и VID**. Число, которое в этом поле — это номер VLAN. Двигаемся дальше.



После тега он отправляет кадр на PC2 (т.к. он в том же VLAN) и на центральный коммутатор по транковому порту.



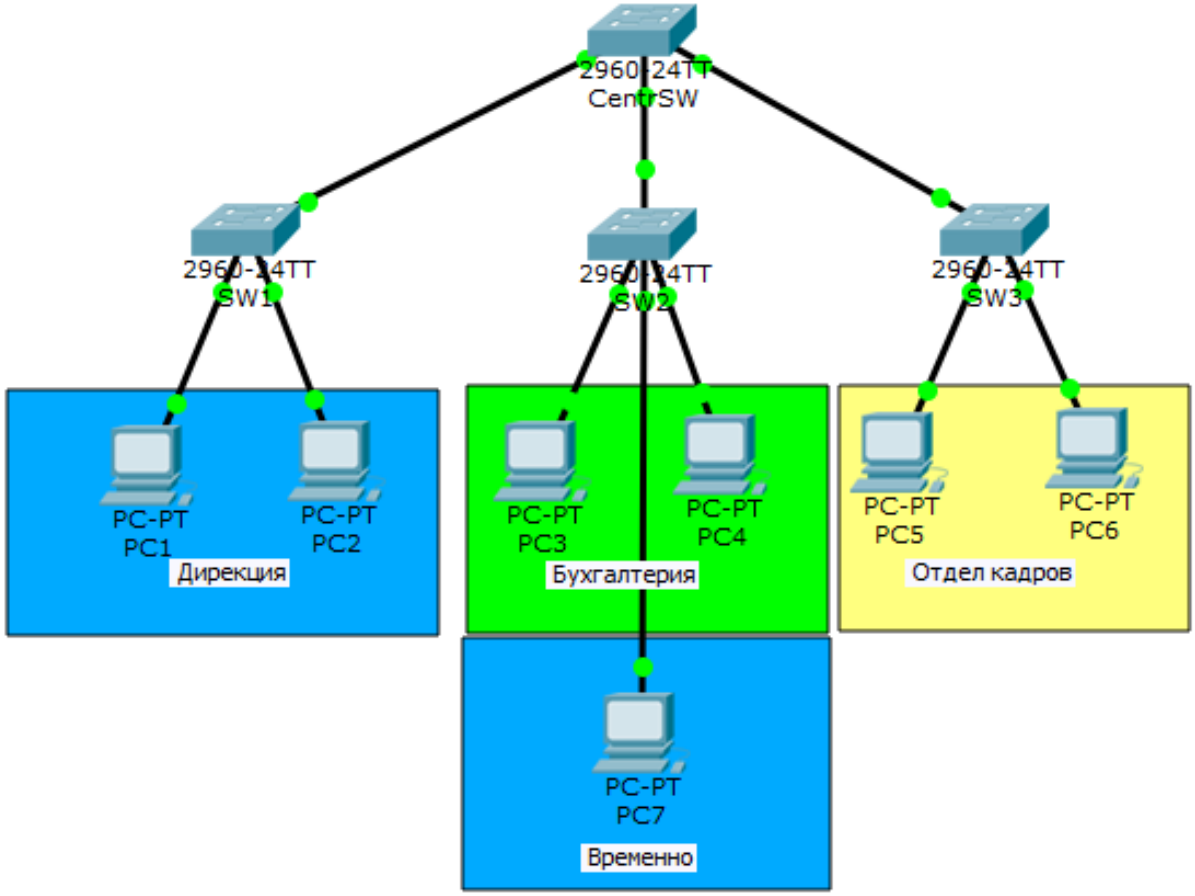
Так как жестко не было прописано какие типы VLAN пропускать по каким портам, то он отправит на оба коммутатора. И вот здесь коммутаторы, увидев номер VLAN, понимают, что устройств с таким VLAN-ом у них нет и смело его отбрасывают.



PC1 ожидает ответ, который так и не приходит. Можно под спойлером посмотреть в виде анимации.

Анимация

Теперь следующая ситуация. В состав дирекции нанимают еще одного человека, но в кабинете дирекции нет места и на время просят разместить человека в отделе бухгалтерии. Решаем эту 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
```

Дальше настраиваем порт FastEthernet 0/3, который смотрит на PC7.

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

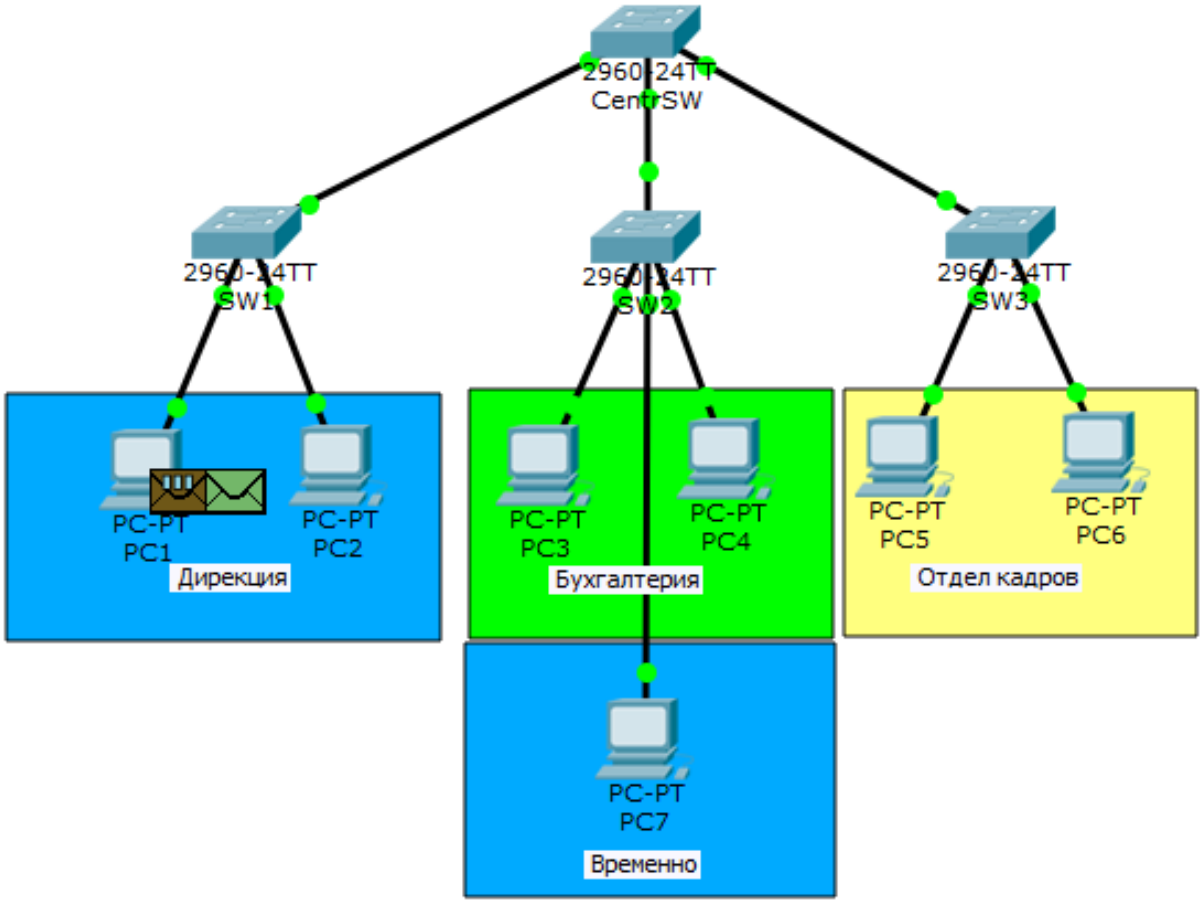
И последнее — настроить транковый порт.

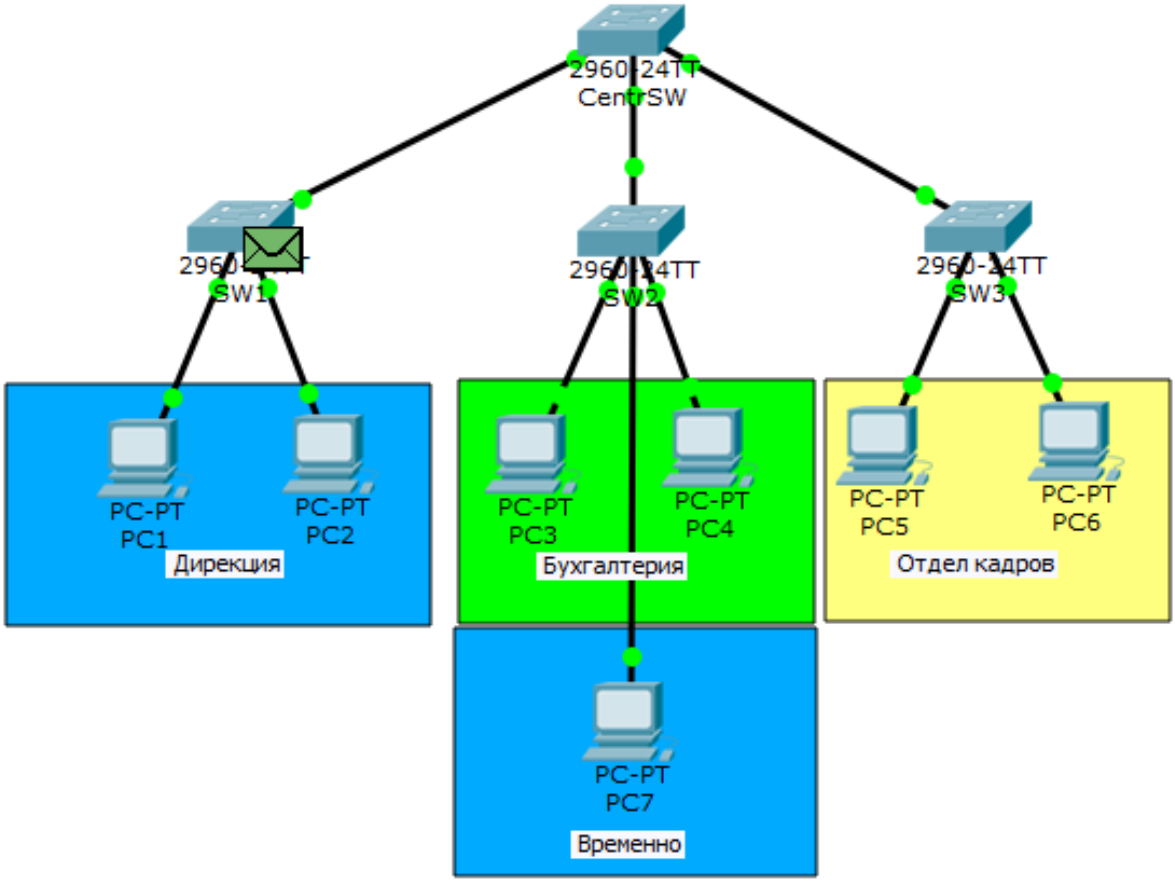
```
SW2(config)#interface fastEthernet 0/24
SW2(config-if)#switchport trunk allowed vlan add 2 - обратите внимание на эту
команду.
А именно на ключевое слово "add". Если не дописать это слово, то вы сотрете все
остальные разрешенные к передаче VLAN на этом порту.
Поэтому если у вас уже был поднят транк на порту и передавались другие VLAN, то
добавлять надо именно так.
```

Чтобы кадры ходили красиво, подкорректирую центральный коммутатор **CentrSW.**

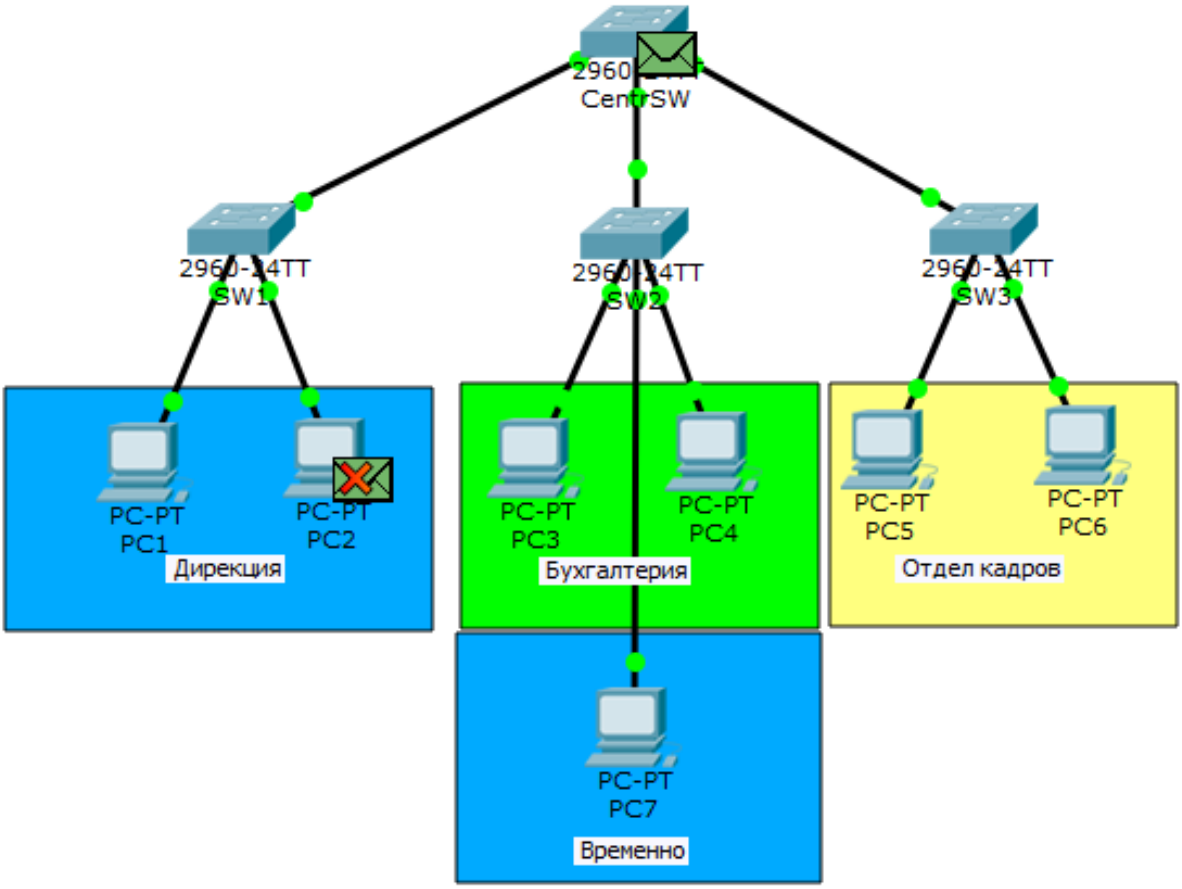
```
CentrSW(config)#interface fastEthernet 0/1
CentrSW(config-if)#switchport trunk allowed vlan 2
CentrSW(config)#interface fastEthernet 0/2
CentrSW(config-if)#switchport trunk allowed vlan 2,3
CentrSW(config)#interface fastEthernet 0/3
CentrSW(config-if)#switchport trunk allowed vlan 4
```

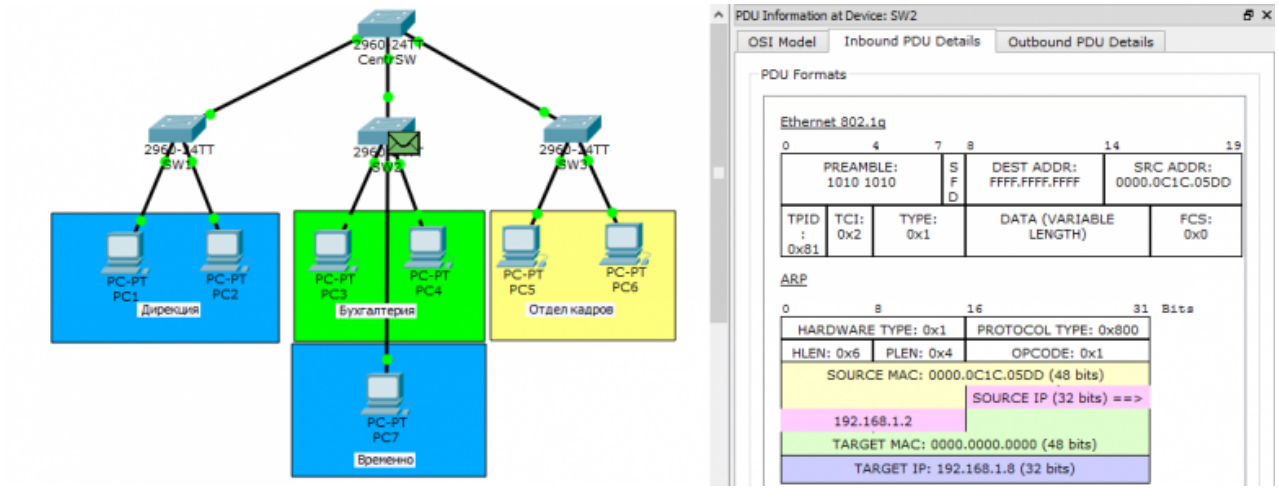
Время проверки. Отправляю ping с PC1 на PC7.



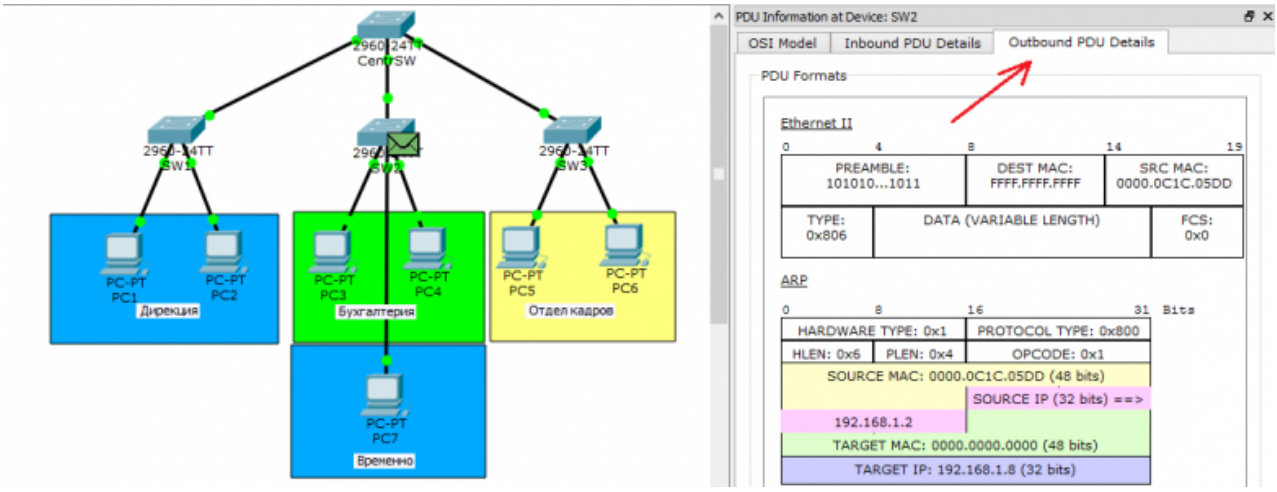


Пока что весь путь аналогичен предыдущему. Но вот с этого момента (с картинки ниже) центральный коммутатор примет другое решение. Он получает кадр и видит, что тот протегирован 2-ым VLAN-ом. Значит отправлять его надо только туда, где это разрешено, то есть на порт fa0/2.

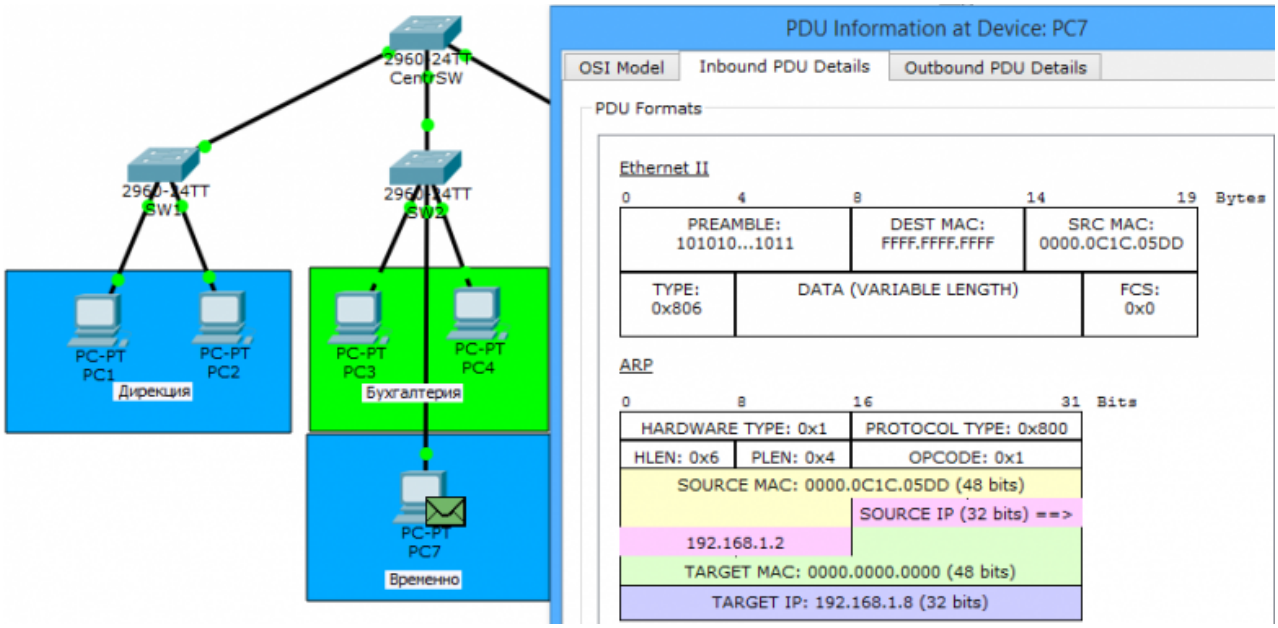




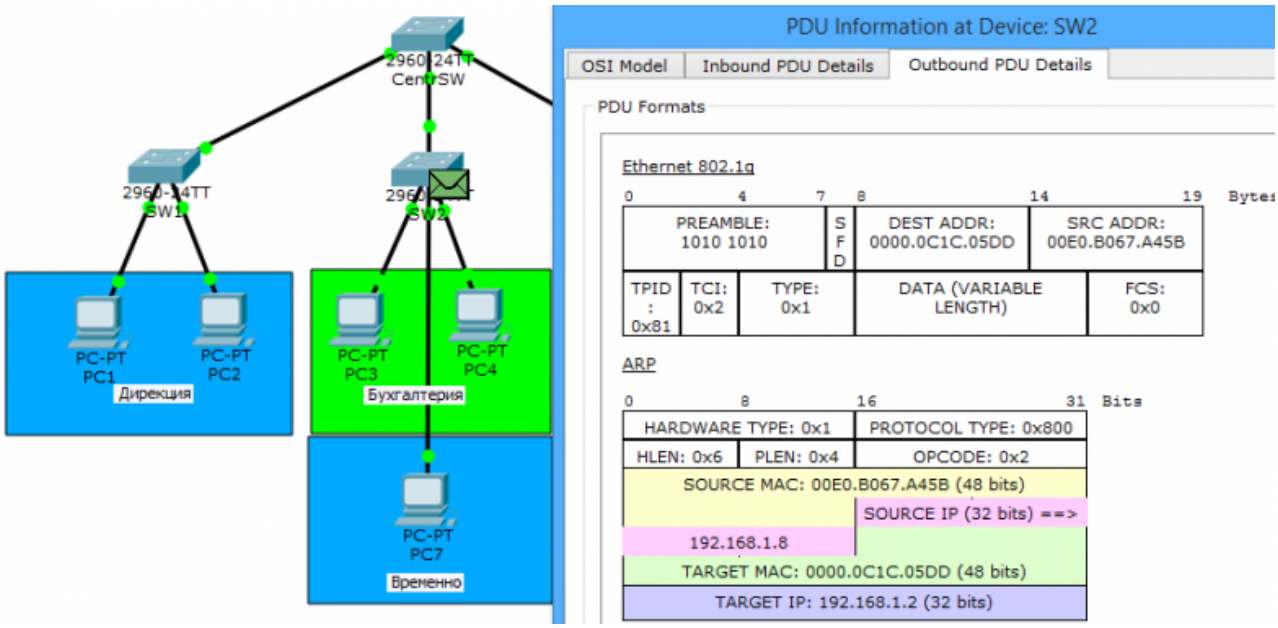
И вот он приходит на SW2. Открываем и видим, что он еще тегированный. Но следующим узлом стоит компьютер и тег надо снимать. Нажимаем на «Outbound PDU Details», чтобы посмотреть в каком виде кадр вылетит из коммутатора.



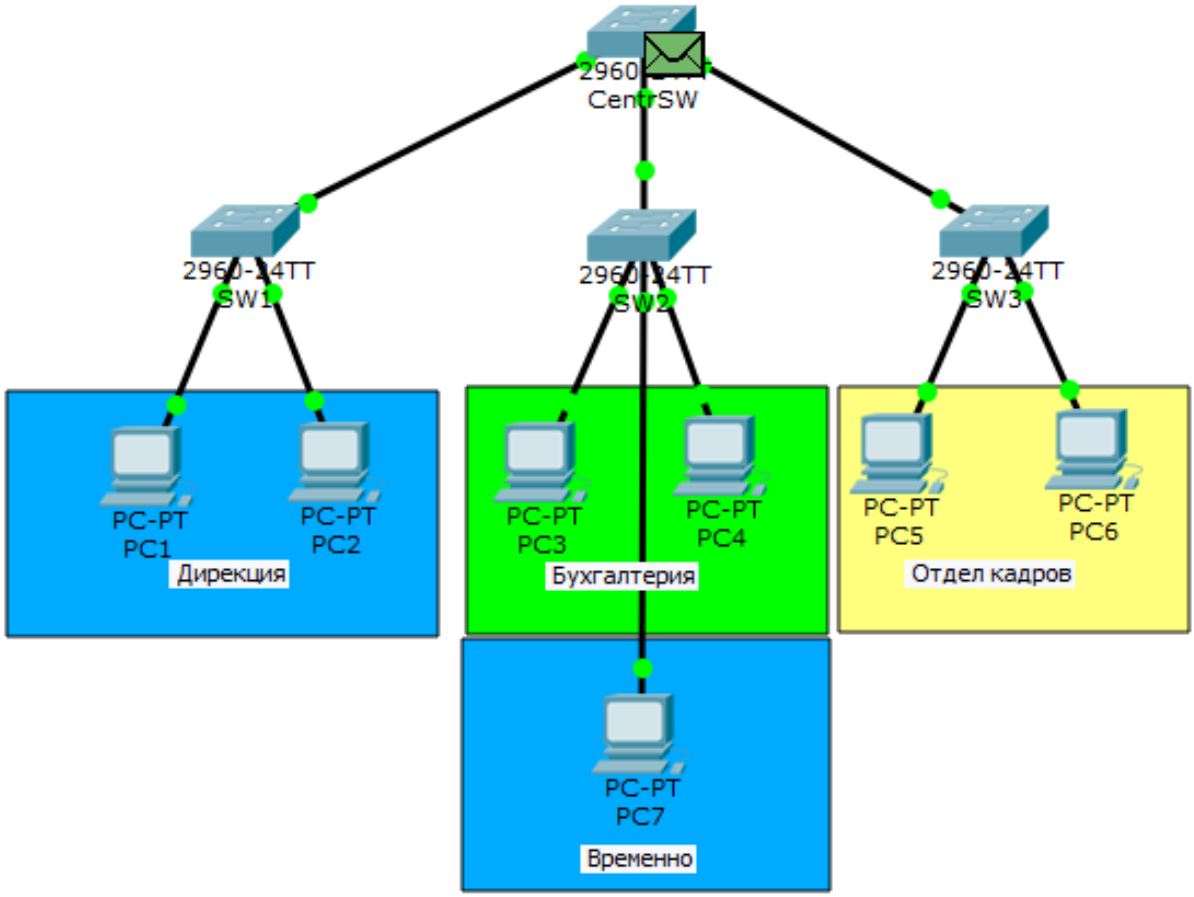
И действительно. Коммутатор отправит кадр в «чистом» виде, то есть без тегов.

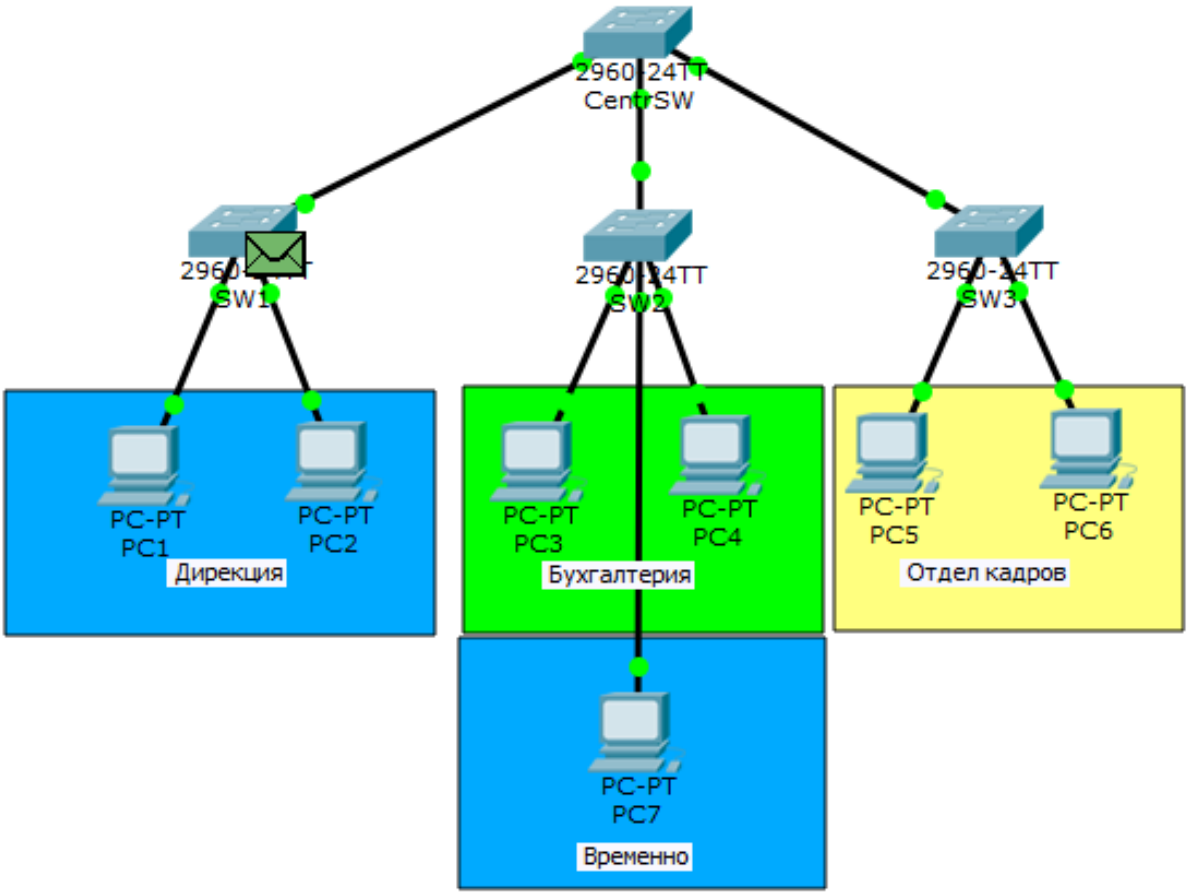


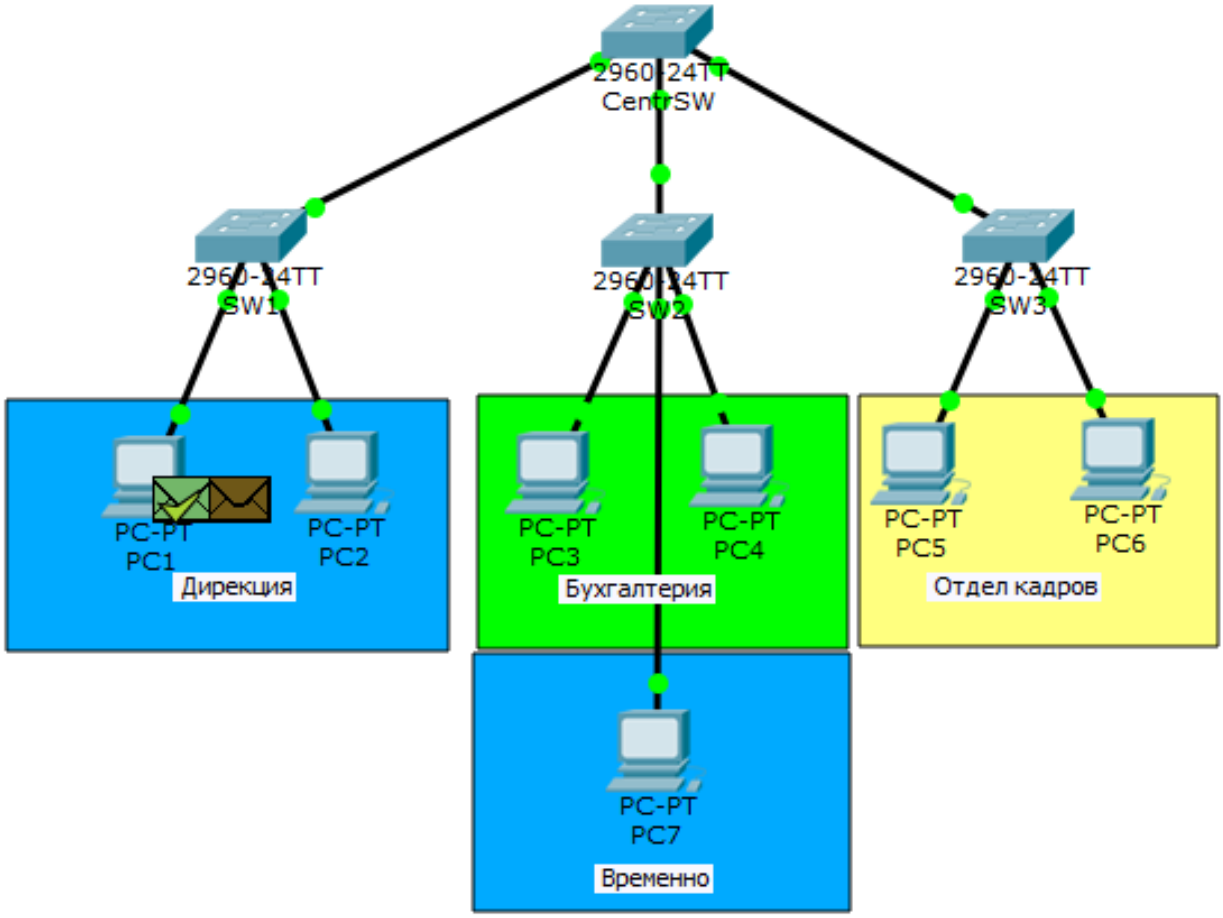
Доходит ARP до PC7. Открываем его и убеждаемся, что кадр не тегированный PC7 узнал себя и отправляет ответ.



Открываем кадр на коммутаторе и видим, что на отправку он уйдет тегированным. Дальше кадр будет путешествовать тем же путем, что и пришел.

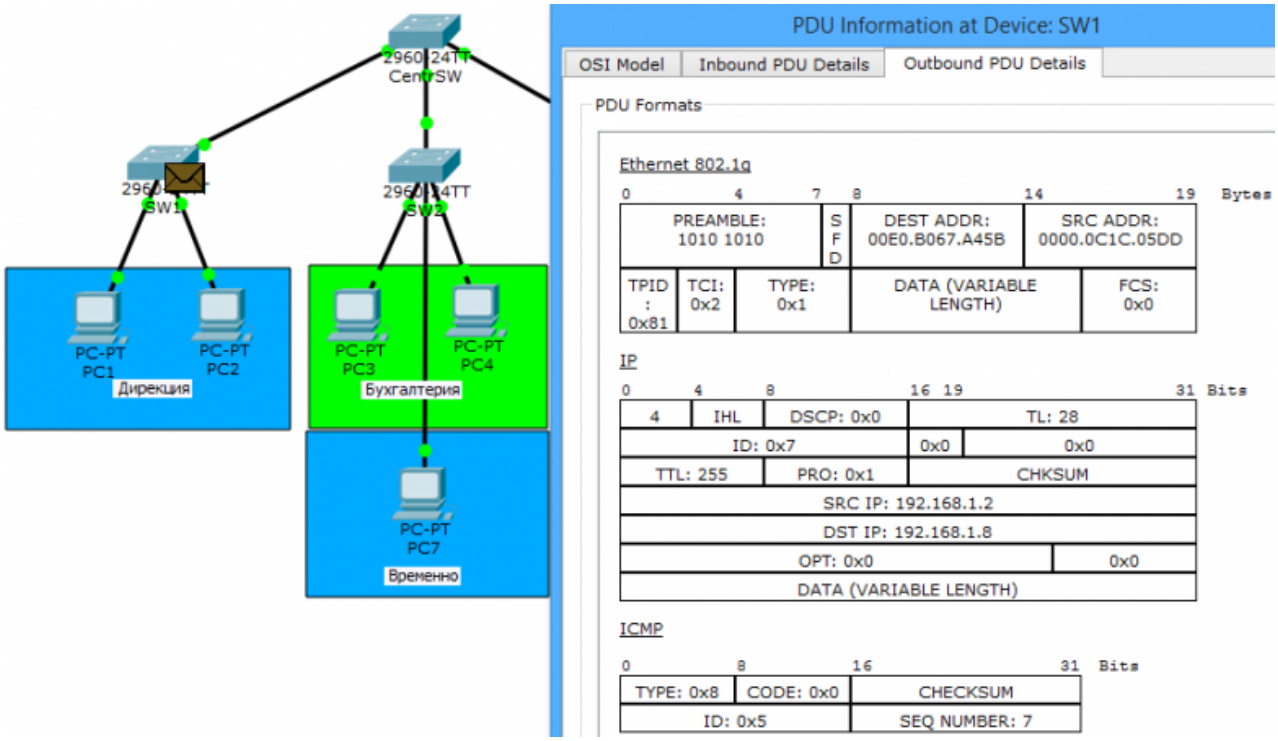




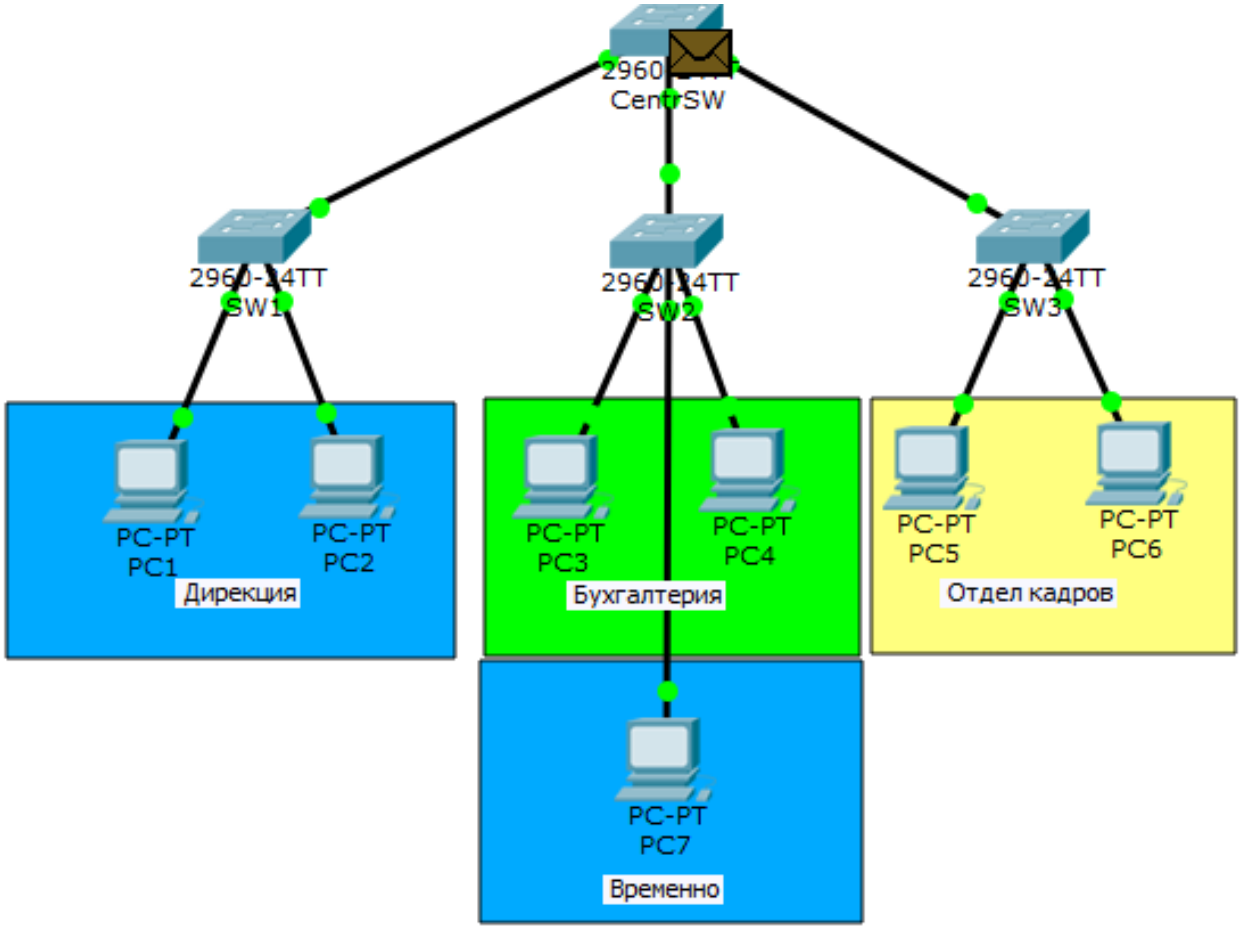


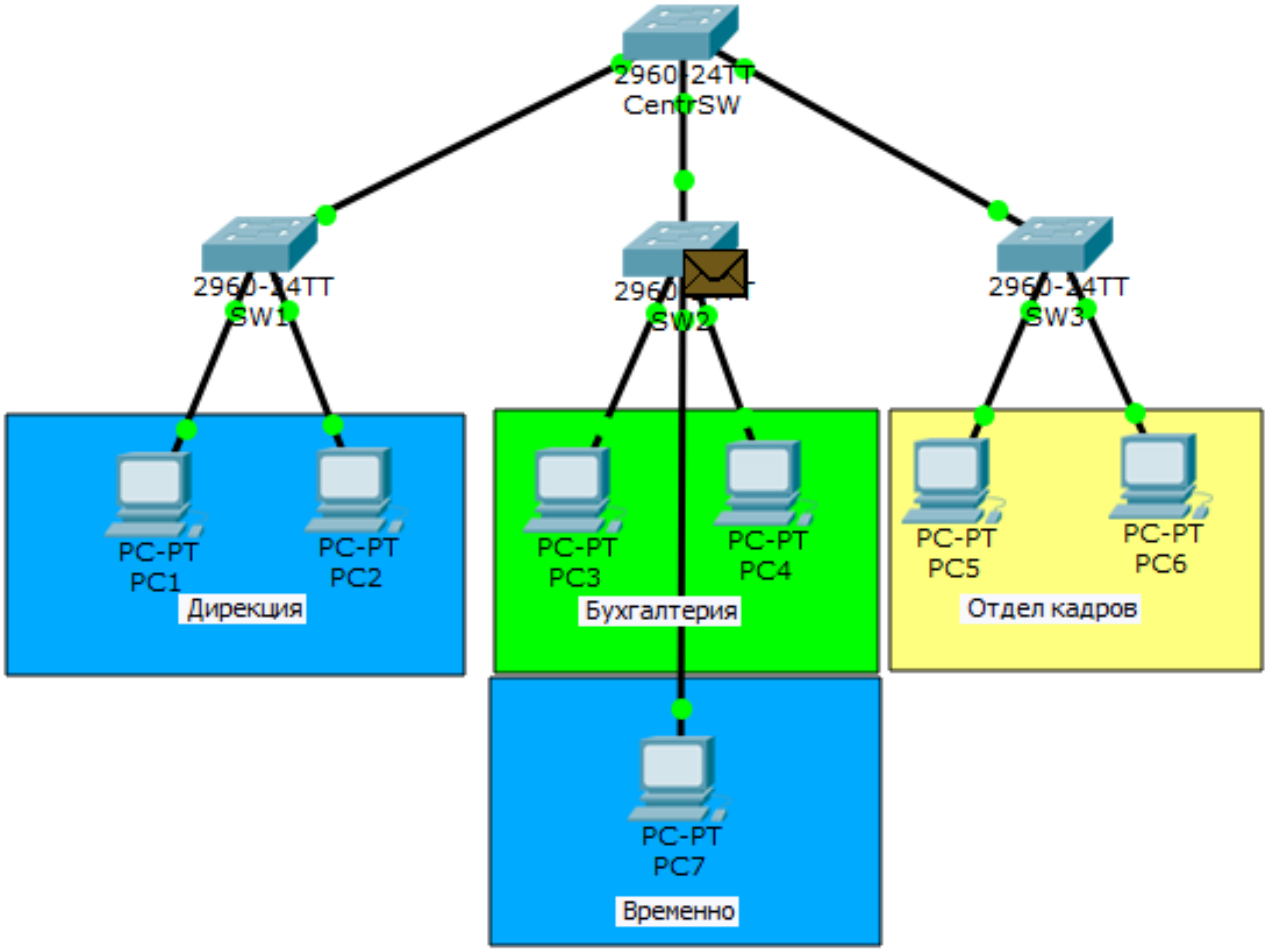
ARP доходит до PC1, о чем свидетельствует галочка на конверте. Теперь ему

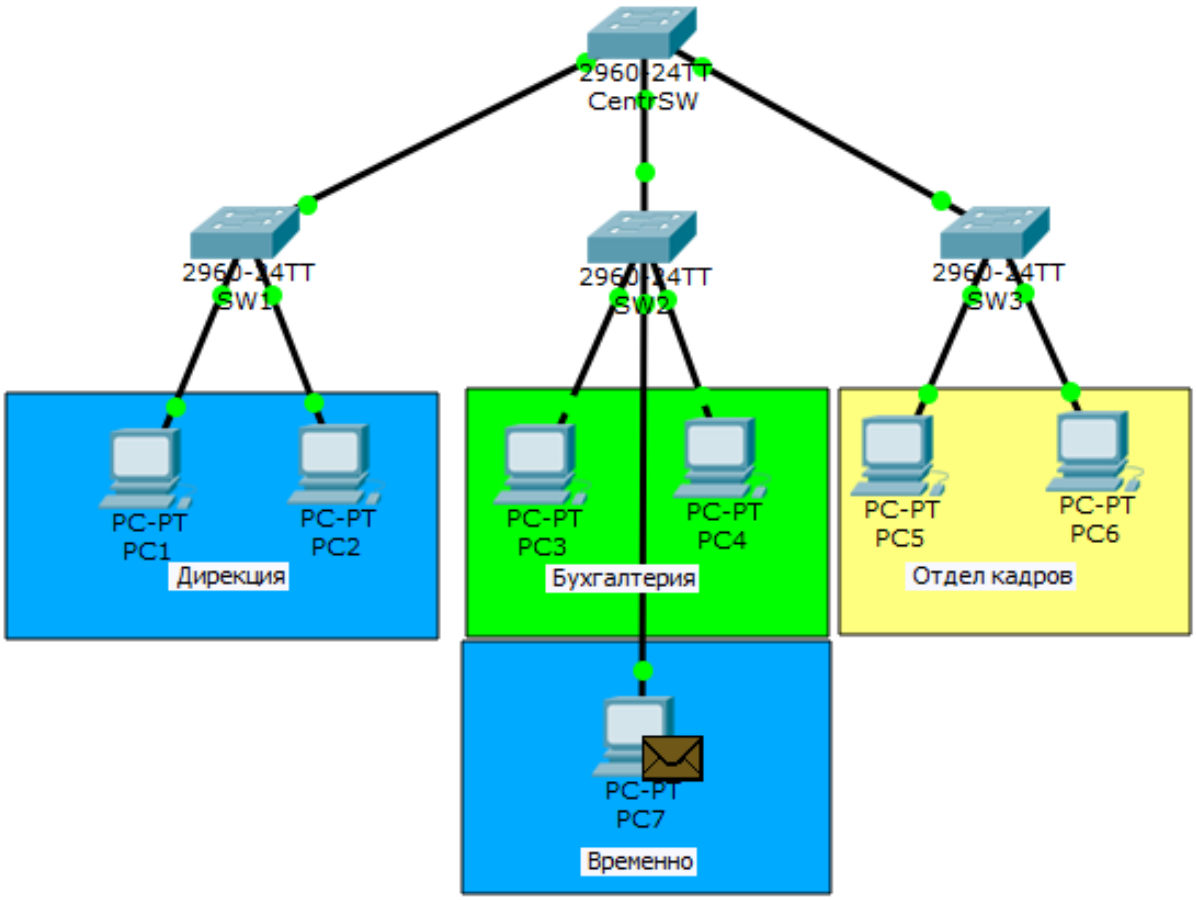
известен MAC-адрес и он пускает в ход ICMP.



Открываем пакет на коммутаторе и наблюдаем такую же картину. На канальном уровне кадр тегируется коммутатором. Так будет с каждым сообщением.




2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
PC-PT
PC5
PC-PT
PC6
Отдел кадров
PC-PT
PC7
Временно



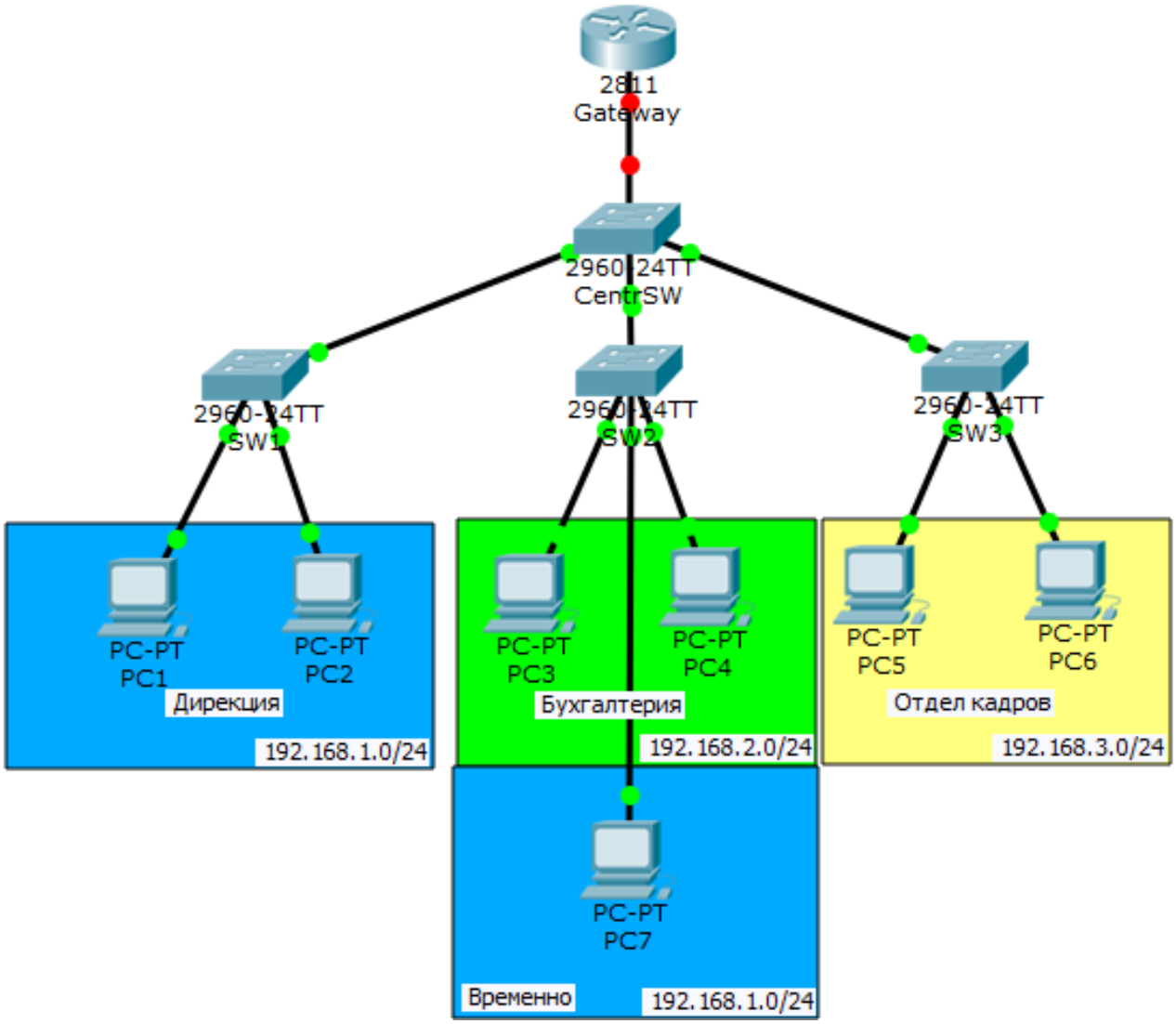
Видим, что пакет успешно доходит до PC7. Обратный путь я показывать не буду, так как он аналогичен. Если кому интересно, можно весь путь увидеть на анимации под спойлером ниже. А если охота самому поковырять эту топологию, прикладываю ссылку на лабораторку.

Логика работы VLAN

Вот в принципе самое популярное применение VLAN-ов. Независимо от физического расположения, можно логически объединять узлы в группы, там самым изолируя их от других. Очень удобно, когда сотрудники физически работают в разных местах, но должны быть объединены. И конечно с точки зрения безопасности VLAN не заменимы. Главное, чтобы к сетевым устройствам имели доступ ограниченный круг лиц, но это уже отдельная тема.
Добились ограничения на канальном уровне. Трафик теперь не гуляет где попало, а ходит строго по назначению. Но теперь встает вопрос в том, что отделам между собой нужно общаться. А так как они в разных канальных средах, то в дело вступает маршрутизация. Но перед началом, приведем топологию в порядок. Самое первое к чему приложим руку — это адресация узлов. Повторюсь, что каждый отдел должен находиться в своей подсети. Итого получаем:

- Дирекция — 192.168.1.0/24
- Бухгалтерия — 192.168.2.0/24

- Отдел кадров — 192.168.3.0/24



Раз подсети определены, то сразу адресуем узлы.

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

Теперь про изменения в топологии. Видим, что добавился маршрутизатор. Он как раз и будет перекидывать трафик с одного VLAN на другой (иными словами маршрутизировать). Изначально соединения между ним и коммутатором нет, так как интерфейсы выключены.
У узлов добавился такой параметр, как адрес шлюза. Этот адрес они используют, когда надо отправить сообщение узлу, находящемуся в другой подсети. Соответственно у каждой подсети свой шлюз.

Осталось настроить маршрутизатор, и я открываю его CLI. По традиции дам осмысленное имя.

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

Далее переходим к настройке интерфейсов.

```
Gateway(config)#interface fastEthernet 0/0 - переходим к требуемому интерфейсу.
Gateway(config-if)#no shutdown - включаем его.
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
```

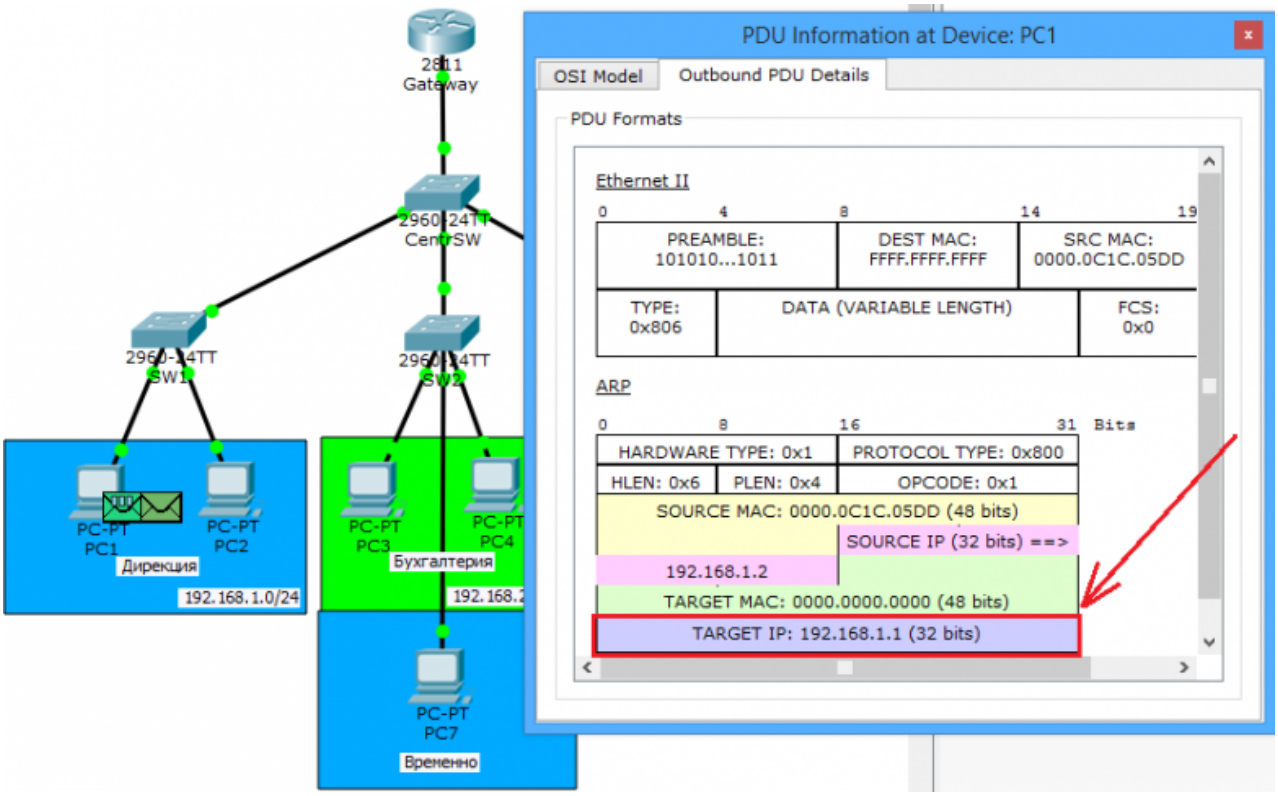
Теперь внимание! Мы включили интерфейс, но не повесили на него IP-адрес. Дело в том, что от физического интерфейса (fastethernet 0/0) нужен только линк или канал. Роль шлюзов будут выполнять виртуальные интерфейсы или сабинтерфейсы (англ. subinterface). На данный момент 3 типа VLAN. Значит и сабинтерфейсов будет 3. Приступаем к настройке.

```
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
```

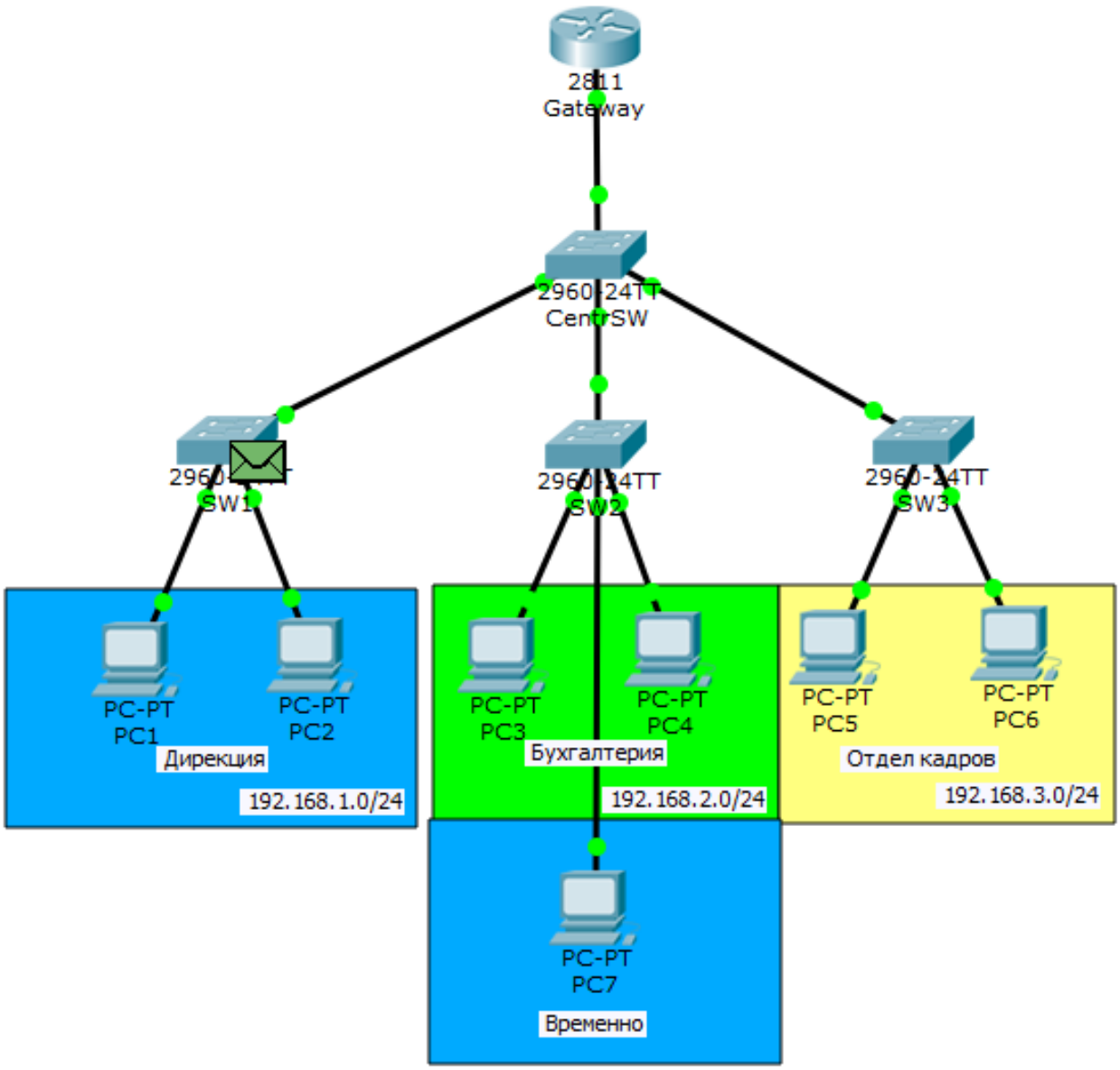
Маршрутизатор настроен. Переходим к центральному коммутатору и настроим на нем транковый порт, чтобы он пропускал тегированные кадры на маршрутизатор.

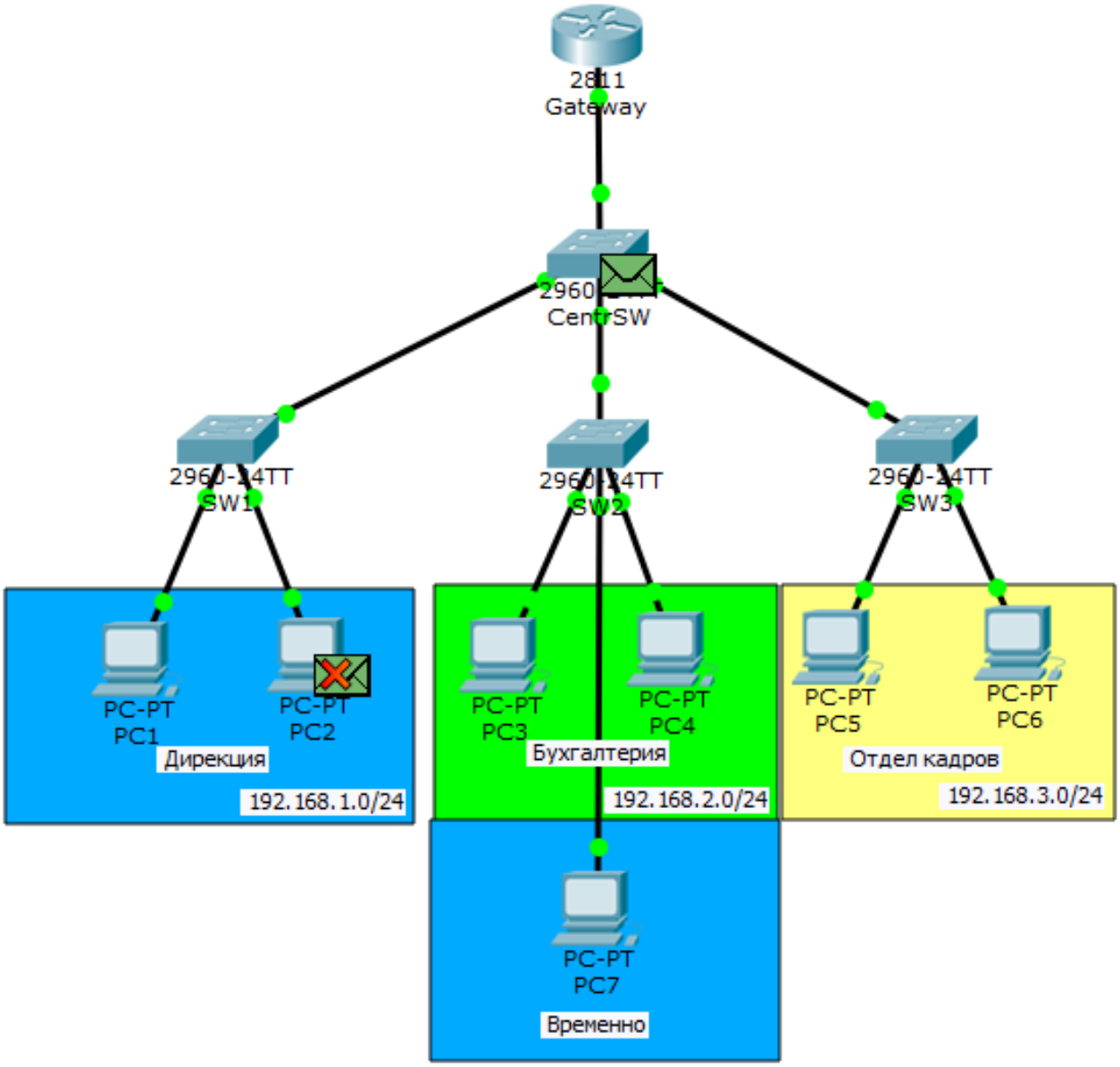
```
CentrSW(config)#interface fastEthernet 0/24
CentrSW(config-if)#switchport mode trunk
CentrSW(config-if)#switchport trunk allowed vlan 2,3,4
```

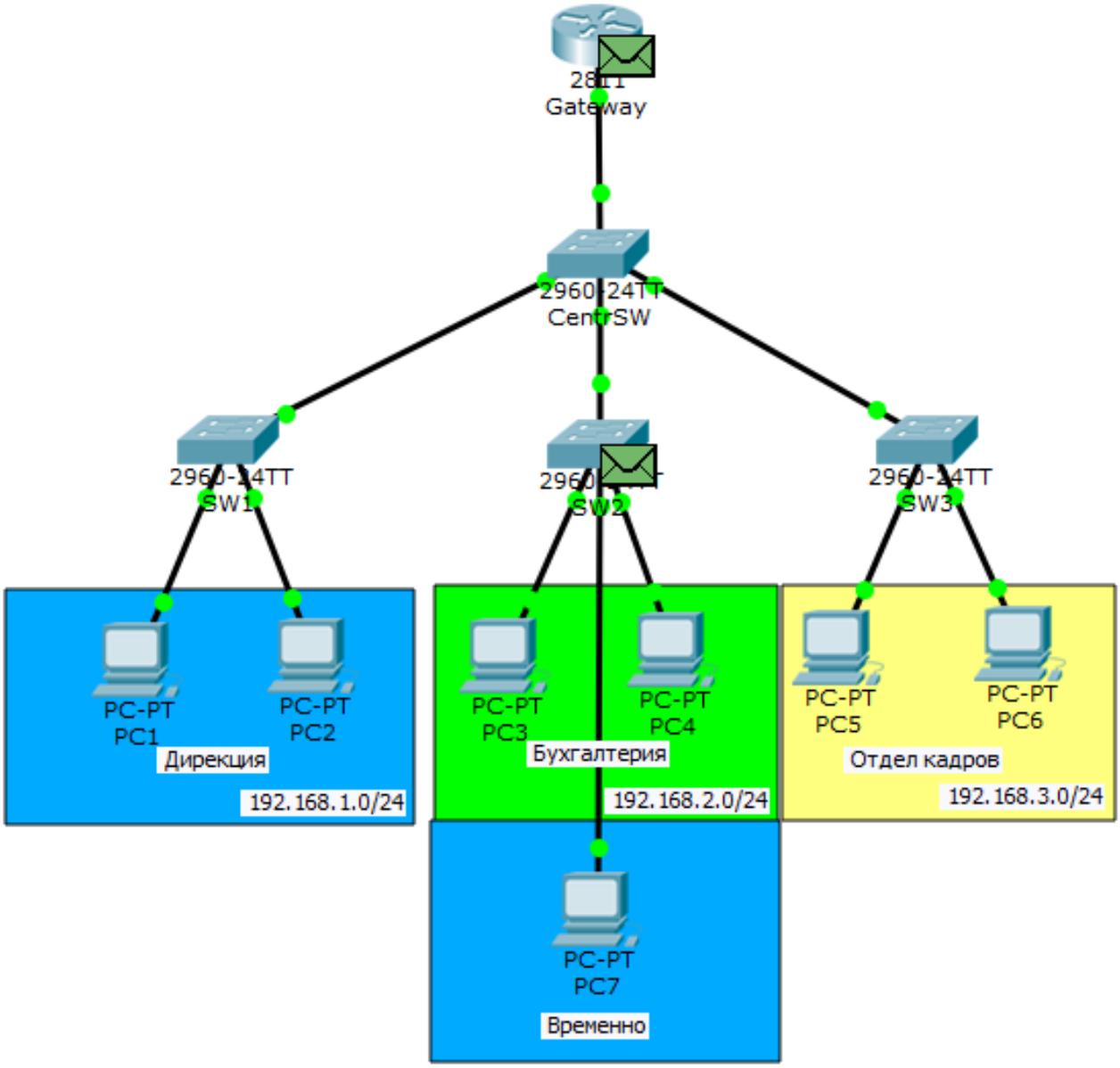
Конфигурация закончена и переходим к практике. Отправляю ping с PC1 на PC6 (то есть на 192.168.3.3).



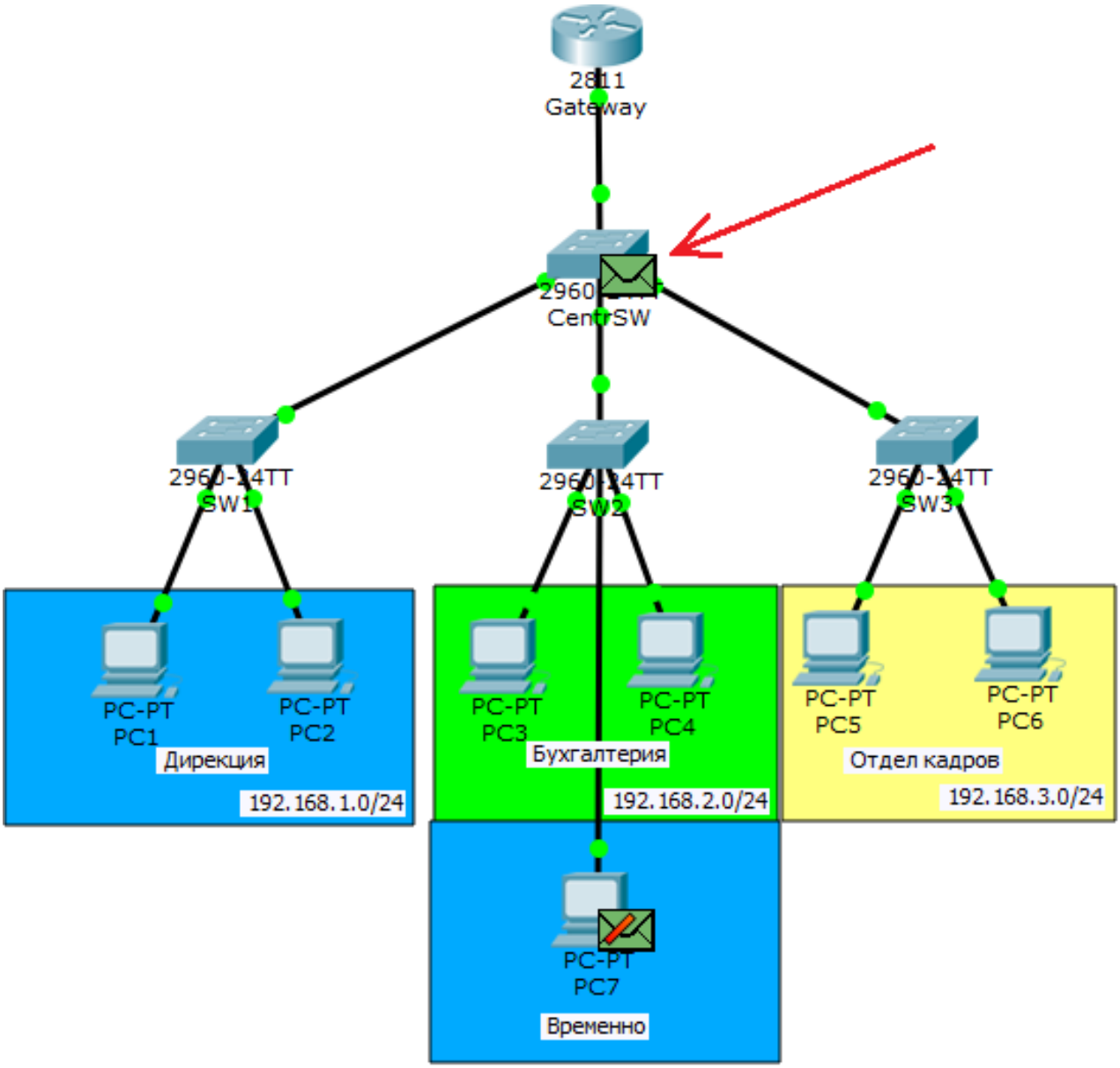
PC1 понятия не имеет, кто такой PC6 или 192.168.3.3, но знает, что они находятся в разных подсетях (как он это понимает описано в предыдущей статье). Поэтому он отправит сообщение через основной шлюз, адрес которого указан в его настройках. И хоть PC1 знает IP-адрес основного шлюза, для полного счастья не хватает MAC-адреса. И он пускает в ход 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

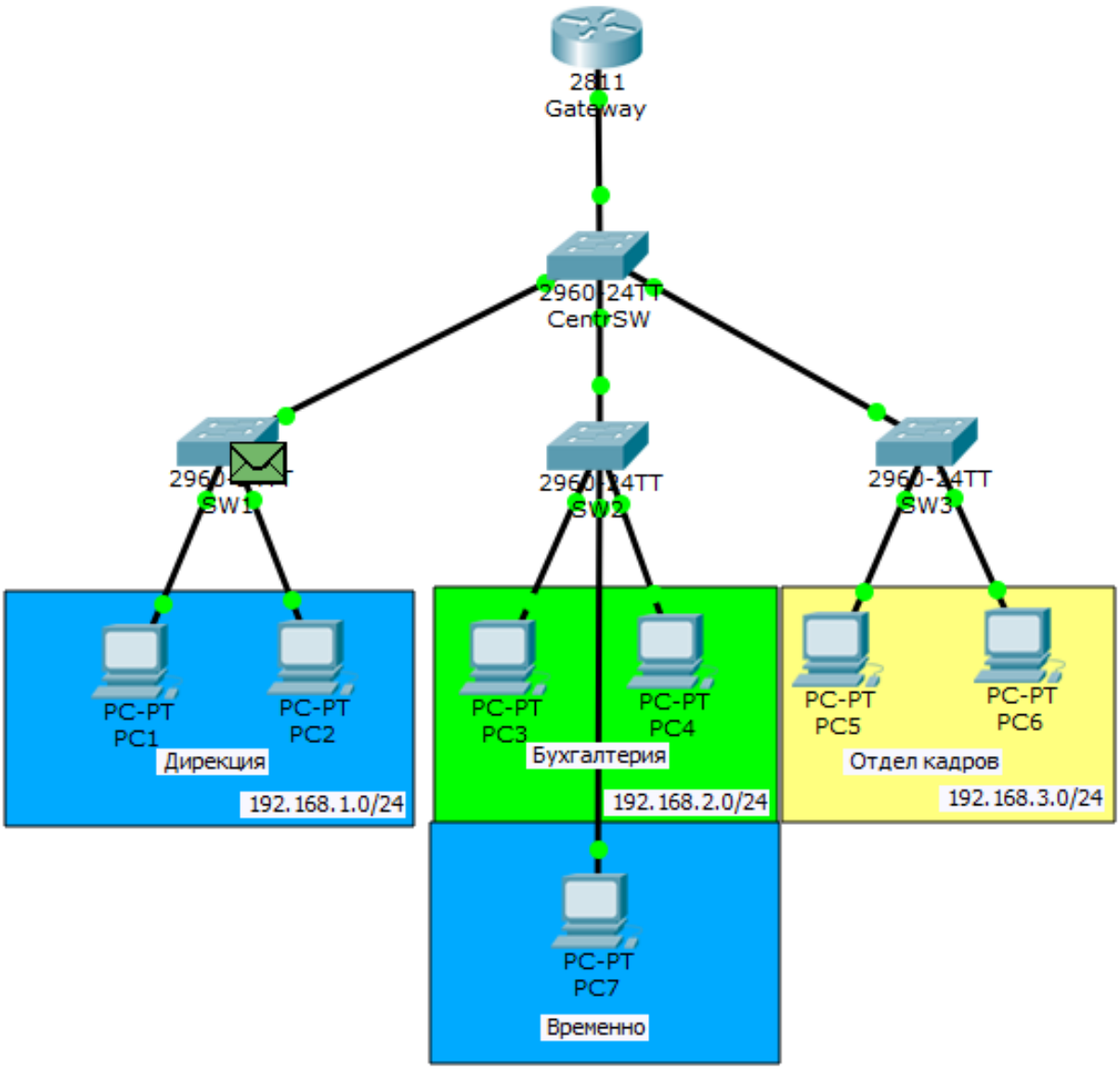

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

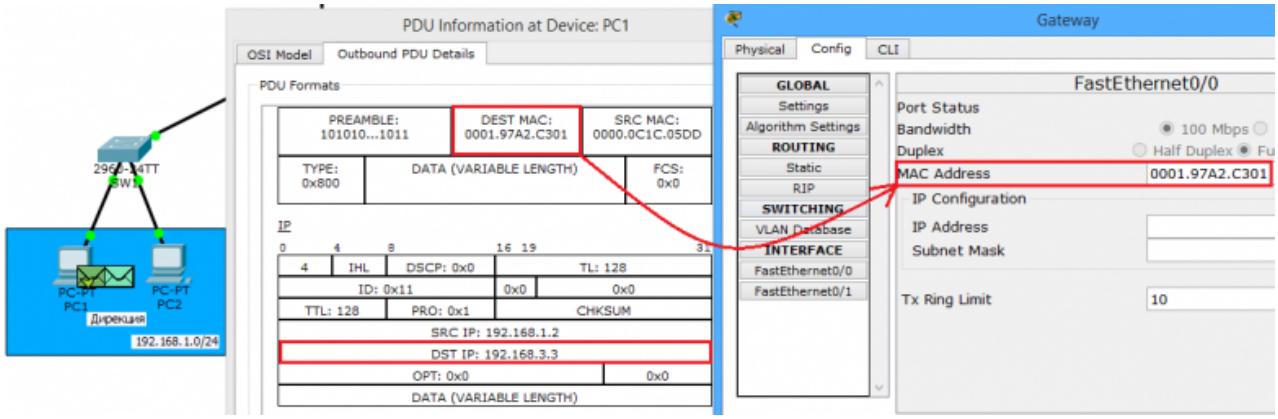


Обратите внимание. Как только кадр прибывает на CentrSW, коммутатор не рассылает его кому попало. Он рассылает только на те порты, где разрешен пропуск 2-го VLAN. То есть на маршрутизатор и на SW2 (там есть пользователь, сидящий во 2-ом VLAN).

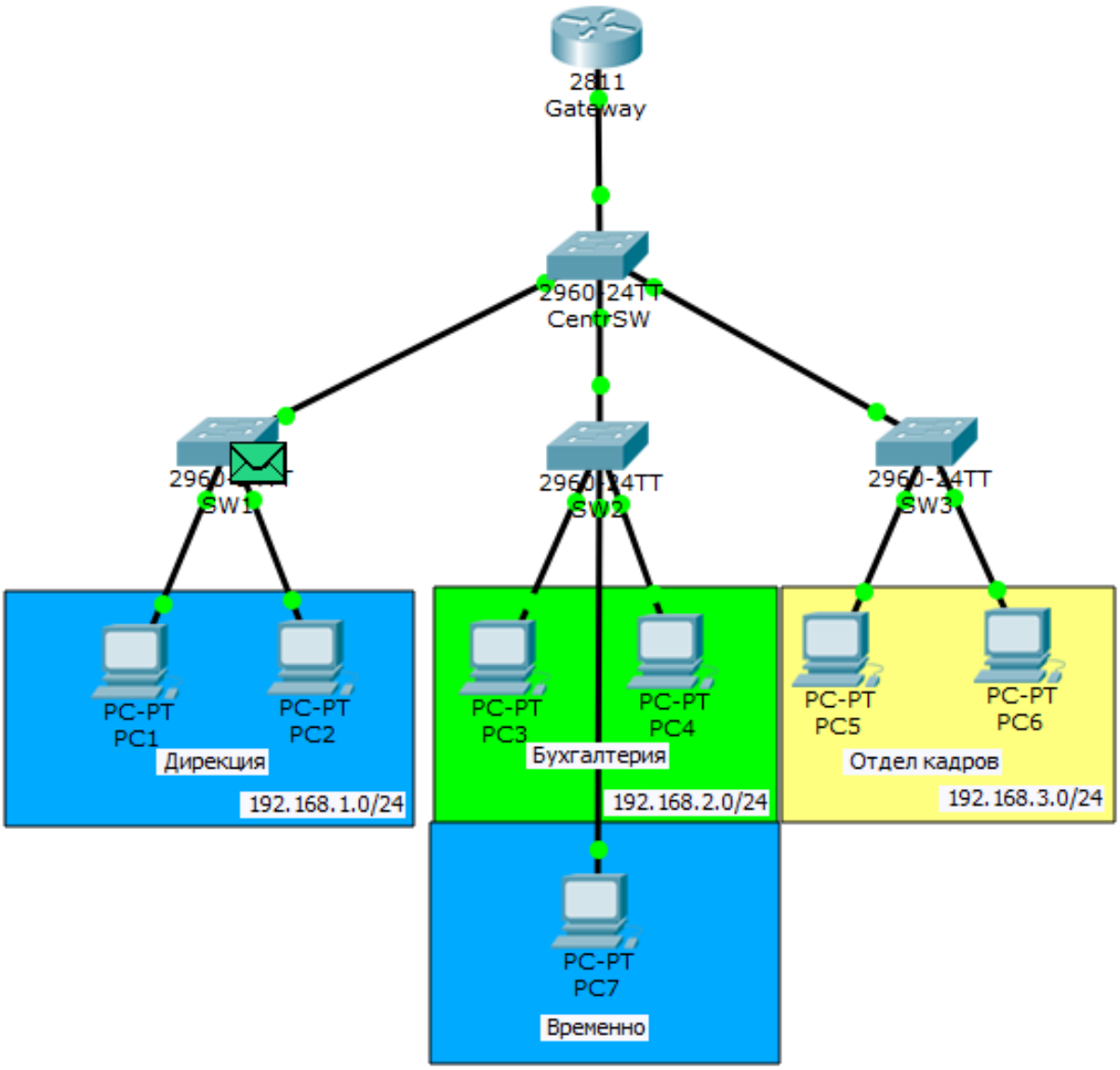


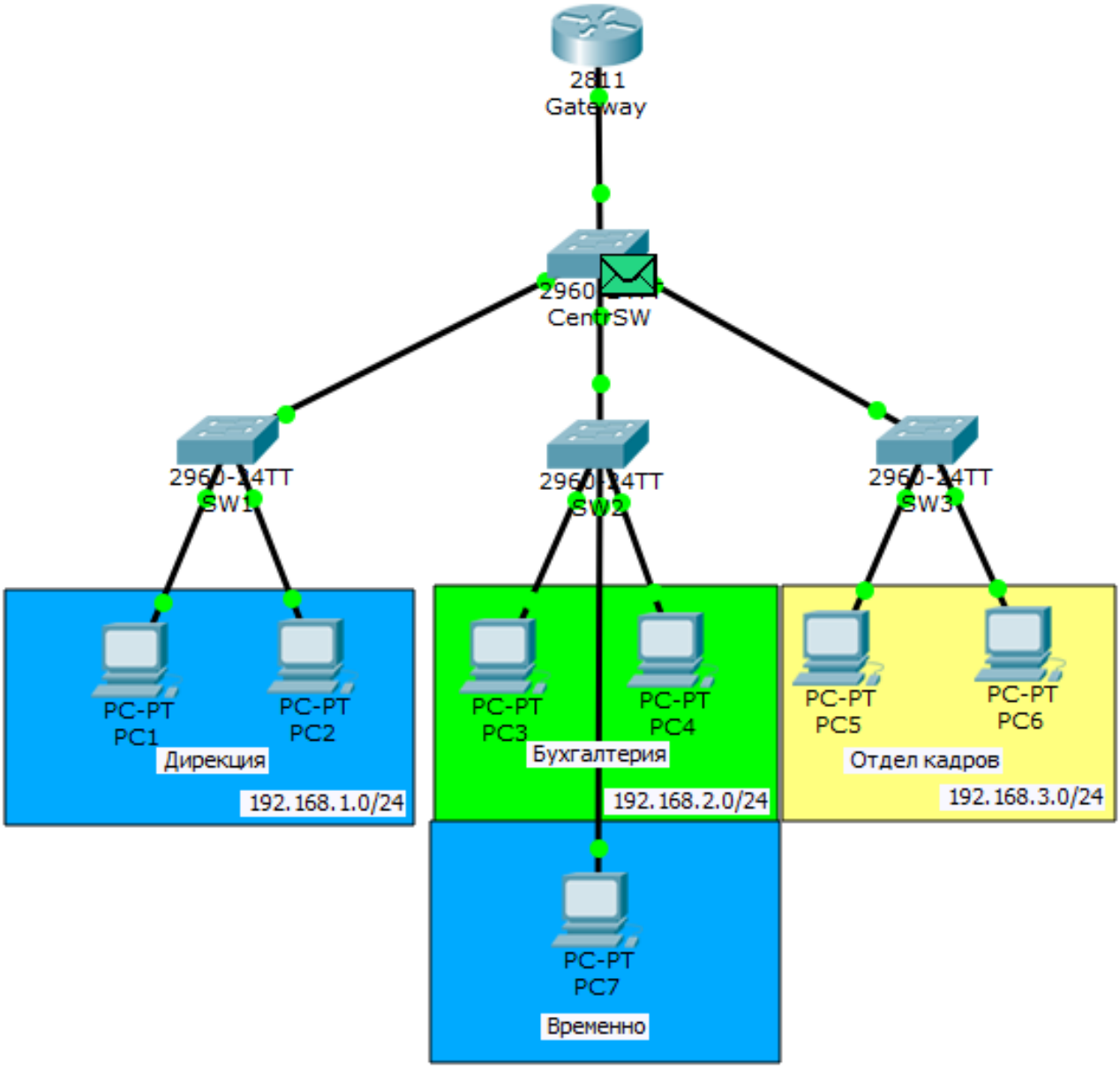
Маршрутизатор узнает себя и отправляет ответ (показан стрелочкой). И обратите внимание на нижний кадр. Когда SW2 получил ARP от центрального коммутатора, он аналогично не стал рассылать его на все компьютеры, а отправил только PC7, который сидит во 2-ом VLAN. Но PC7 его отбрасывает, так как он не для него. Смотрим дальше.

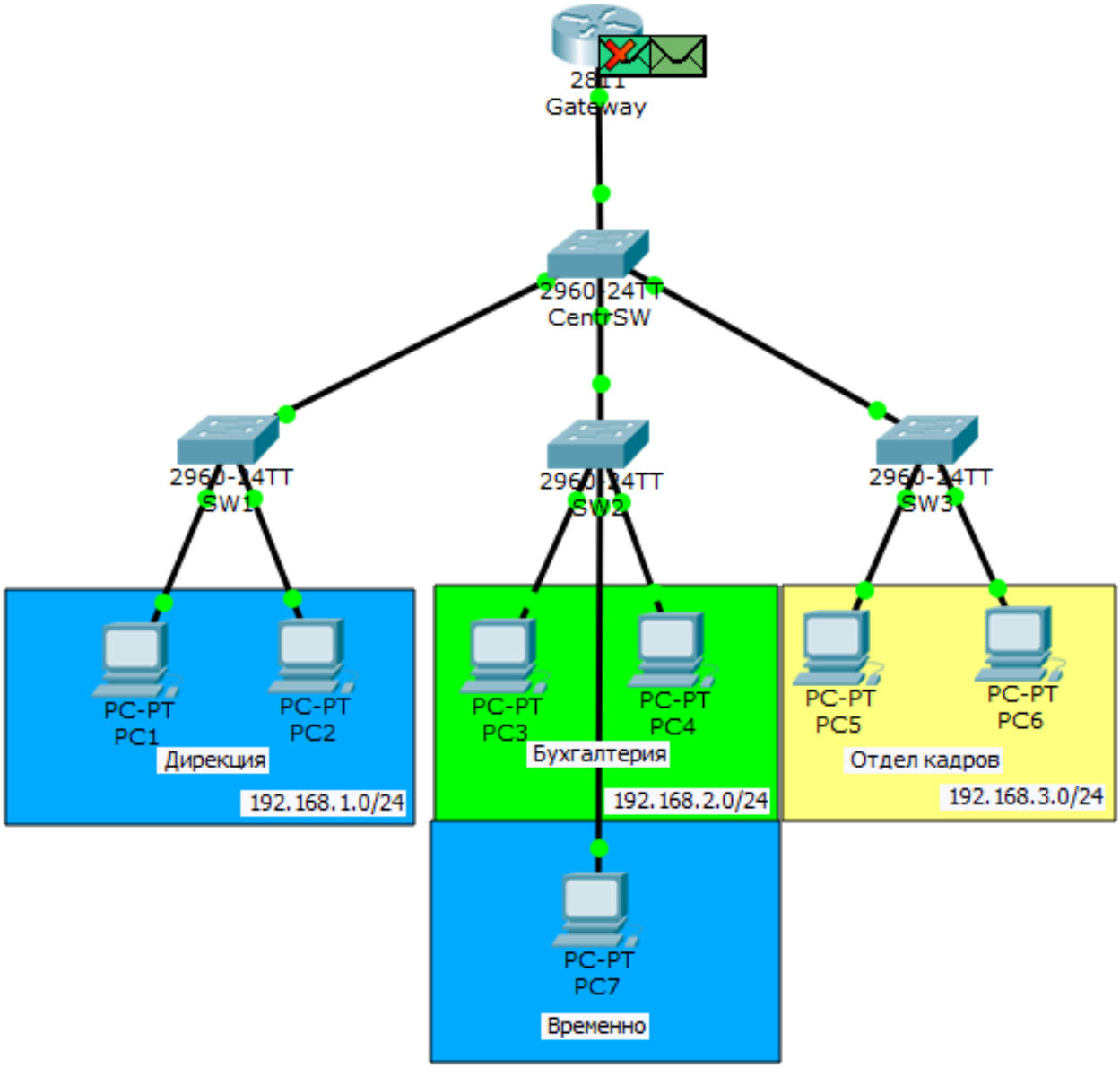




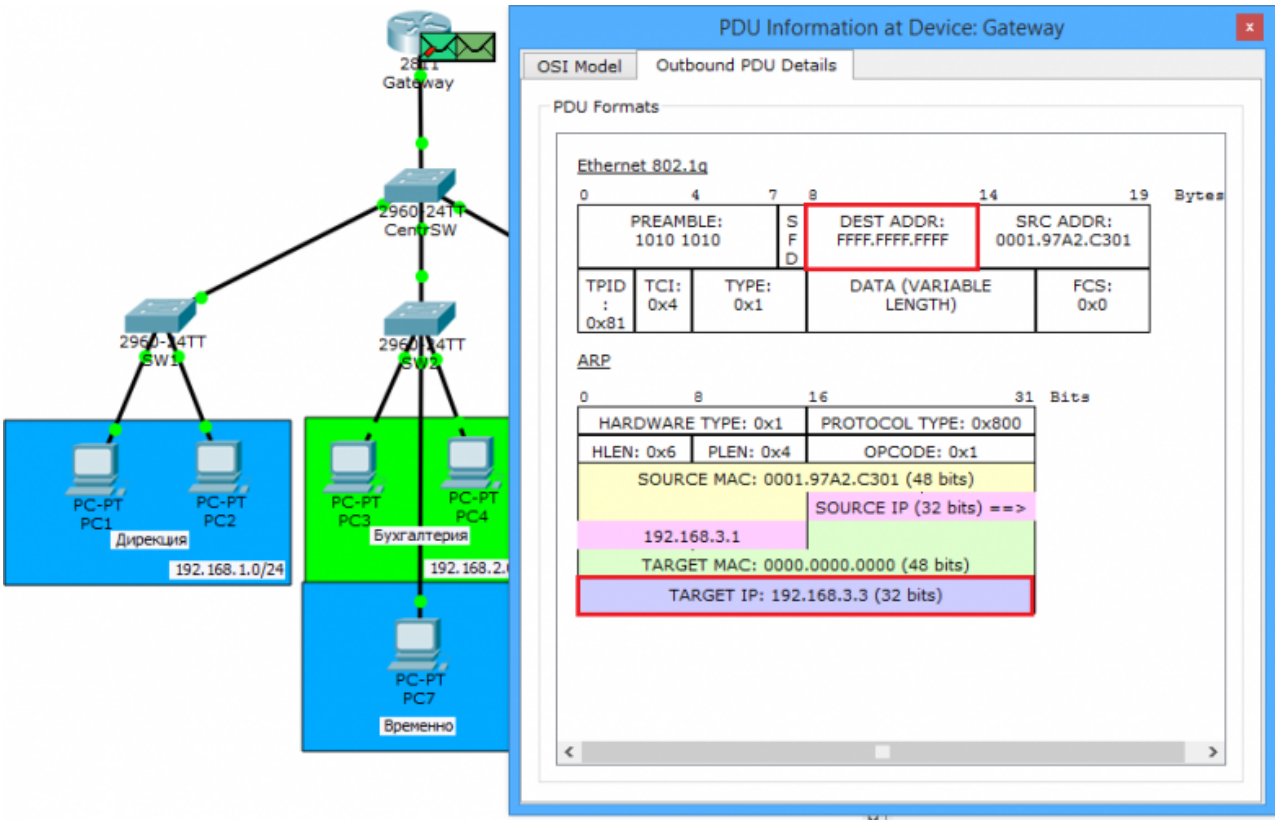
ARP дошел до PC1. Теперь ему все известно и можно отправлять ICMP. Еще раз обращу внимание на то, что в качестве MAC-адреса назначения (канальный уровень), будет адрес маршрутизатора, а в качестве IP-адреса назначения (сетевой уровень), адрес PC6.

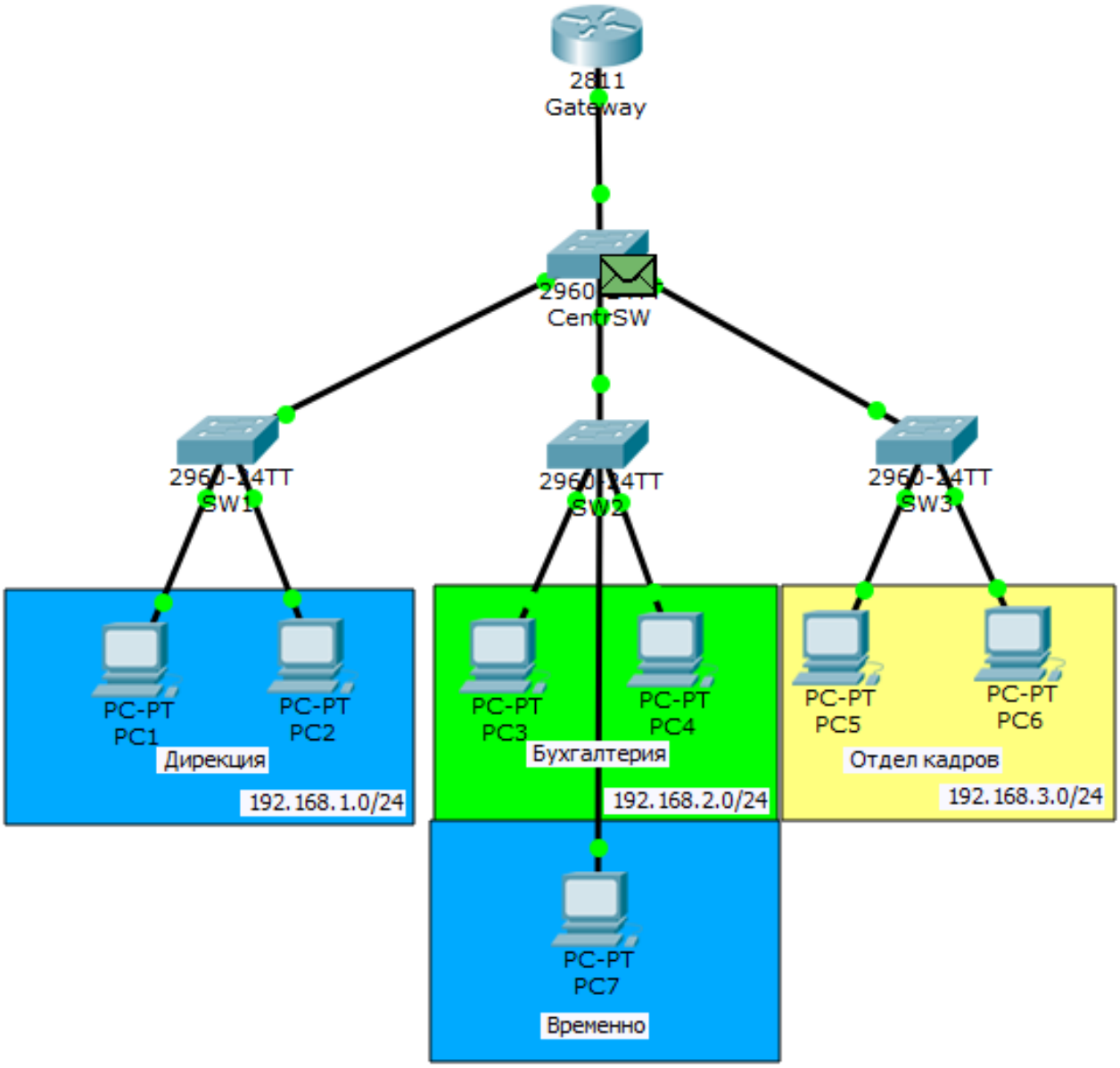

2811
Gateway
2960-24TT
CentrSW
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

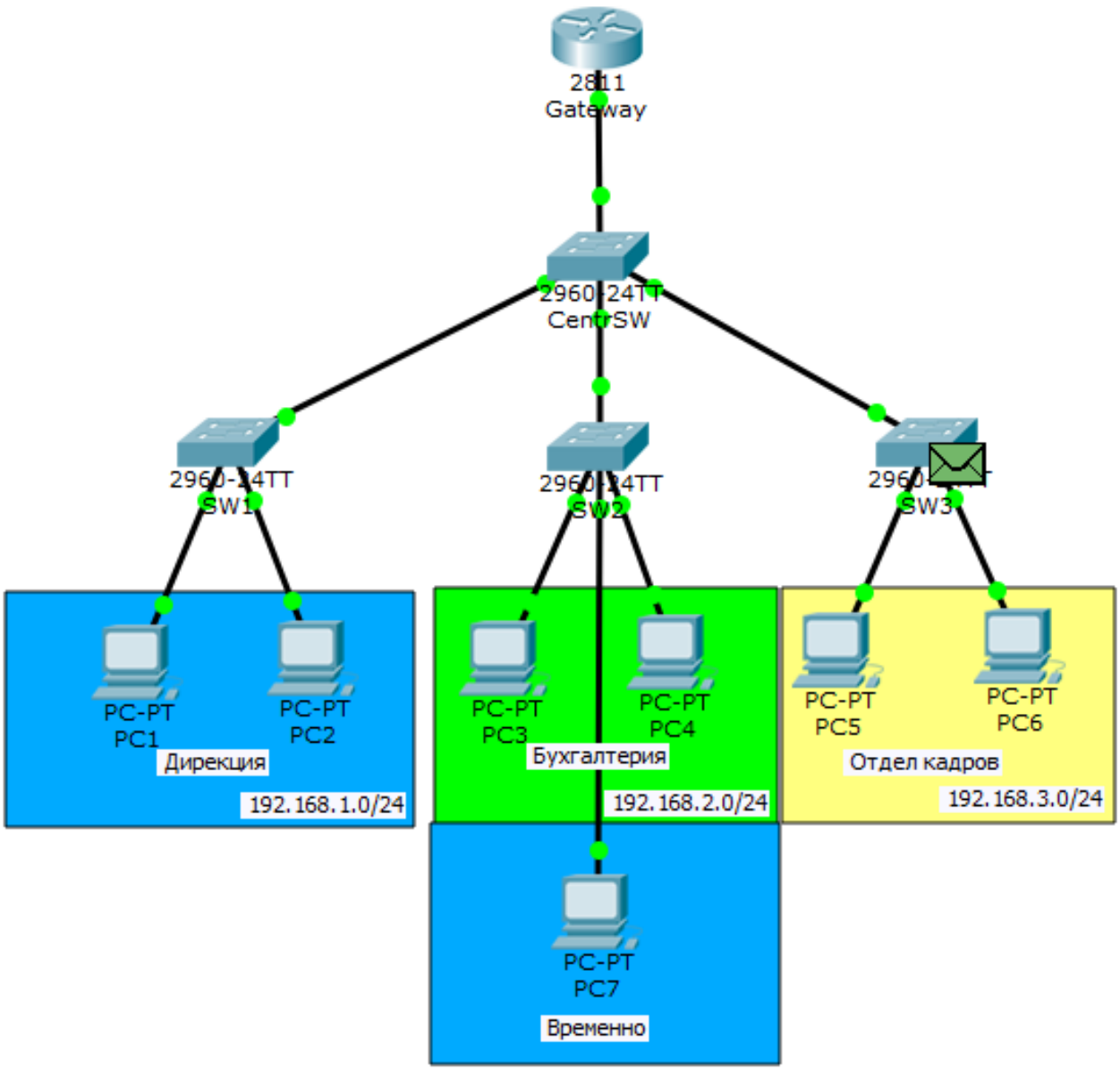

2811
Gateway
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

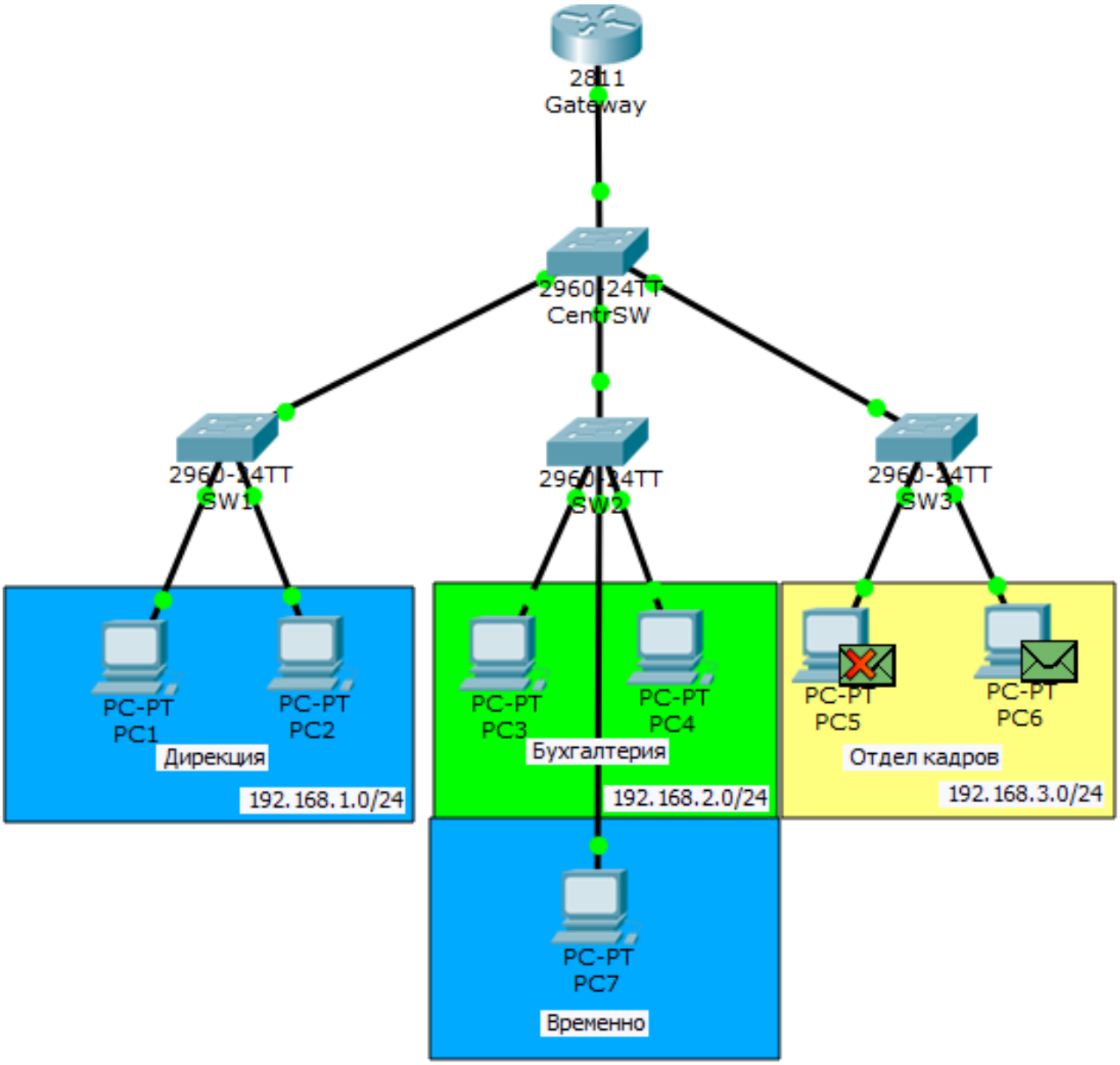


Доходит ICMP до маршрутизатора. Он смотрит в свою таблицу и понимает, что не знает никого под адресом 192.168.3.3. Отбрасывает прибывший ICMP и пускает разведать ARP.

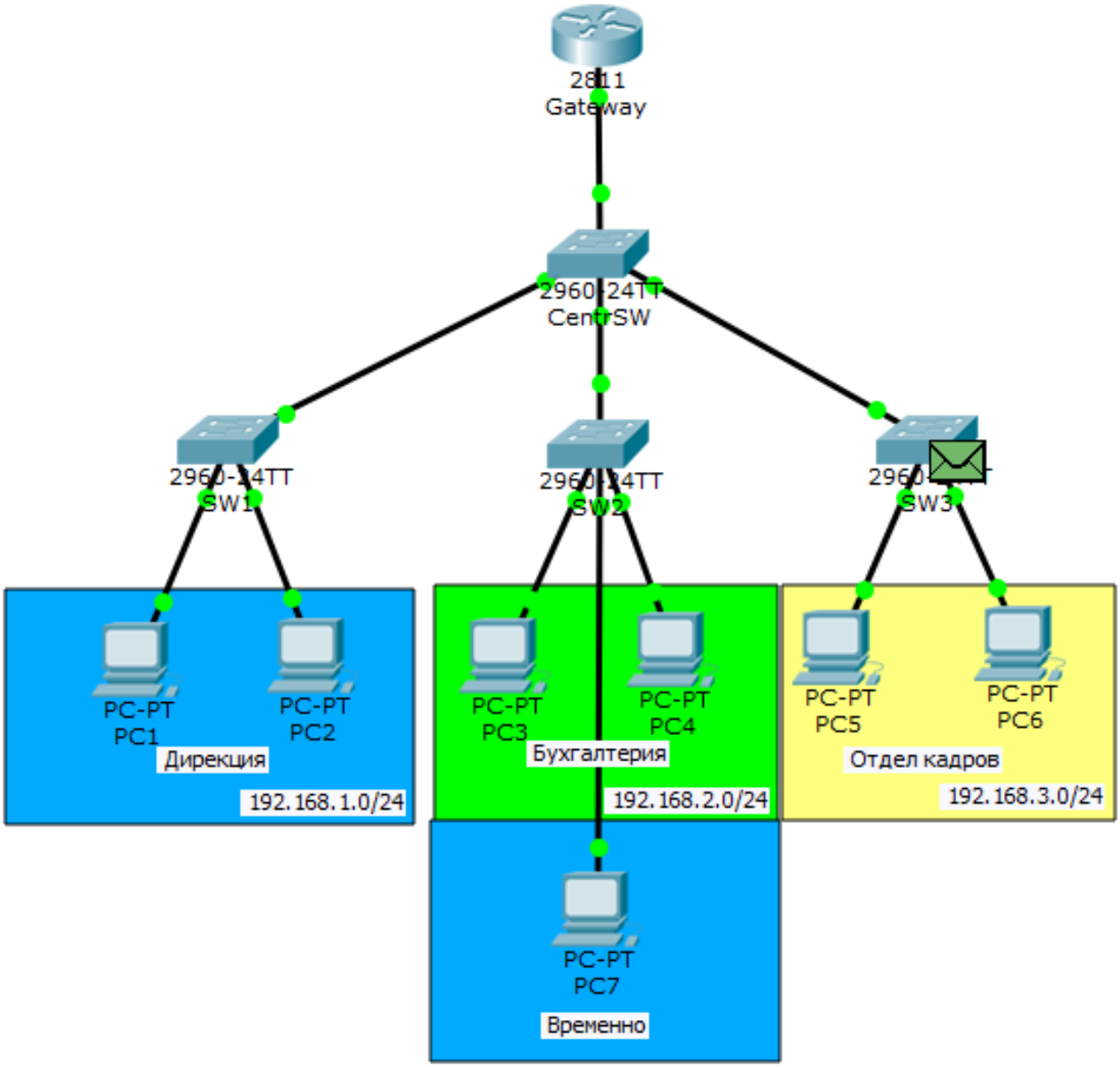

Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
PC-PT
PC7
Временно
PDU Information at Device: Gateway
OSI Model
Outbound PDU Details
PDU Formats
Ethernet 802.1q
0 4 7 8 14 19 Bytes
PREAMBLE: 1010 1010
SFD
DEST ADDR: FFFF.FFFF.FFFF
SRC ADDR: 0001.97A2.C301
TPID : 0x81
TCI: 0x4
TYPE: 0x1
DATA (VARIABLE LENGTH)
FCS: 0x0
ARP
0 8 16 31 Bits
HARDWARE TYPE: 0x1
PROTOCOL TYPE: 0x800
HLEN: 0x6
PLEN: 0x4
OPCODE: 0x1
SOURCE MAC: 0001.97A2.C301 (48 bits)
SOURCE IP (32 bits) ==>
192.168.3.1
TARGET MAC: 0000.0000.0000 (48 bits)
TARGET IP: 192.168.3.3 (32 bits)

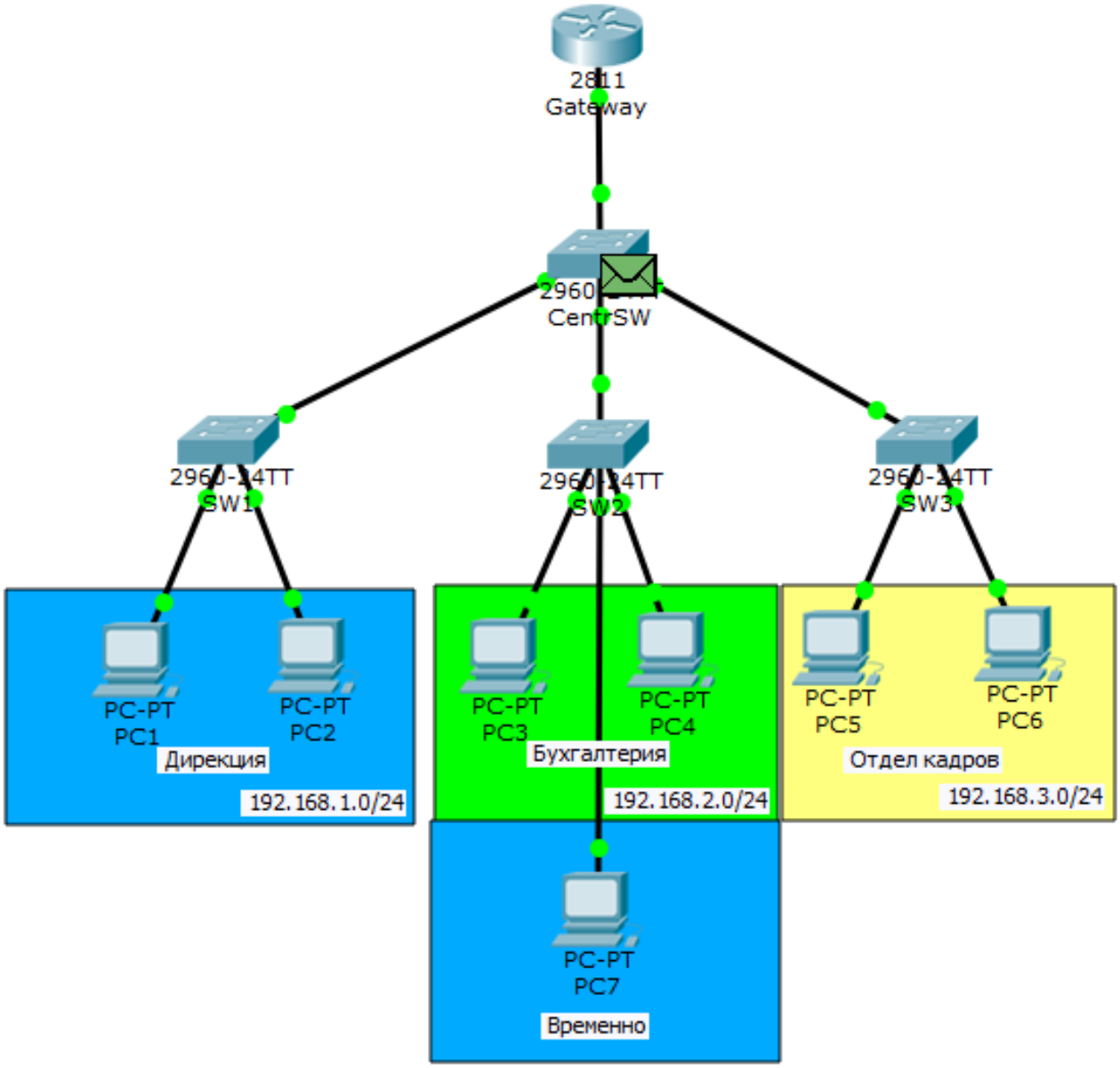

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

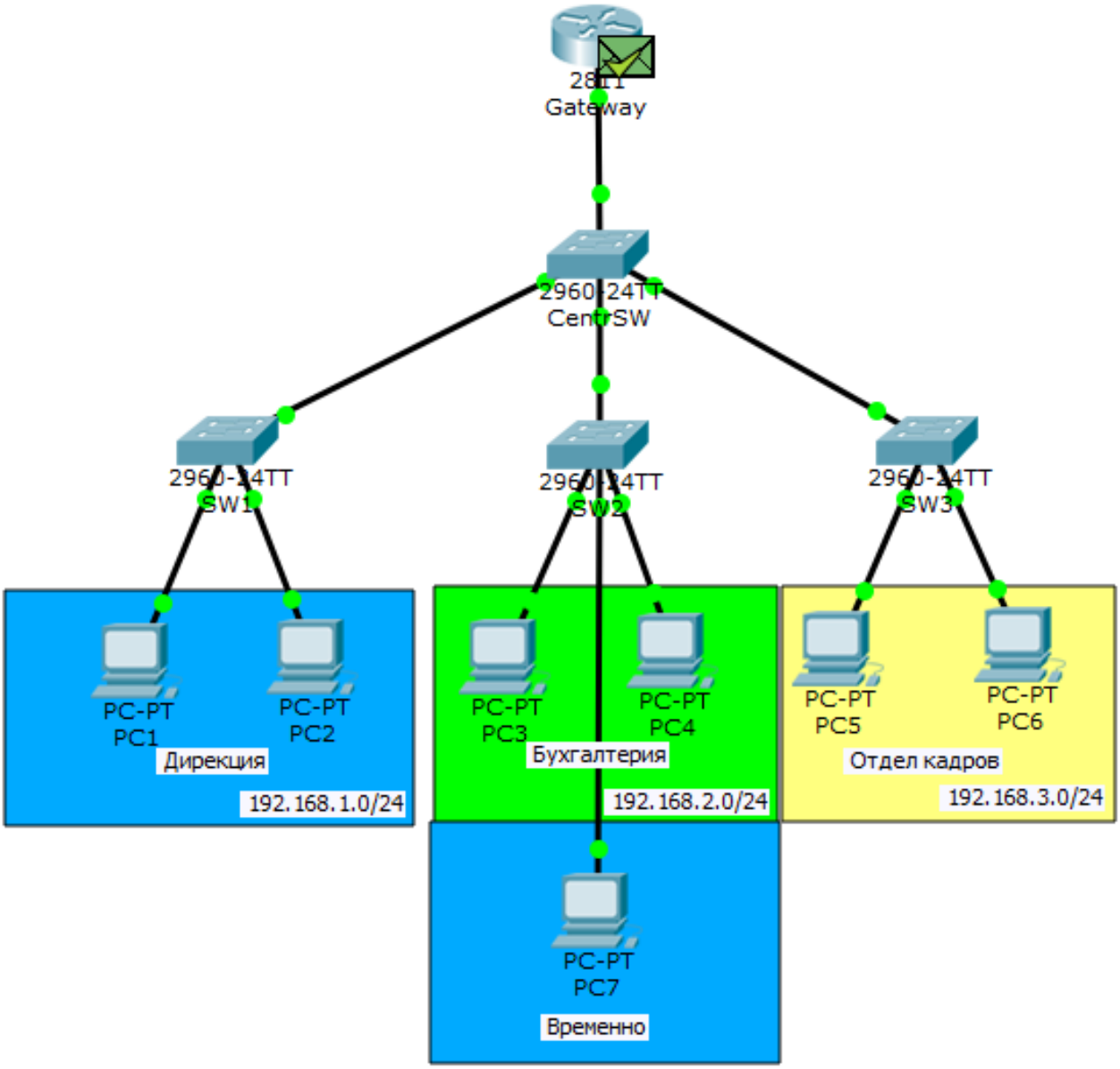

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно



PC6 узнает себя и отправляет ответ.


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

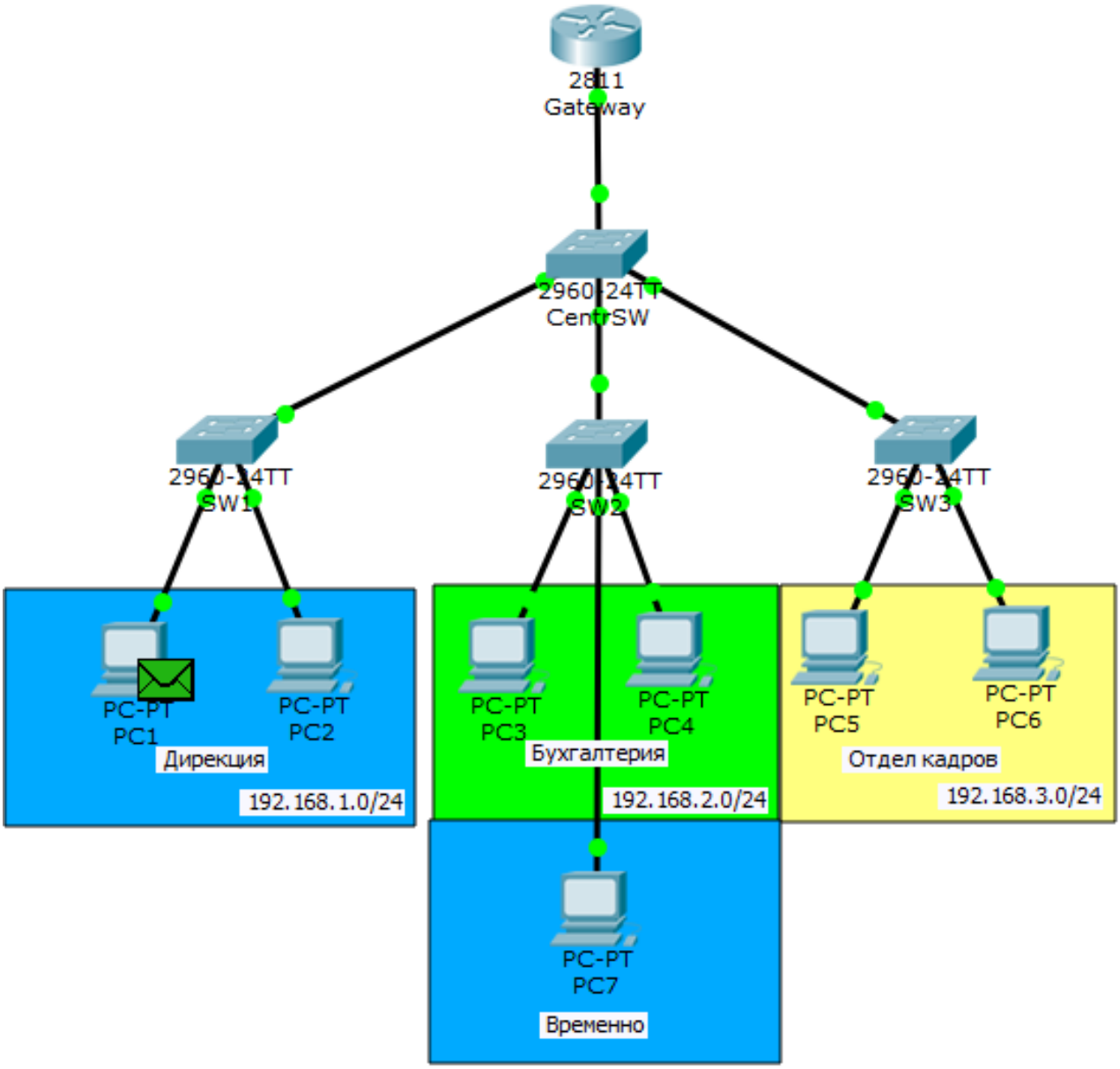

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

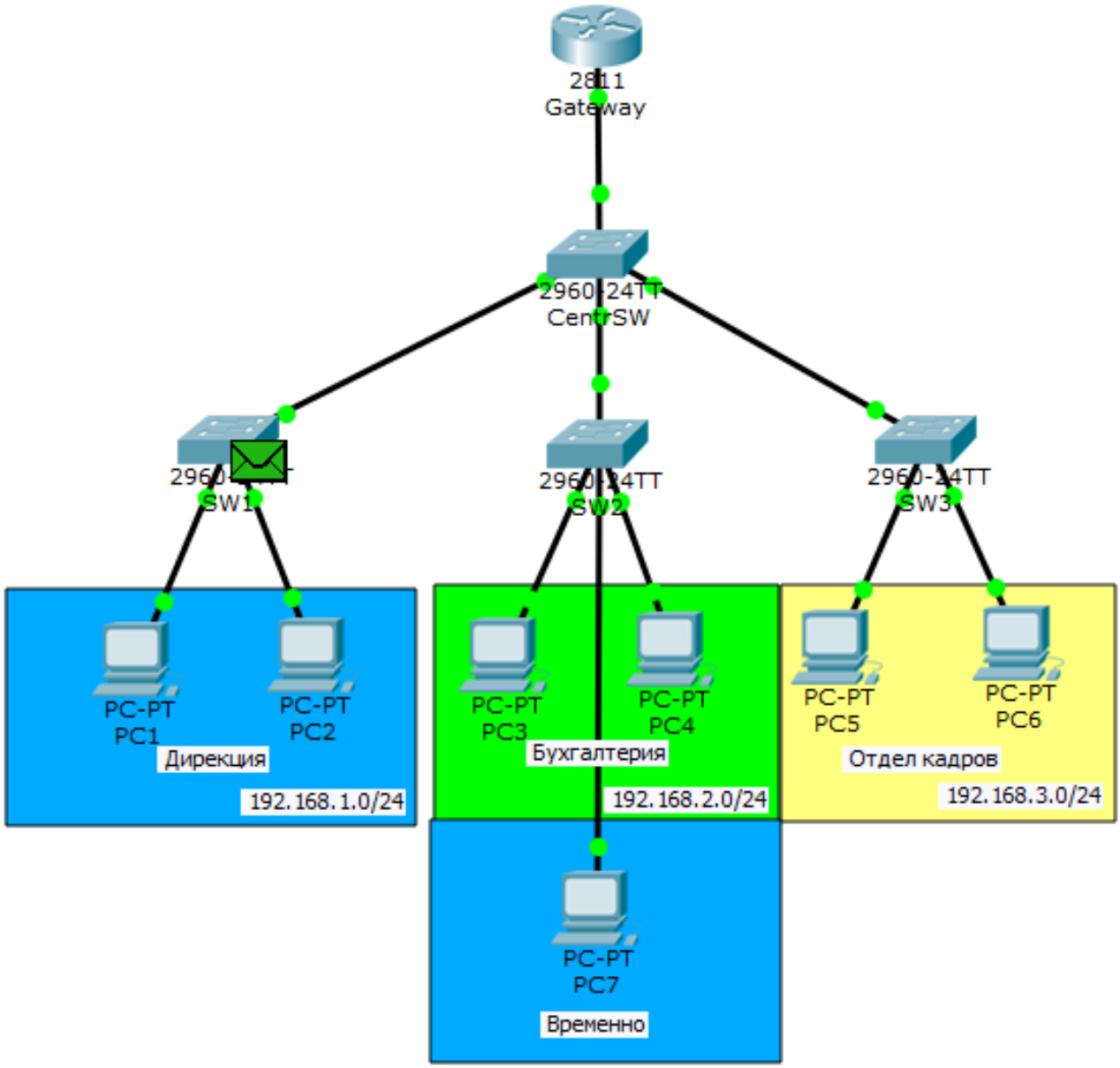


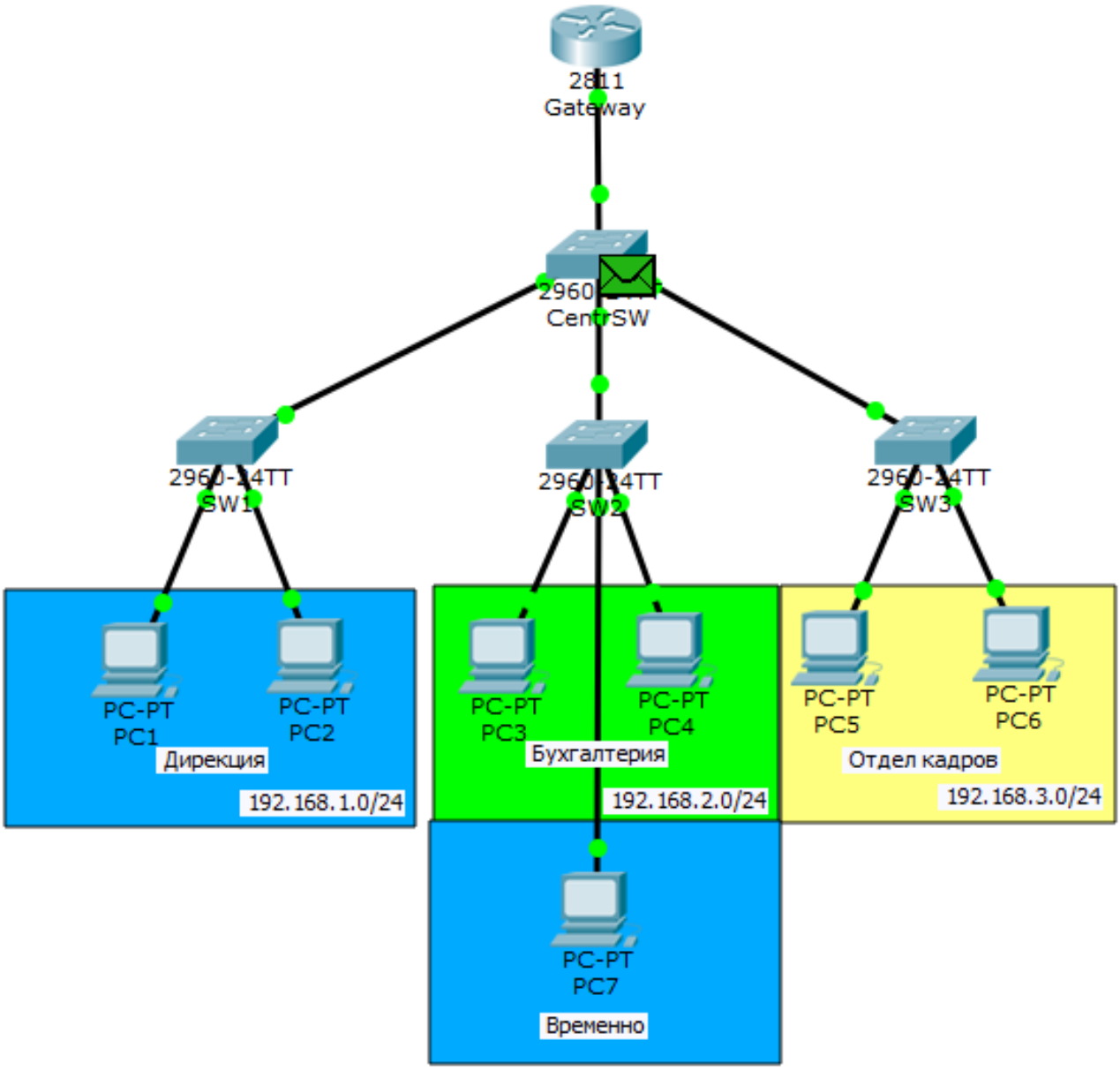
Доходит до маршрутизатора ответ и он добавляет запись в своей таблице. Посмотреть таблицу ARP можно командой **show arp**.

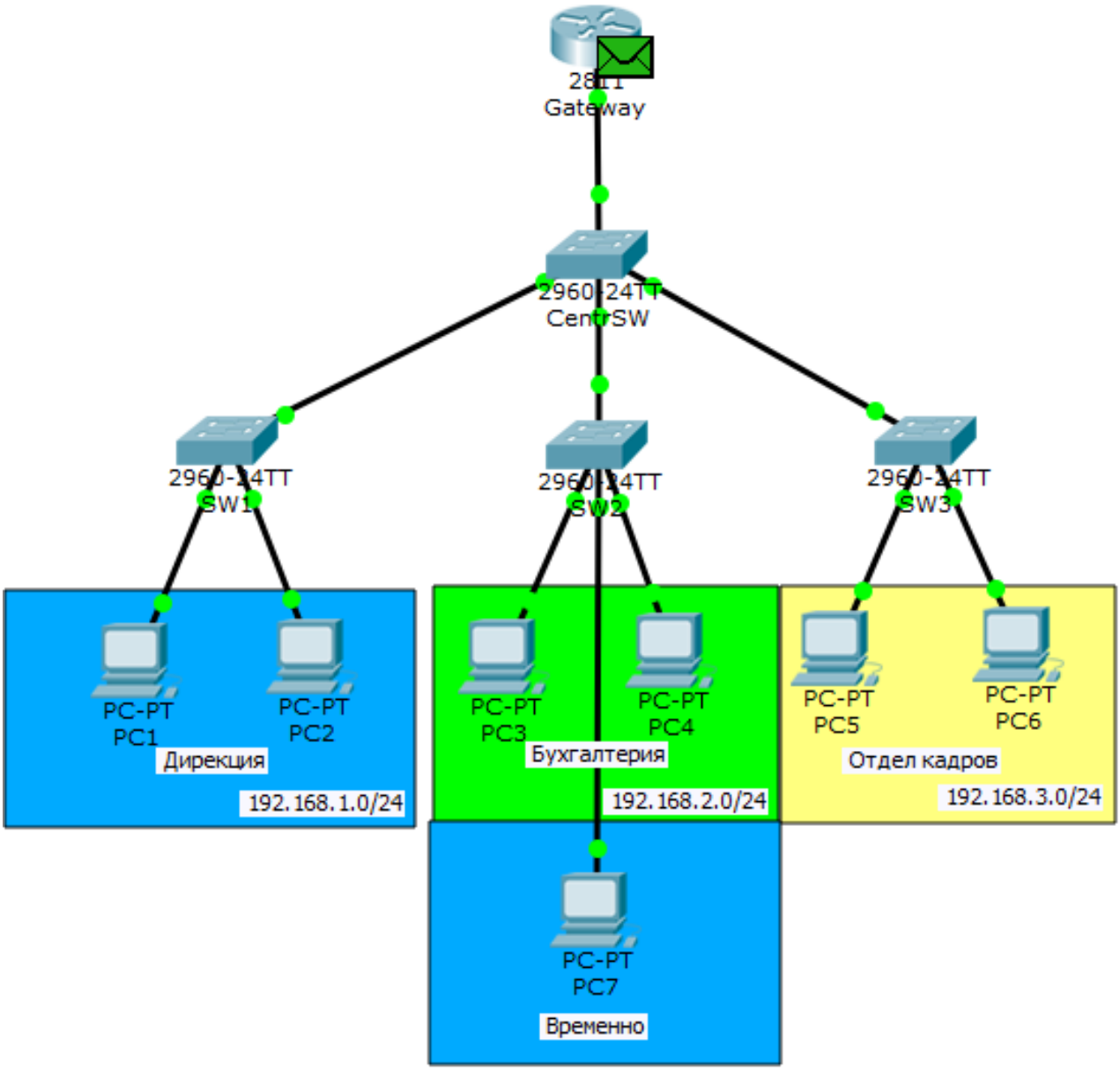
```
Gateway#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.2              0   0000.0C1C.05DD  ARPA   FastEthernet0/0.2
Internet  192.168.3.3              0   0002.17A5.D5B4  ARPA   FastEthernet0/0.4
```

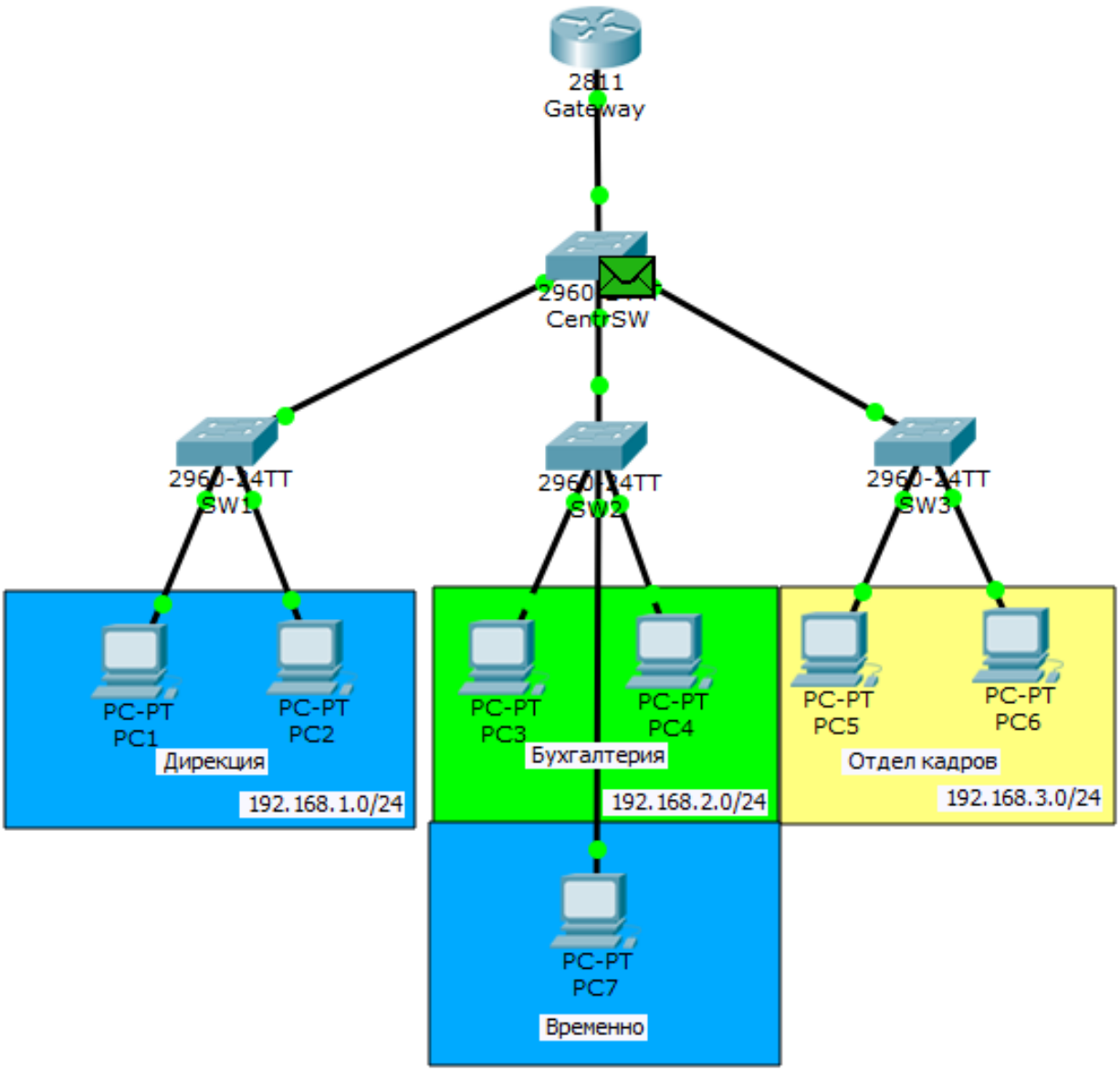
Двигаемся дальше. PC1 недоволен, что ему никто не отвечает и отправляет следующее ICMP-сообщение.

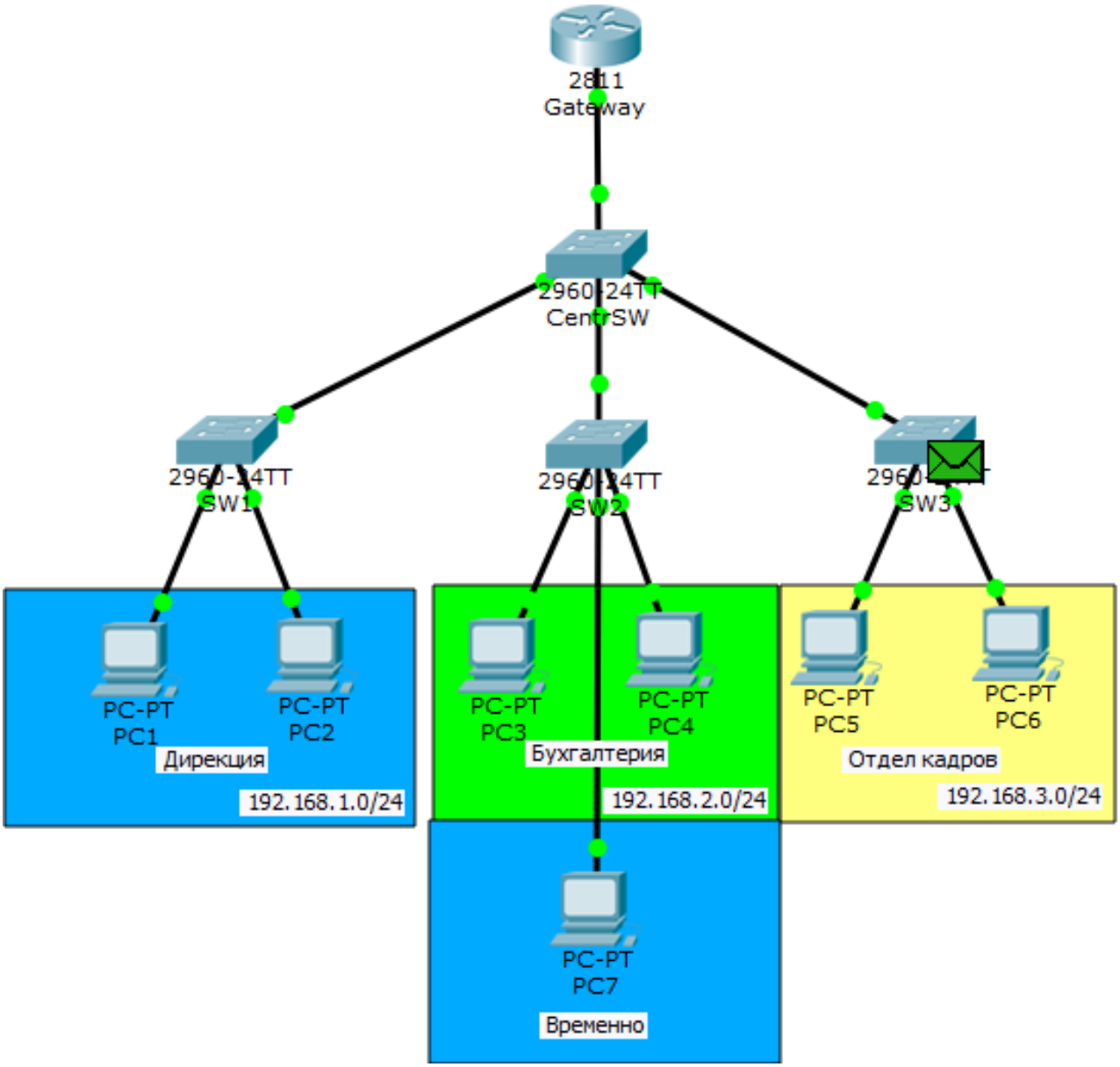

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно

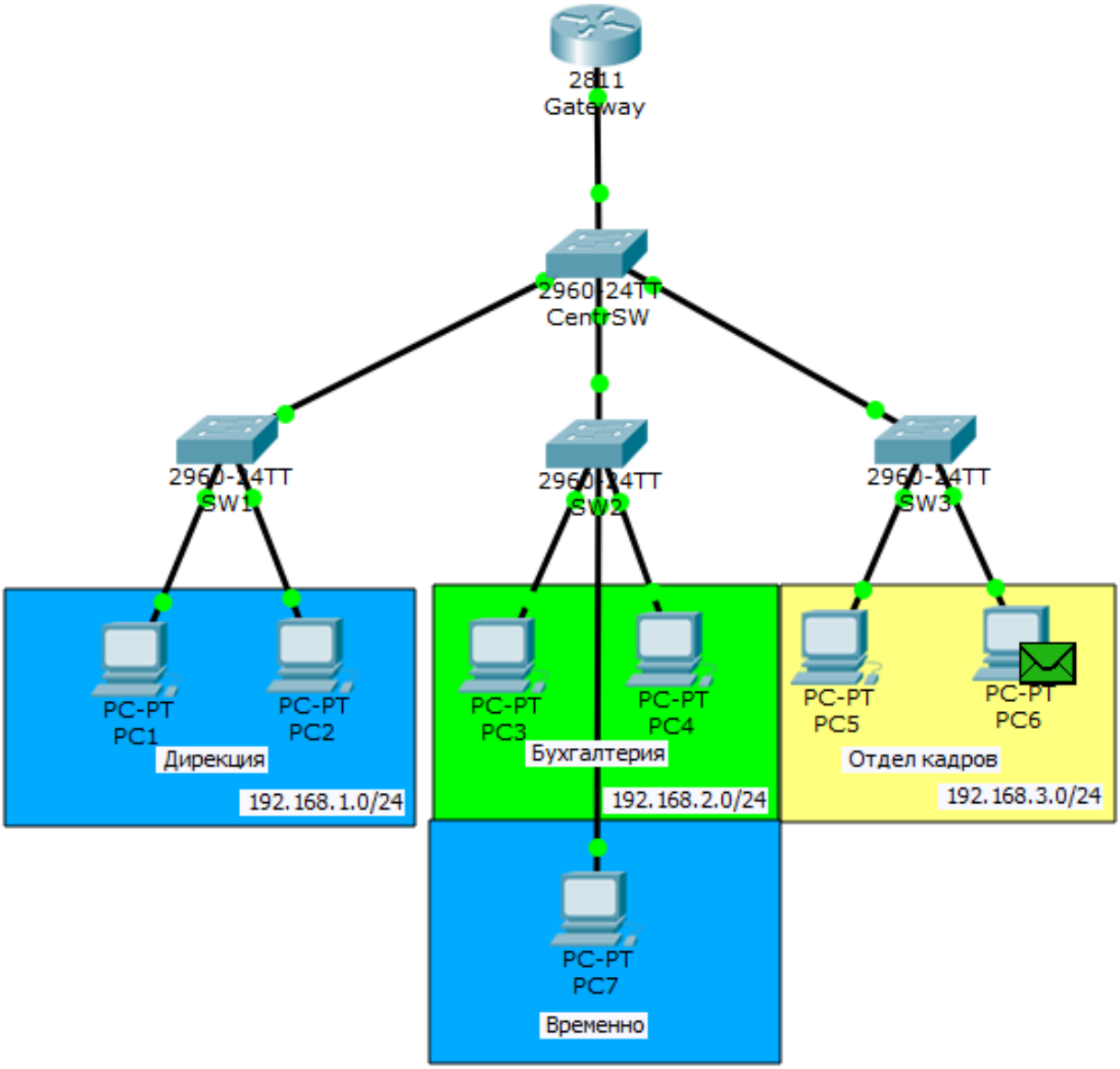

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно


2811
Gateway
2960
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

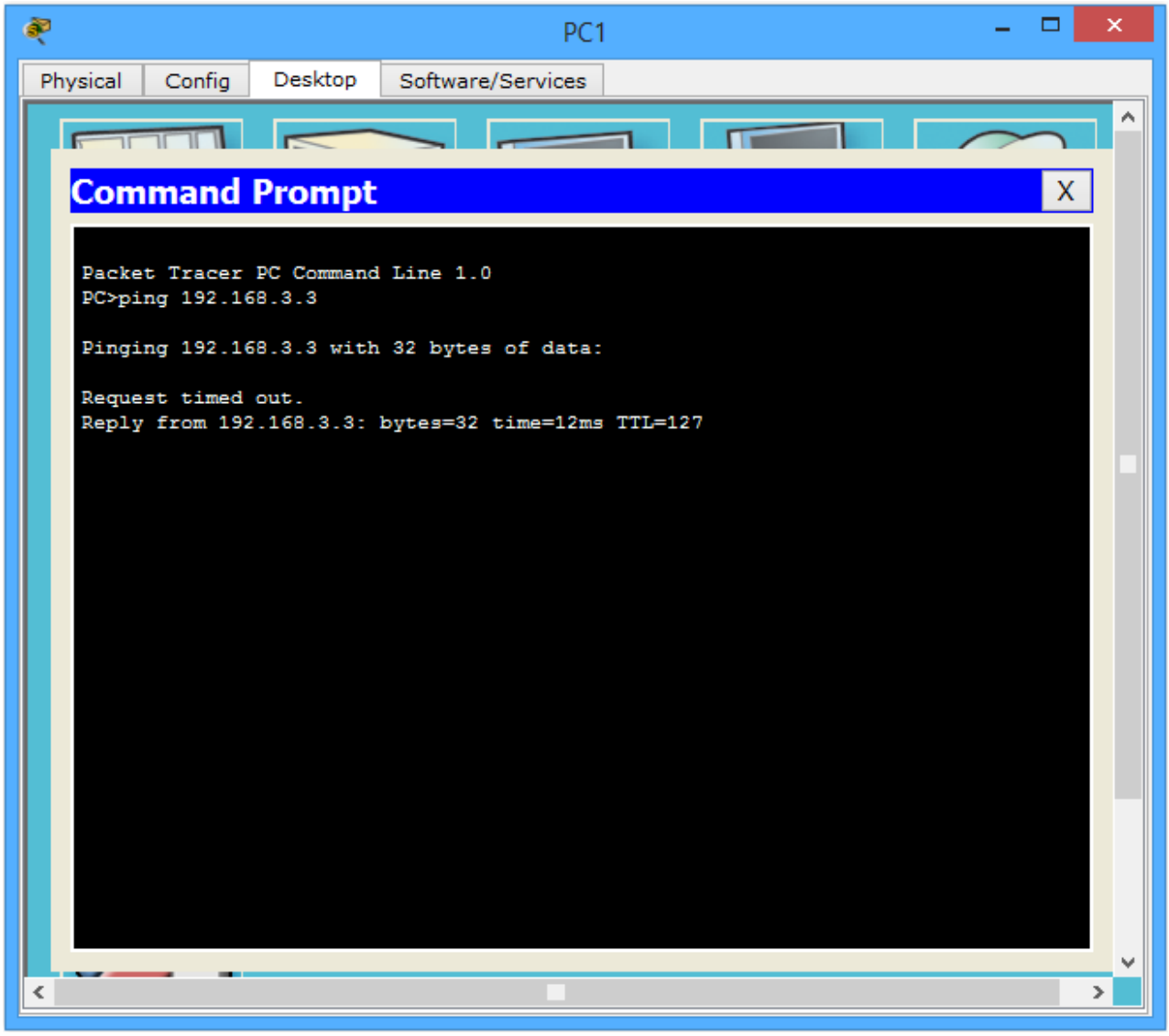

2811
Gateway
2960-24TT
CentrSW
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
PC-PT
PC1
PC-PT
PC2
Дирекция
192.168.1.0/24
PC-PT
PC3
PC-PT
PC4
Бухгалтерия
192.168.2.0/24
PC-PT
PC5
PC-PT
PC6
Отдел кадров
192.168.3.0/24
PC-PT
PC7
Временно


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



На этот раз ICMP доходит без проблем. Обратно он проследует тем же маршрутом. Я лишь покажу конечный результат.



Первый пакет затерялся (в результате работы ARP), а второй дошел без проблем. Кому интересно увидеть в анимации, добро пожаловать под спойлер.

InterVLAN Routing

Итак. Мы добились того, что если узлы находятся в одной подсети и в одном VLAN, то ходить они будут напрямую через коммутаторы. В случае, когда нужно передать сообщение в другую подсеть и VLAN, то передавать будут через роутер Gateway, который осуществляет «межвлановую» маршрутизацию. Данная топология получила название **«router on a stick»** или **«роутер на палочке»**. Как вы поняли она очень удобна. Мы создали 3 виртуальных интерфейса и по одному проводу гоняли разные тегированные кадры. Без использования сабинтерфейсов и VLAN-ов, пришлось бы для каждой подсети задействовать отдельный физический интерфейс, что совсем не выгодно.

Кстати очень хорошо этот вопрос разобран в этом видео (видео идет около 3-х часов, поэтому ссылка с привязкой именно к тому моменту времени). Если после прочтения и просмотра видео захочется добить все собственными руками,

прикладываю ссылку на скачивание.

Разобрались с VLAN-ами и переходим к одному из протоколов, работающего с ним. **DTP (англ. Dynamic Trunking Protocol)** или на русском **динамический транковый протокол** — проприетарный протокол компании Cisco, служащий для реализации trunk режима между коммутаторами. Хотя в зависимости от состояния, они могут согласоваться и в режим access.

В DTP есть 4 режима: Dynamic auto, Dynamic desirable, Trunk, Access. Рассмотрим как они согласуются.

Режимы	**Dynamic auto**	**Dynamic desirable**	**Trunk**	**Access**
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Отсутствие соединения
Access	Access	Access	Отсутствие соединения	Access

То есть левая колонка это 1-ое устройство, а верхняя строка 2-ое устройство. По-умолчанию коммутаторы находятся в режиме «dynamic auto». Если посмотреть таблицу сопоставления, то два коммутатора в режиме «dynamic auto» согласуются в режим «access». Давайте это и проверим. Создаю я новую лабораторную работу и добавлю 2 коммутатора.

Соединять их пока не буду. Мне надо убедиться, что оба коммутатора в режиме «dynamic auto». Проверять буду командой **show interfaces switchport**.

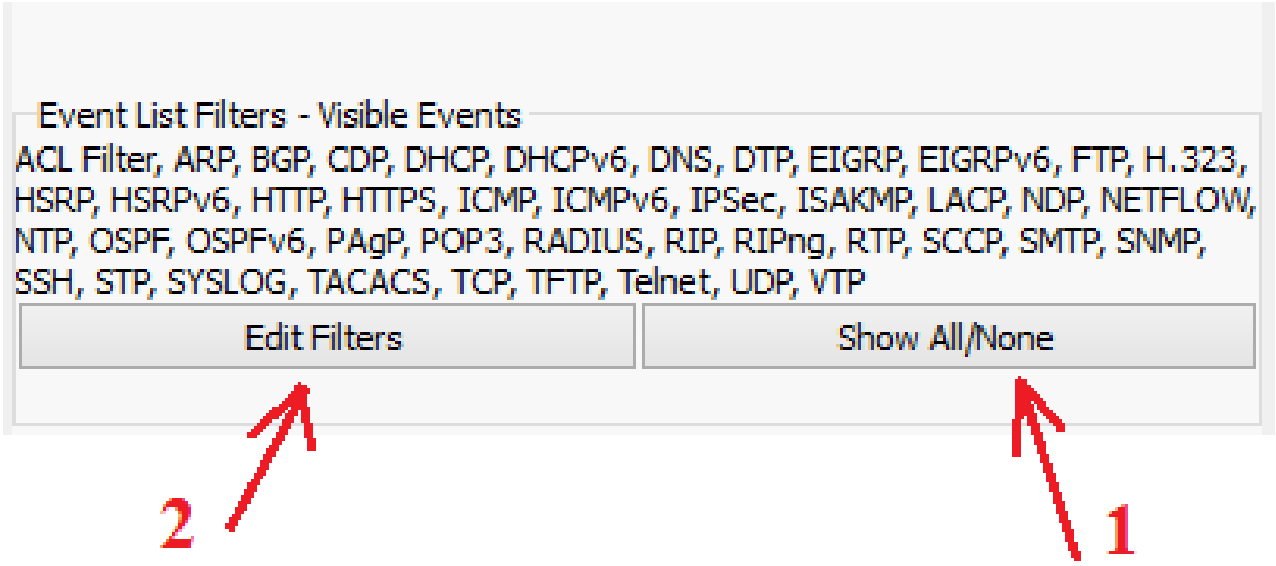
```
SW1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)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

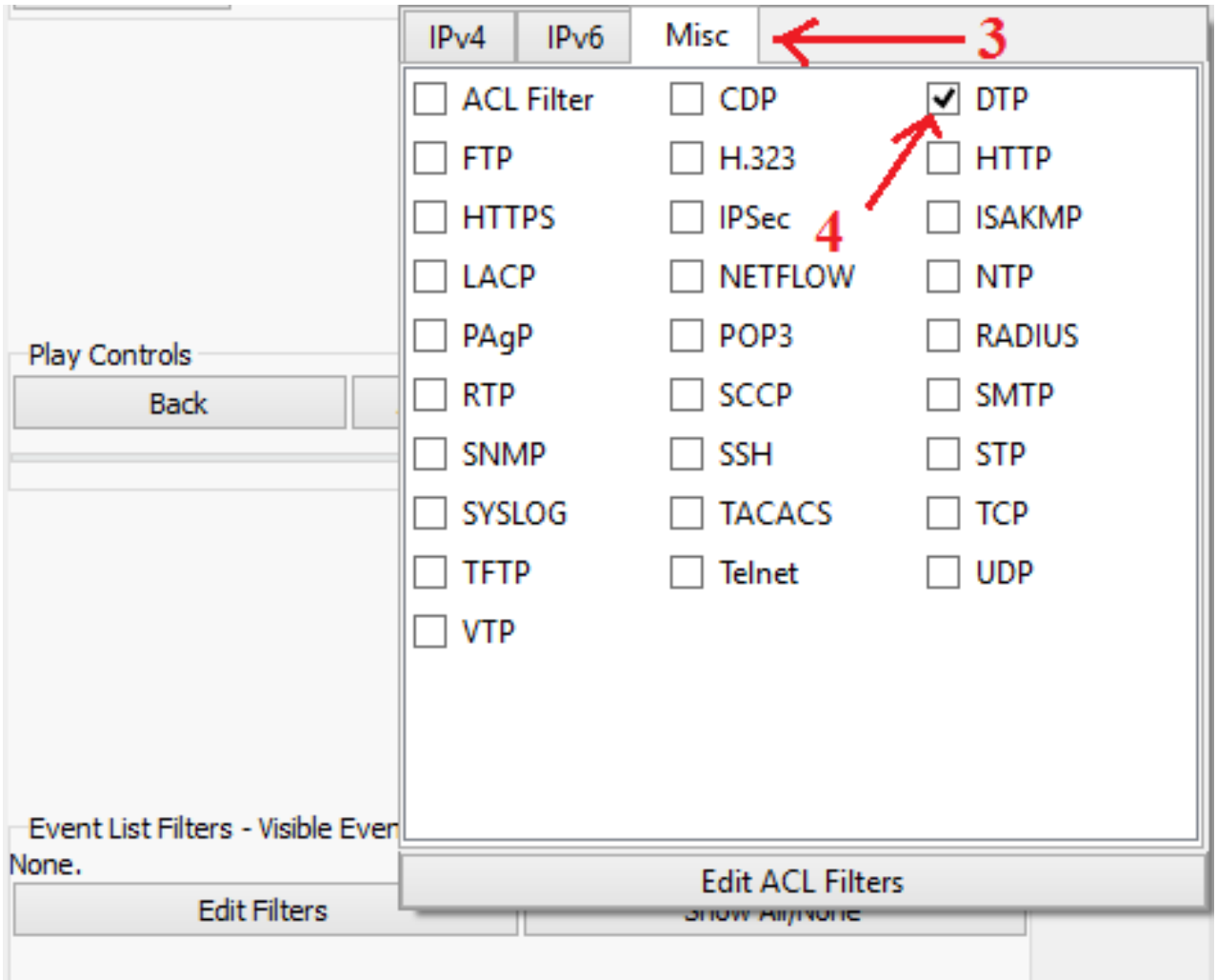
```
SW2#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)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

Результат этой команды очень большой, поэтому я его обрезал и выделил интересующие пункты. Начнем с **Administrative Mode**. Эта строка показывает, в каком из 4-режимов работает данный порт на коммутаторе. Убеждаемся, что на обоих коммутаторах порты в режиме «Dynamic auto». А строка **Operational Mode** показывает, в каком режиме работы они согласовали работу. Мы пока их не соединяли, поэтому они в состоянии «down».

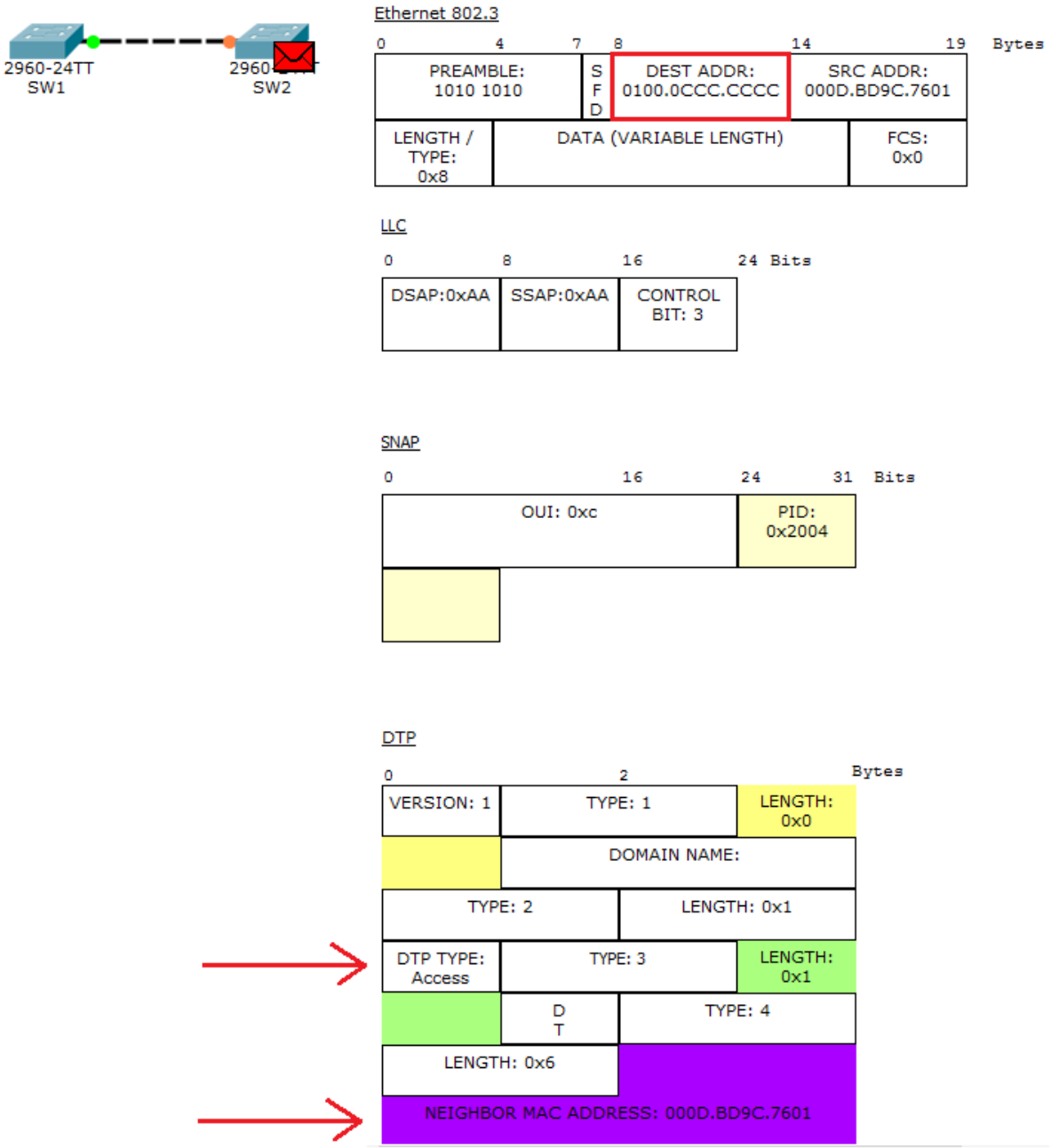
Сразу дам вам хороший совет. При тестировании какого либо протокола, пользуйтесь фильтрами. Отключайте показ работы всех ненужных вам протоколов.

Перевожу CPT в режим simulation и отфильтрую все протоколы, кроме DTP.





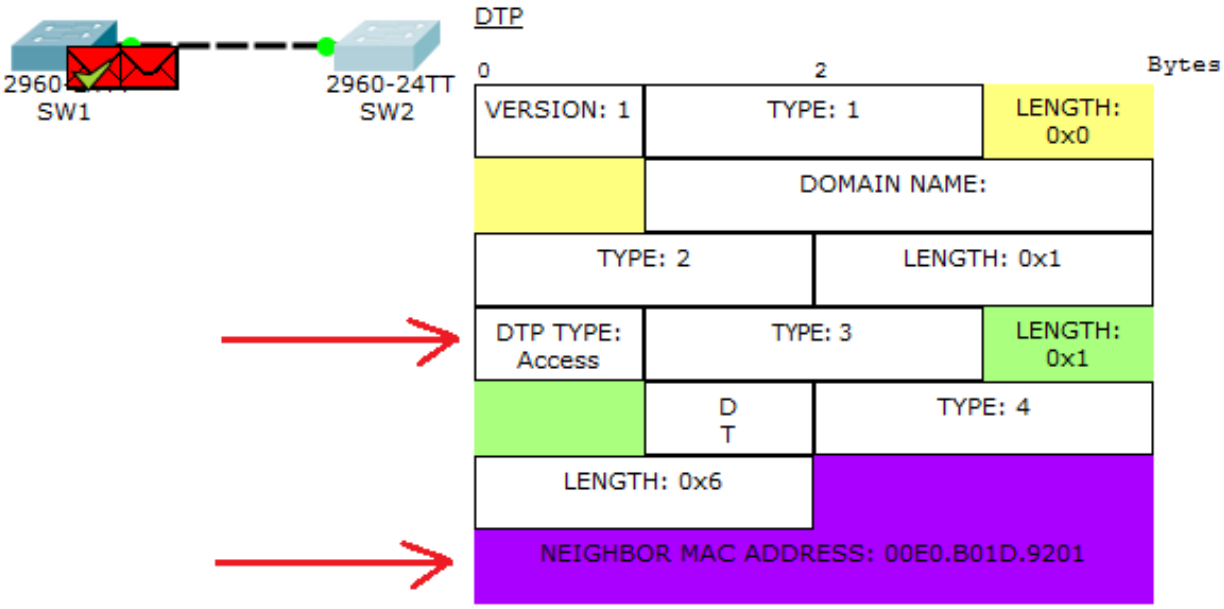
Думаю здесь все понятно. Соединяю коммутаторы кабелем и, при поднятии линков, один из коммутаторов генерирует DTP-сообщение.



Открываю и вижу, что это DTP инкапсулированный в Ethernet-кадр. Отправляет он его на мультикастовый адрес «0100.0ccc.cccc», который относится к протоколам DTP, VTP, CDP.
И обращу внимание на 2 поля в заголовке DTP.

1) **DTP Type** — сюда отправляющий вставляет предложение. То есть в какой режим он хочет согласоваться. В нашем случае он предлагает согласовать «access».
2) **Neighbor MAC-address** — в это поле он записывает MAC-адрес своего порта.

Отправляет он и ждет реакции от соседа.



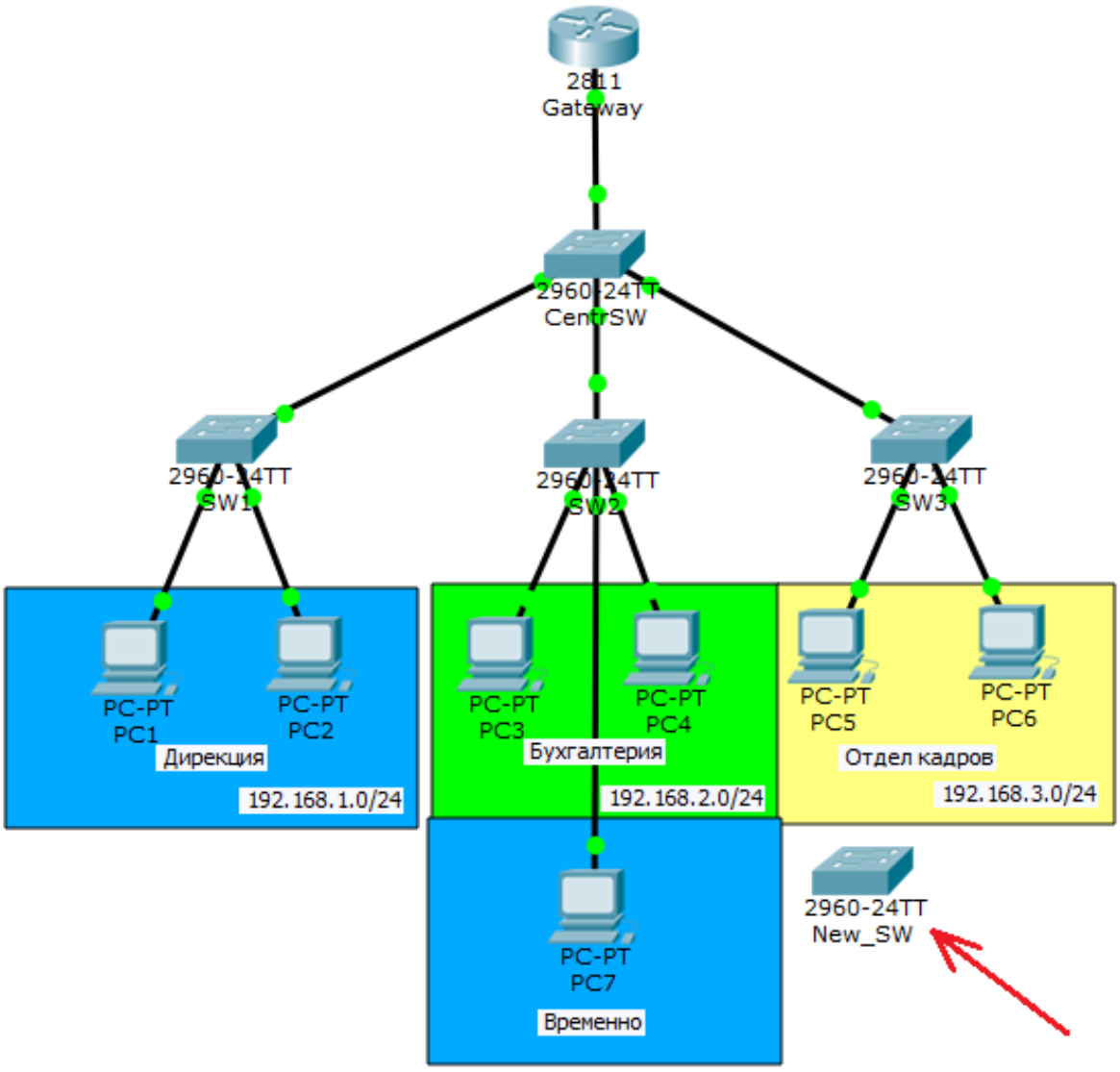
Доходит до SW1 сообщение и он генерирует ответный. Где также согласует режим «access», вставляет свой MAC-адрес и отправляет в путь до SW2.

Успешно доходит DTP. По идее они должны были согласоваться в режиме «access». Проверю.

```
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
```

Как и предполагалось, согласовались они в режим «access».
Кто то говорит, что технология удобная и пользуется ею. Но я крайне не рекомендую использовать этот протокол в своей сети. Рекомендую это не только я, и сейчас объясню почему. Смысл в том, что этот протокол открывает большую дыру в безопасности. Я открою лабораторку, в которой разбиралась работа «Router on a stick» и добавлю туда еще один коммутатор.



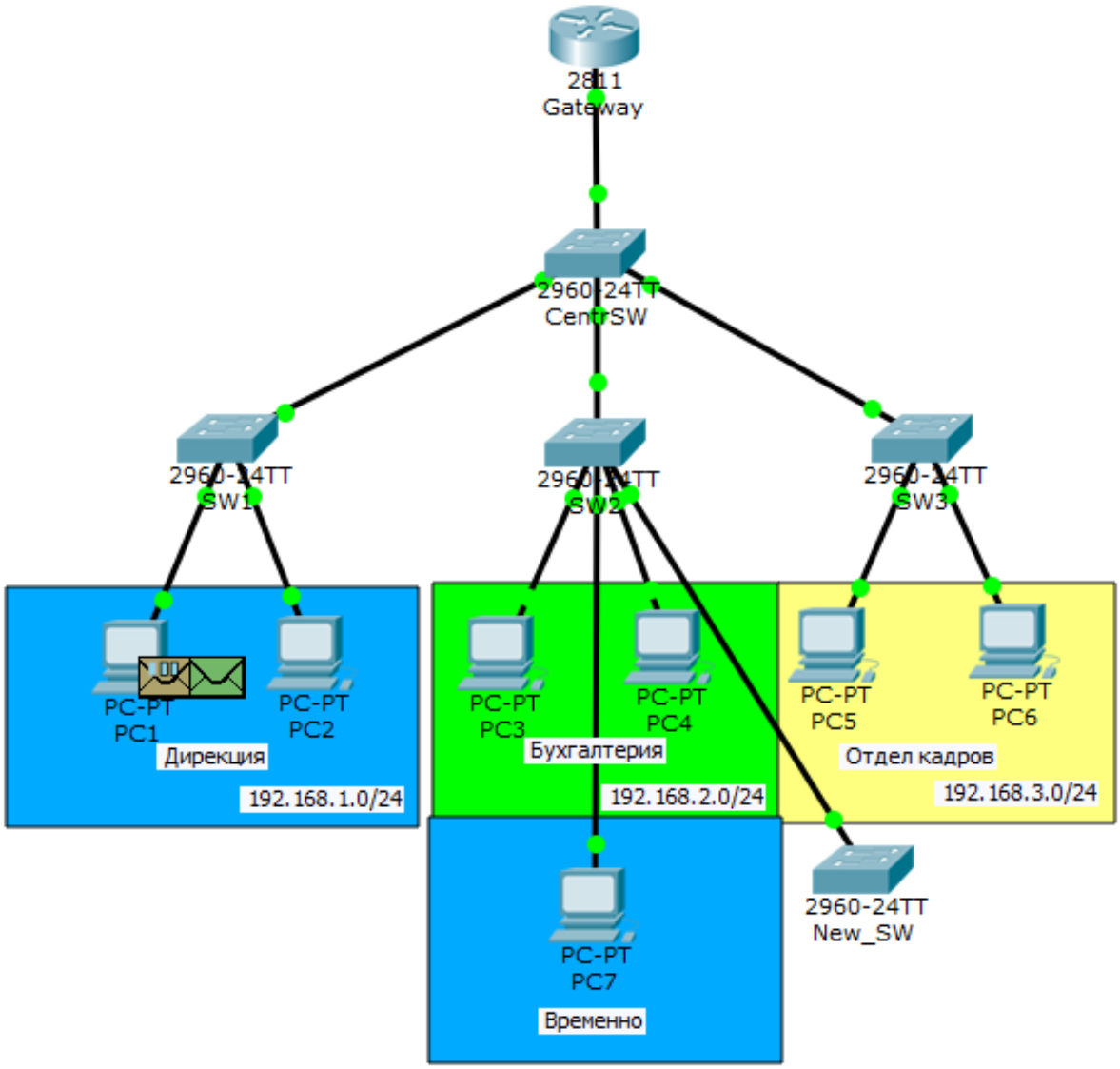
Теперь зайду в настройки нового коммутатора и жестко пропишу на порту работу в режиме trunk.

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

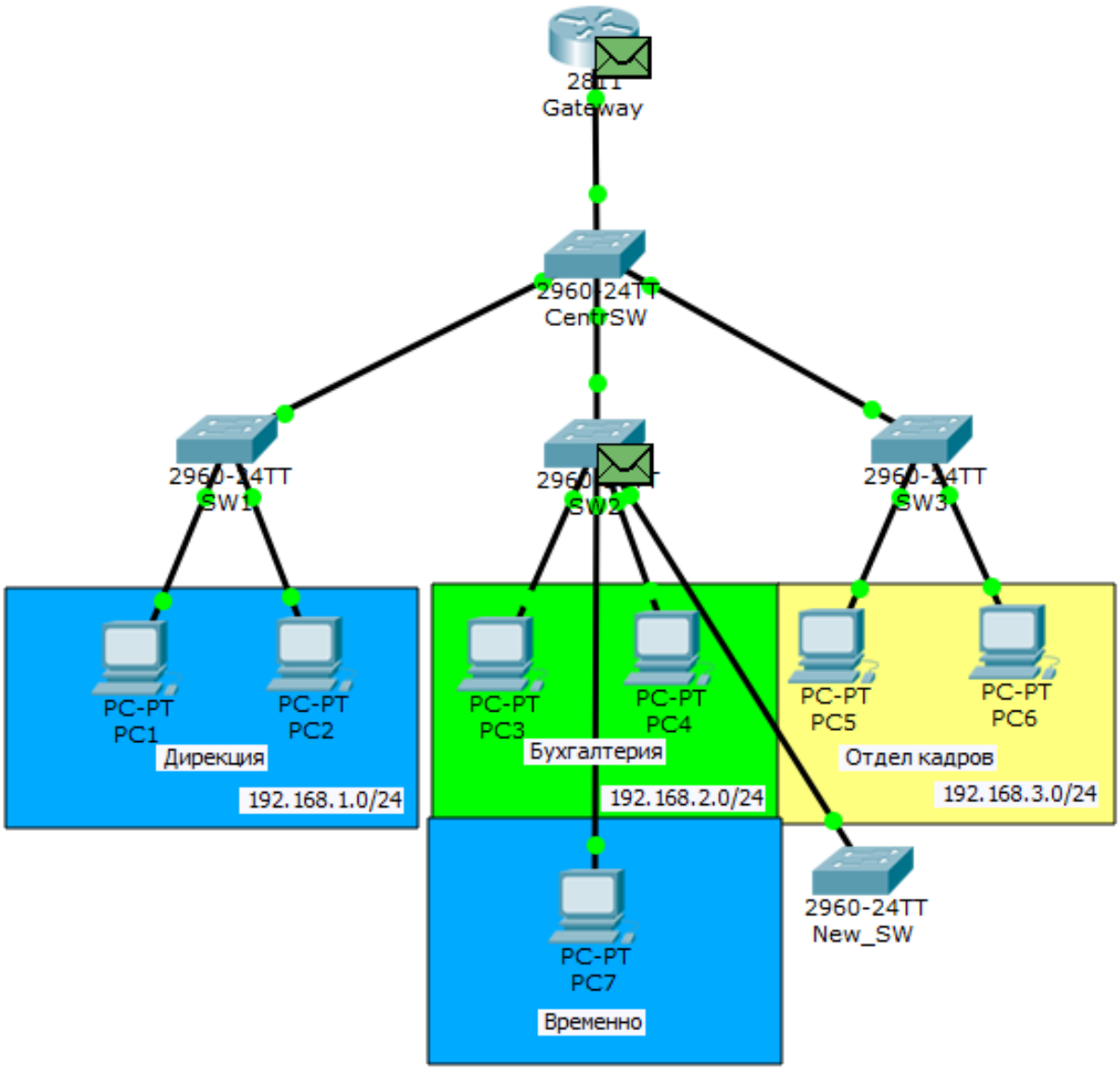
Соединяю их и смотрю, как они согласовались.

```
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
```

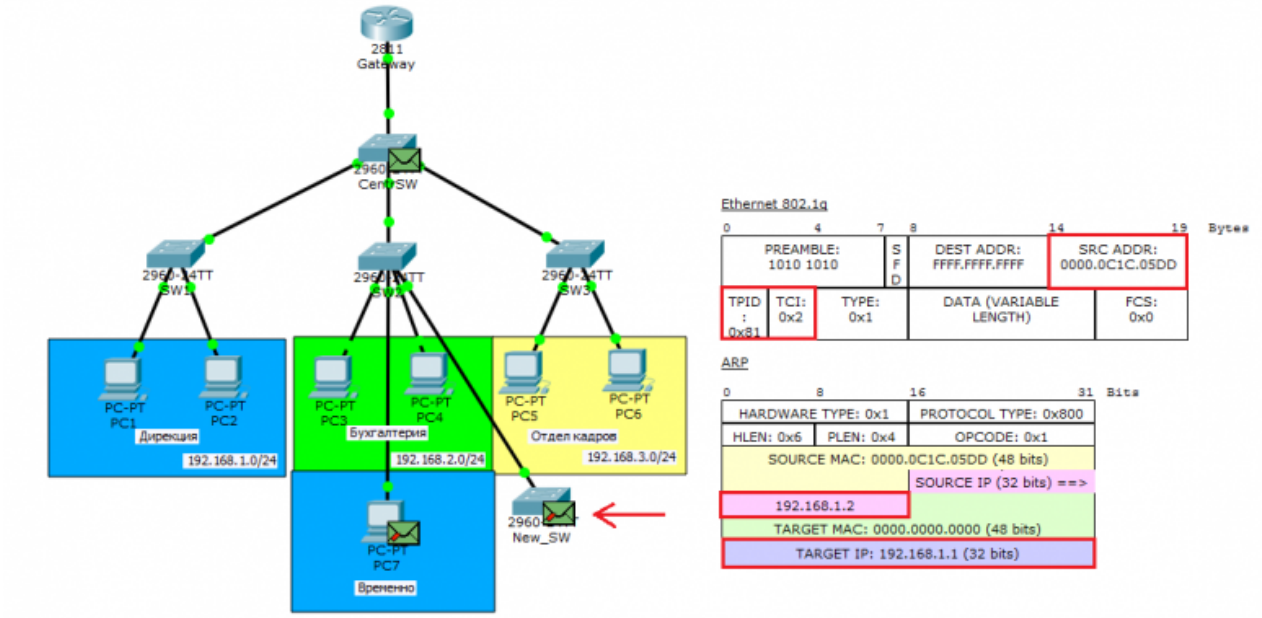
Все верно. Режимы «dynamic auto» и «trunk» согласуются в режим **trunk**. Теперь ждем, когда кто- то начнет проявлять активность. Допустим PC1 решил кому то отправить сообщение. Формирует ARP и выпускает в сеть.



Пропустим его путь до того момента, когда он попадет на SW2.



И вот самое интересное.



Он отправляет его на вновь подключенный коммутатор. Объясняю, что произошло. Как только мы согласовали с ним trunk, он начинает отправлять ему все пришедшие кадры. Хоть на схеме и показано, что коммутатор отбрасывает кадры, это ничего не значит. К коммутатору или вместо коммутатора можно подключить любое перехватывающее устройство (sniffer) и спокойно просматривать, что творится в сети. Вроде перехватил он безобидный ARP. Но если взглянуть глубже, то можно увидеть, что уже известен MAC-адрес «0000.0C1C.05DD» и IP-адрес «192.168.1.2». То есть PC1 не думая выдал себя. Теперь злоумышленник знает о таком компьютере. Вдобавок он знает, что он сидит во 2-ом VLAN. Дальше он может натворить многого. Самое банальное — это подменить свой MAC-адрес, IP-адрес, согласоваться быстро в Access и и выдавать себя за PC1. Но самое интересное. Ведь сразу можно этого не понять. Обычно, когда мы прописываем режим работы порта, он сразу отображается в конфигурации. Ввожу **show running-config** .

Но здесь настройки порта пустые. Ввожу **show interfaces switchport** и проматываю до fa0/4.

```
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
```

```
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
```

А вот здесь видим, что согласован trunk. Не всегда show running-config дает

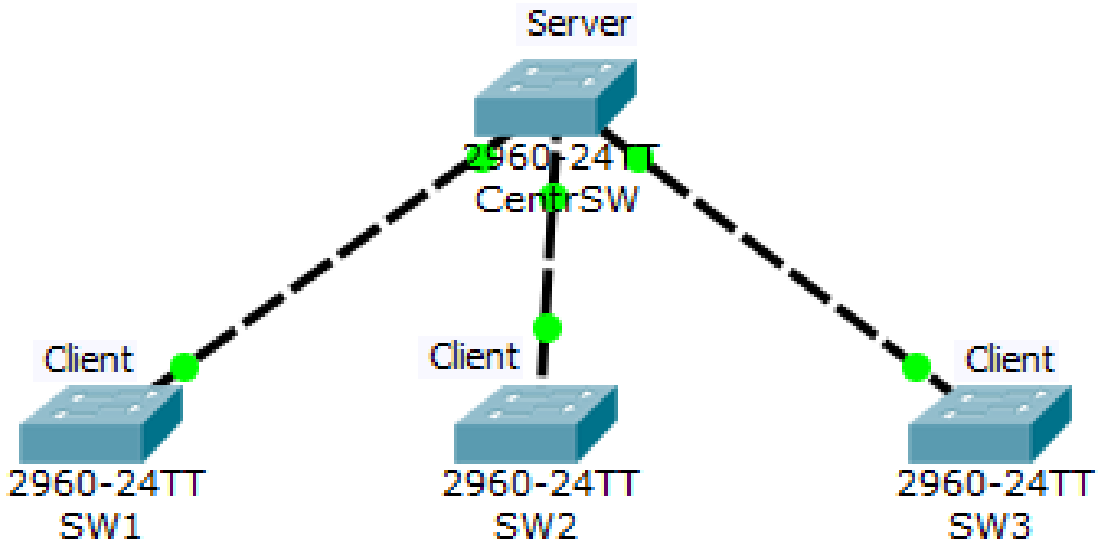
исчерпывающую информацию. Поэтому запоминайте и другие команды.

Думаю понятно почему нельзя доверять этому протоколу. Он вроде облегчает жизнь, но в то же время может создать огромную проблему. Поэтому полагайтесь на ручной метод. При настройке сразу же обозначьте себе какие порты будут работать в режиме trunk, а какие в access. И самое главное — всегда отключайте согласование. Чтобы коммутаторы не пытались ни с кем согласоваться. Делается это командой «switchport nonegotiate».

Переходим к следующему протоколу.

VTP (англ. VLAN Trunking Protocol) — проприетарный протокол компании Cisco, служащий для обмена информацией о VLAN-ах.

Представьте ситуацию, что у вас 40 коммутаторов и 70 VLAN-ов. По хорошему нужно вручную на каждом коммутаторе их создать и прописать на каких trunk-ых портах разрешать передачу. Дело это муторное и долгое. Поэтому эту задачу может взвалить на себя VTP. Вы создаете VLAN на одном коммутаторе, а все остальные синхронизируются с его базой. Взгляните на следующую топологию.



Здесь присутствуют 4 коммутатора. Один из них является VTP-сервером, а 3 остальных клиентами. Те VLAN, которые будут созданы на сервере, автоматически синхронизируются на клиентах. Объясню как работает VTP и что он умеет.

Итак. VTP может создавать, изменять и удалять VLAN. Каждое такое действие влечет к тому, что увеличивается номер ревизии (каждое действие увеличивает номер на +1). После он рассылает объявления, где указан номер ревизии. Клиенты, получившие это объявление, сравнивают свой номер ревизии с пришедшим. И если пришедший номер выше, они синхронизируют свою базу с ней. В противном случае объявление игнорируется.

Но это еще не все. У VTP есть роли. По-умолчанию все коммутаторы работают в роли сервера. Расскажу про них.

1. **VTP Server**. Умеет все. То есть создает, изменяет, удаляет VLAN. Если получает объявление, в которых ревизия старше его, то синхронизируется. Постоянно рассылает объявления и ретранслирует от соседей.
2. **VTP Client** — Эта роль уже ограничена. Создавать, изменять и удалять VLAN нельзя. Все VLAN получает и синхронизирует от сервера. Периодически сообщает соседям о своей базе VLAN-ов.
3. **VTP Transparent** — эта такая независимая роль. Может создавать, изменять и удалять VLAN только в своей базе. Никому ничего не навязывает и ни от кого не принимает. Если получает какое то объявление, передает дальше, но со своей базой не синхронизирует. Если в предыдущих ролях, при каждом изменении увеличивался номер ревизии, то в этом режиме номер ревизии всегда равен 0.

Это все, что касается VTP версии 2. В VTP 3-ей версии добавилась еще одна роль — **VTP Off**. Он не передает никакие объявления. В остальном работа аналогична режиму **Transparent**.

Начитались теории и переходим к практике. Проверим, что центральный коммутатор в режиме Server. Вводим 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)
```

Видим, что VTP Operating Mode: Server. Также можно заметить, что версия VTP 2-ая. К сожалению, в CPT 3-ья версия не поддерживается. Версия ревизии нулевая. Теперь настроим нижние коммутаторы.

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

Видим сообщение, что устройство перешло в клиентский режим. Остальные настраиваются точно также.

Чтобы устройства смогли обмениваться объявлениями, они должны находиться в одном домене. Причем тут есть особенность. Если устройство (в режиме Server или Client) не состоит ни в одном домене, то при первом полученном объявлении, перейдет в объявленный домен. Если же клиент состоит в каком то домене, то принимать объявления от других доменов не будет. Откроем SW1 и убедимся, что он не состоит ни в одном домене.

```
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
```

Убеждаемся, что тут пусто.

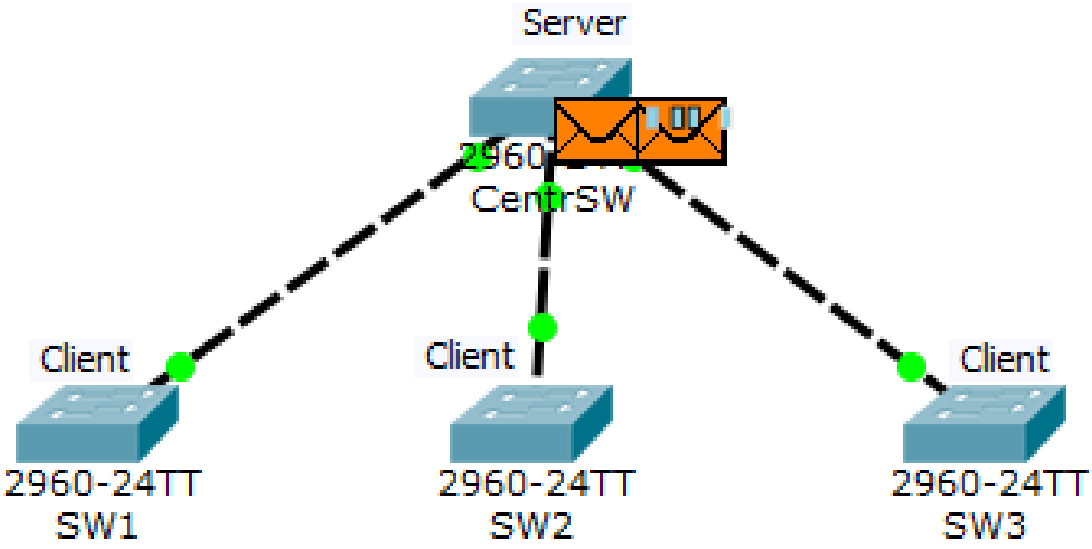
Теперь переходим центральному коммутатору и переведем его в домен.

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

Видим сообщение, что он перевелся в домен cisadmin.ru.
Проверим 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.ru
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)
```

И действительно. Имя домена изменилось. Обратите внимание, что номер ревизии пока что нулевой. Он изменится, как только мы создадим на нем VLAN. Но перед созданием надо перевести симулятор в режим simulation, чтобы посмотреть как он сгенерирует объявления. Создаем 20-ый VLAN и видим следующую картинку.



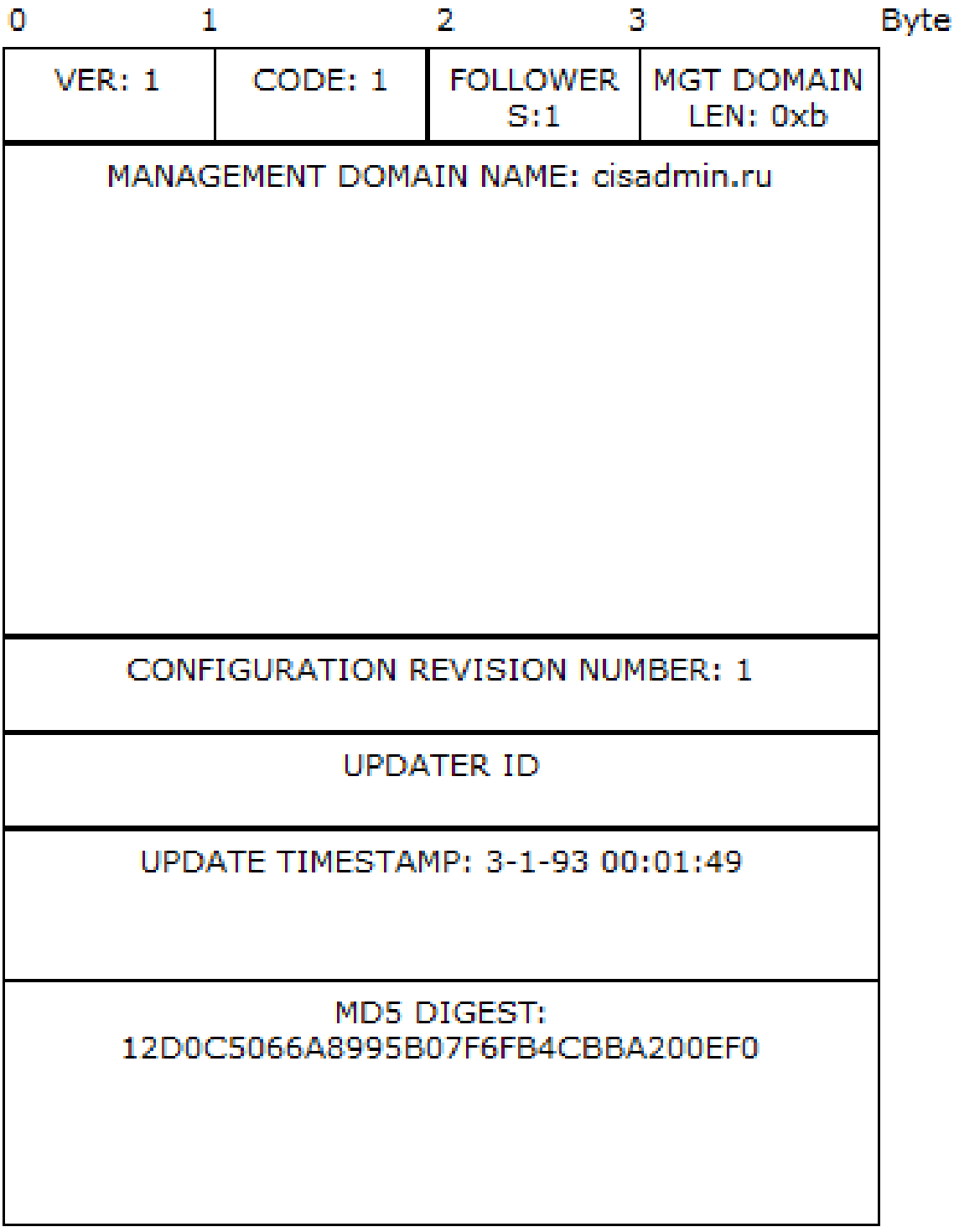
Как только создан VLAN и увеличился номер ревизии, сервер генерирует объявления. У него их два. Сначала откроем тот, что левее. Это объявление называется «Summary Advertisement» или на русском «сводное объявление». Это объявление генерируется коммутатором раз в 5 минут, где он рассказывает о имени домена и текущей ревизии. Смотрим как выглядит.

Ethernet 802.3

0 4	7	8 14	19 Bytes
PREAMBLE: 1010 1010	SFD	DEST ADDR: 0100.0CCC.CCCC	SRC ADDR: 00D0.BC22.BD03
LENGTH / TYPE: 0x8	DATA (VARIABLE LENGTH)		FCS: 0x0

В Ethernet-кадре обратите внимание на Destination MAC-адрес. Он такой же, как и выше, когда генерировался DTP. То есть, в нашем случае на него отреагируют только те, у кого запущен VTP. Теперь посмотрим на следующее поле.

VTP Summary Advertisement



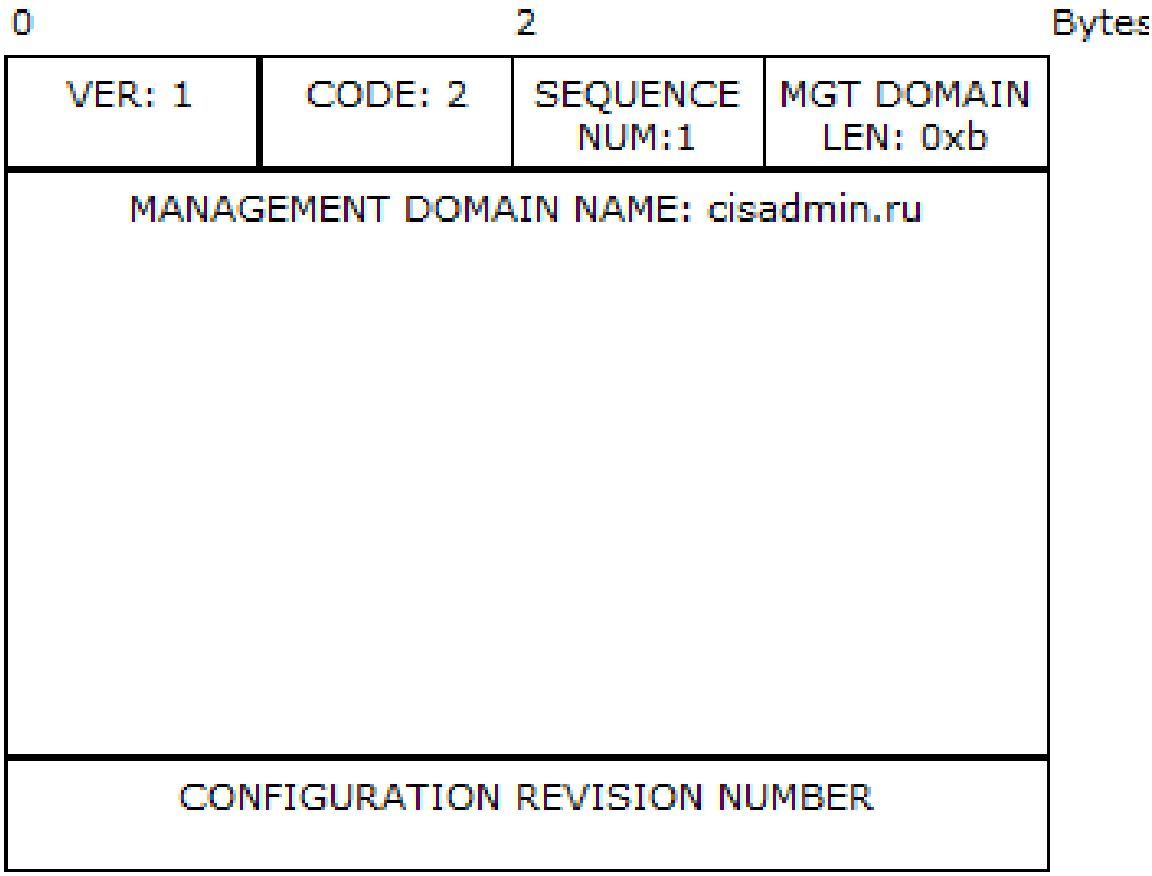
Здесь как раз вся информация. Пройдусь по самым важным полям.

- Management Domain Name — имя самого домена (в данном случае cisadmin.ru).
- Updater Identity — идентификатор того, кто обновляет. Здесь, как правило, записывается IP-адрес. Но так как адрес коммутатору не присваивали, то поле пустое
- Update Timestamp — время обновления. Время на коммутаторе не менялось, поэтому там стоит заводское.

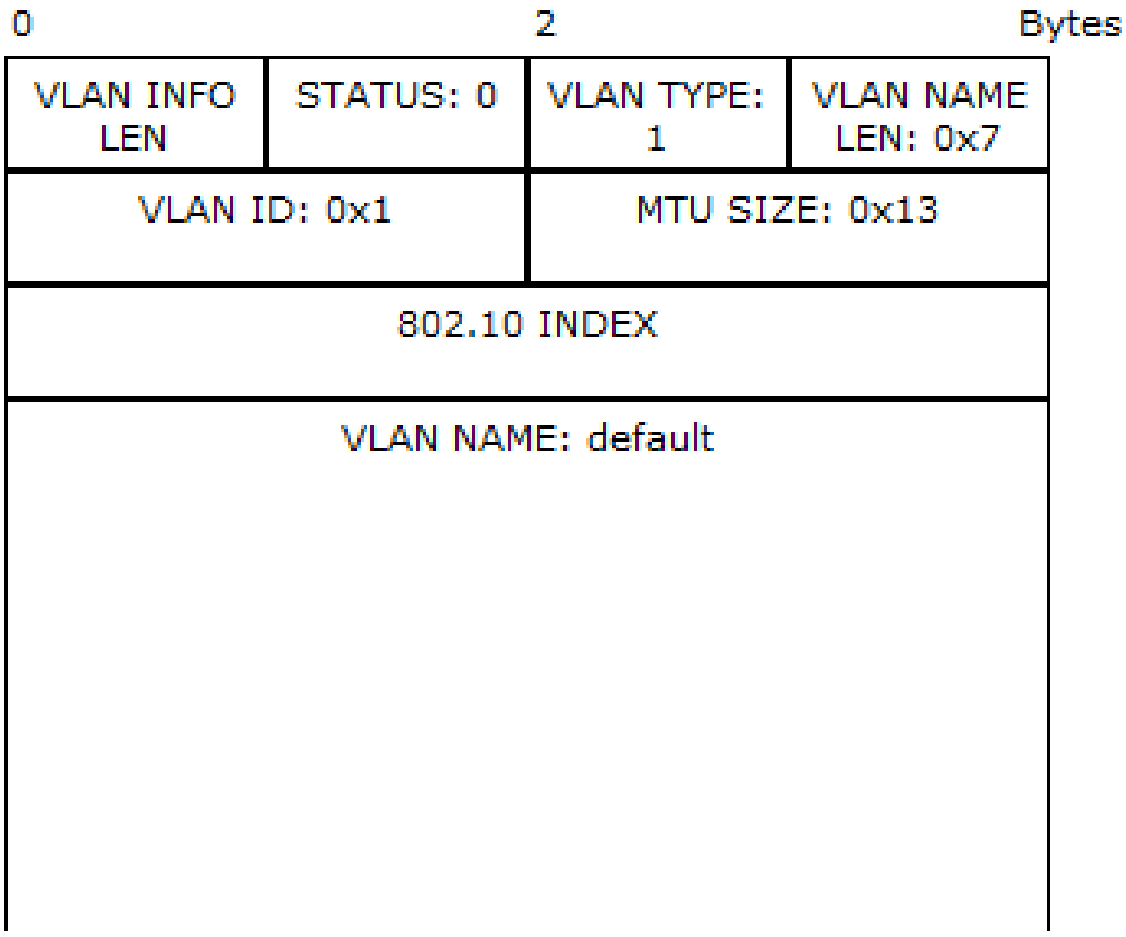
- MD5 Digest — хеш MD5. Оно используется для проверки полномочий. То есть, если на VTP стоит пароль. Мы пароль не меняли, поэтому хэш по-умолчанию.

Теперь посмотрим на следующее генерируемое сообщение (то, что справа). Оно называется «Subset Advertisement» или «подробное объявление». Это такая подробная информация о каждом передаваемом VLAN.

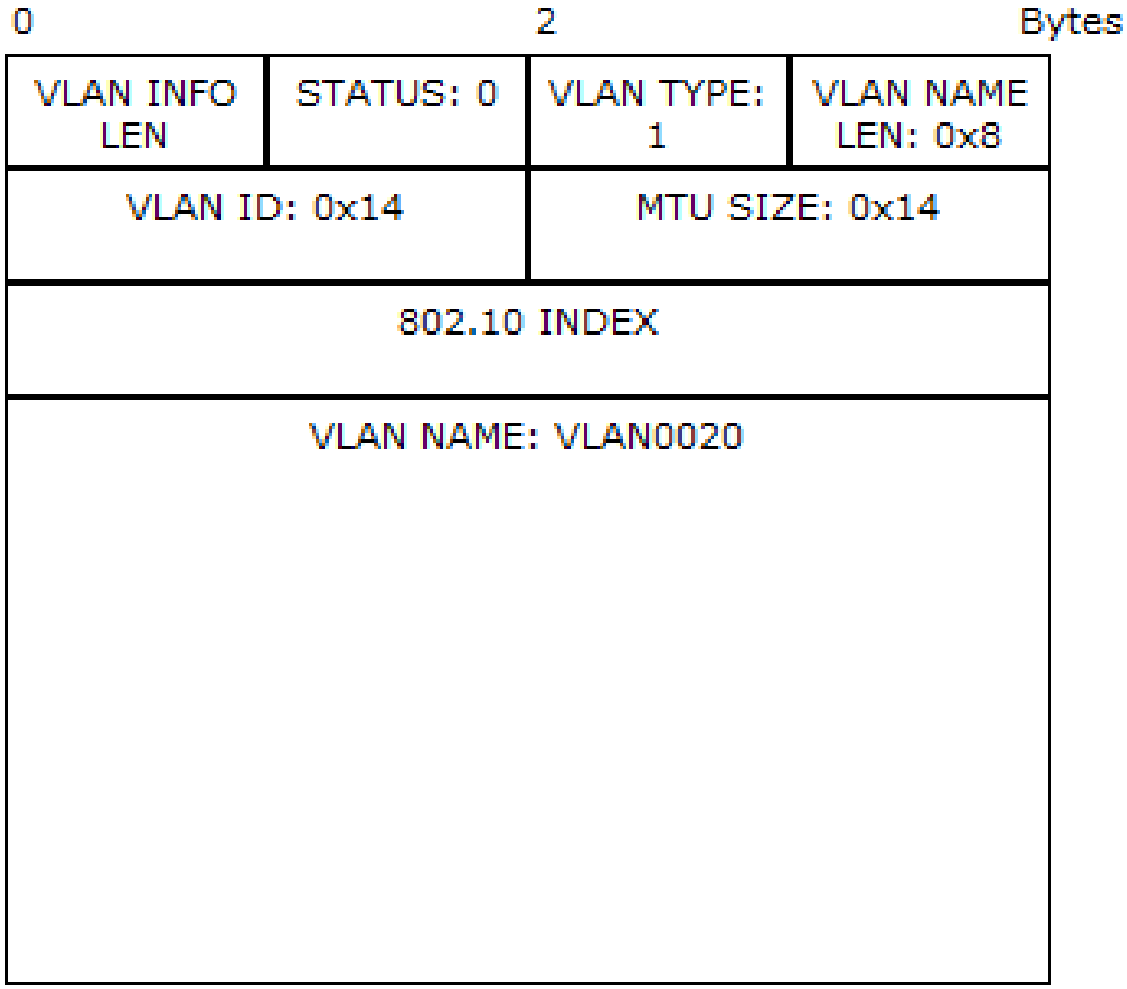
VTP Subset Advertisement



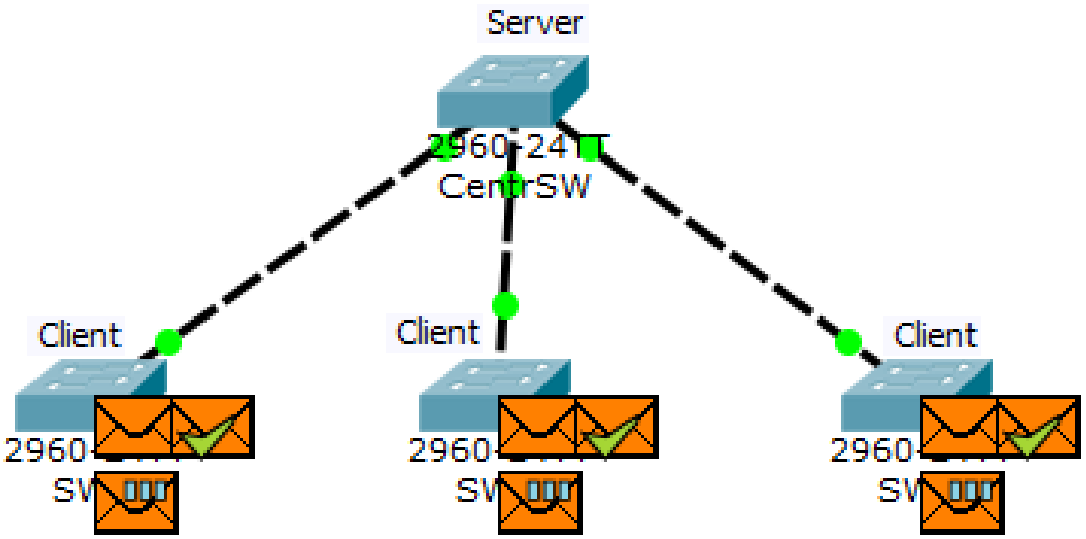
VTP VLAN Information



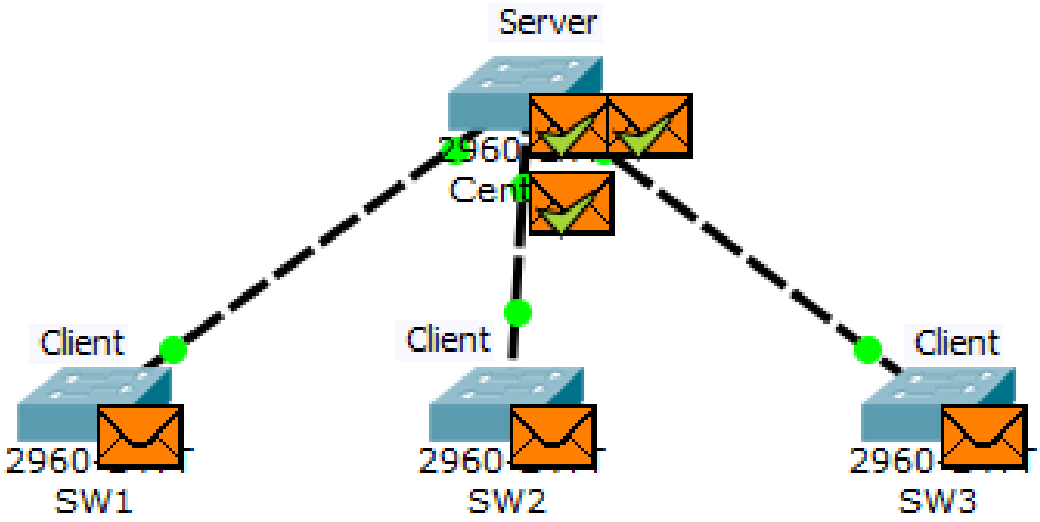
VTP VLAN Information



Думаю здесь понятно. Отдельный заголовок для каждого типа VLAN. Список настолько длинный, что не поместился в экран. Но они точно такие, за исключением названий. Заморачивать голову, что означает каждый код не буду. Да и в CPT они тут больше условность.
Смотрим, что происходит дальше.



Получают клиенты объявления. Видят, что номер ревизии выше, чем у них и синхронизируют базу. И отправляют сообщение серверу о том, что база VLAN-ов изменилась.



Принцип работы протокола VTP

Вот так в принципе работает протокол VTP. Но у него есть очень большие минусы. И минусы эти в плане безопасности. Объясню на примере этой же лабораторки. У нас есть центральный коммутатор, на котором создаются VLAN, а потом по мультикасту он их синхронизирует со всеми коммутаторами. В нашем случае он рассказывает про VLAN 20. Предлагаю еще раз глянуть на его конфигурацию.

```
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
```

И тут в сеть мы добавляем новый коммутатор. У него нет новых VLAN-ов, кроме стандартных и он не состоит ни в одном VTP-домене, но подкручен номер ревизии.

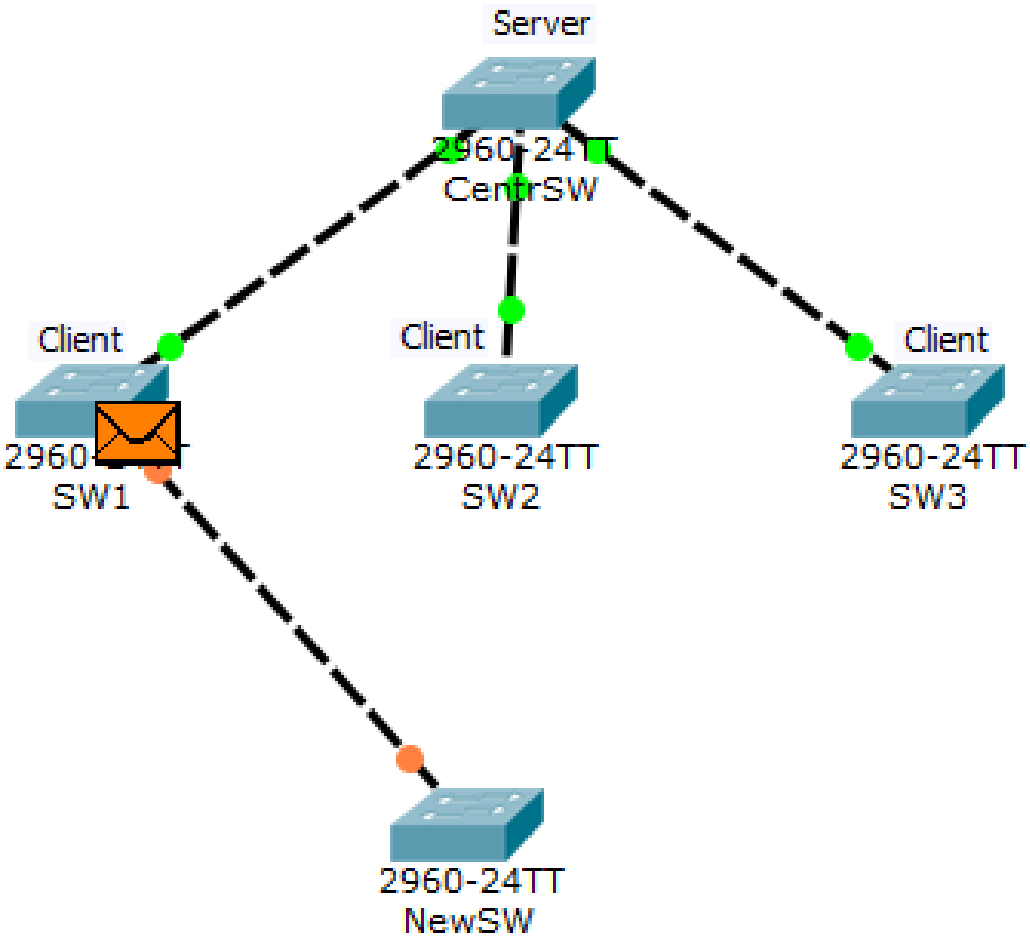
```
NewSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode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

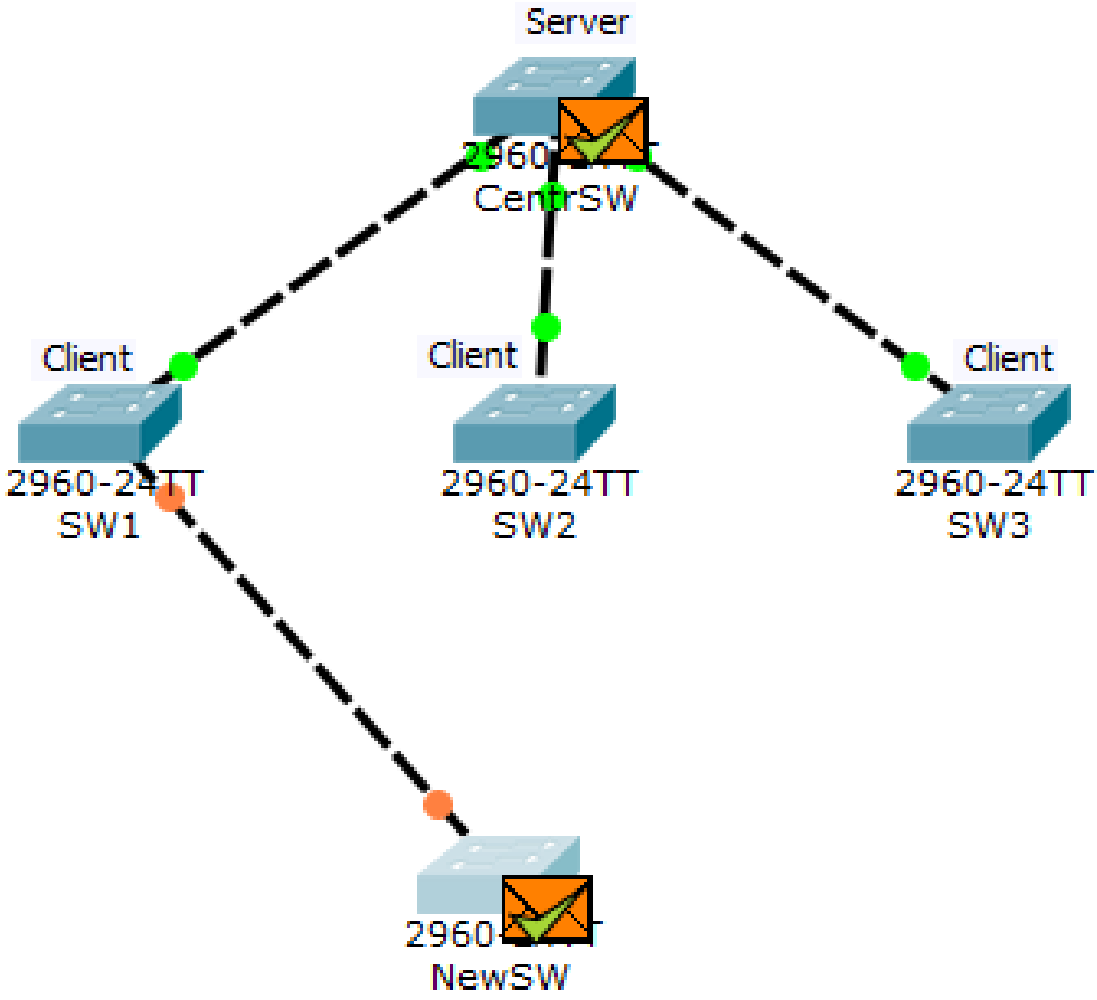
```
NewSW#show vlan

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
```

И перед тем как его воткнуть в сеть, переводим порт в 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
```

Теперь переключаю CPT в «Simulation Mode» и отфильтровываю все, кроме VTP. Подключаюсь и смотрю, что происходит.

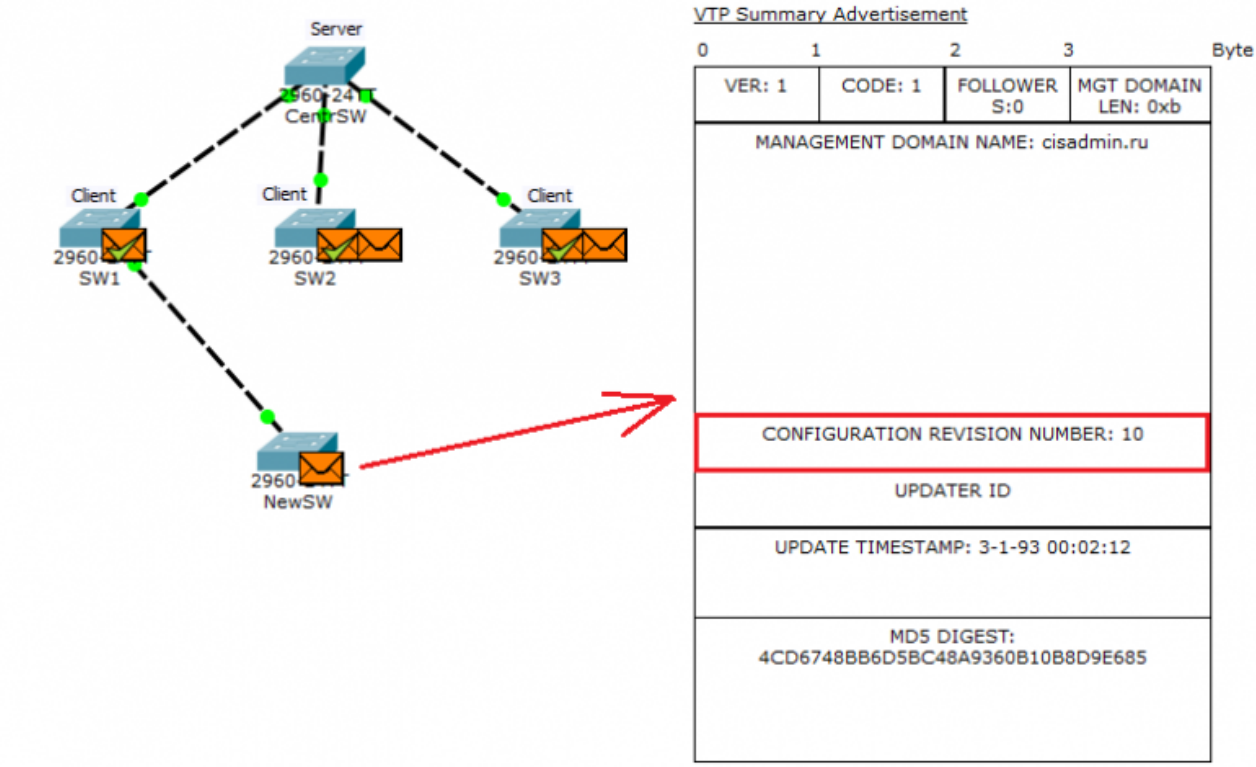

Server
2960-24TT
CentrSW
Client
Client
Client
2960-24TT
SW1
2960-24TT
SW2
2960-24TT
SW3
2960-24TT
NewSW



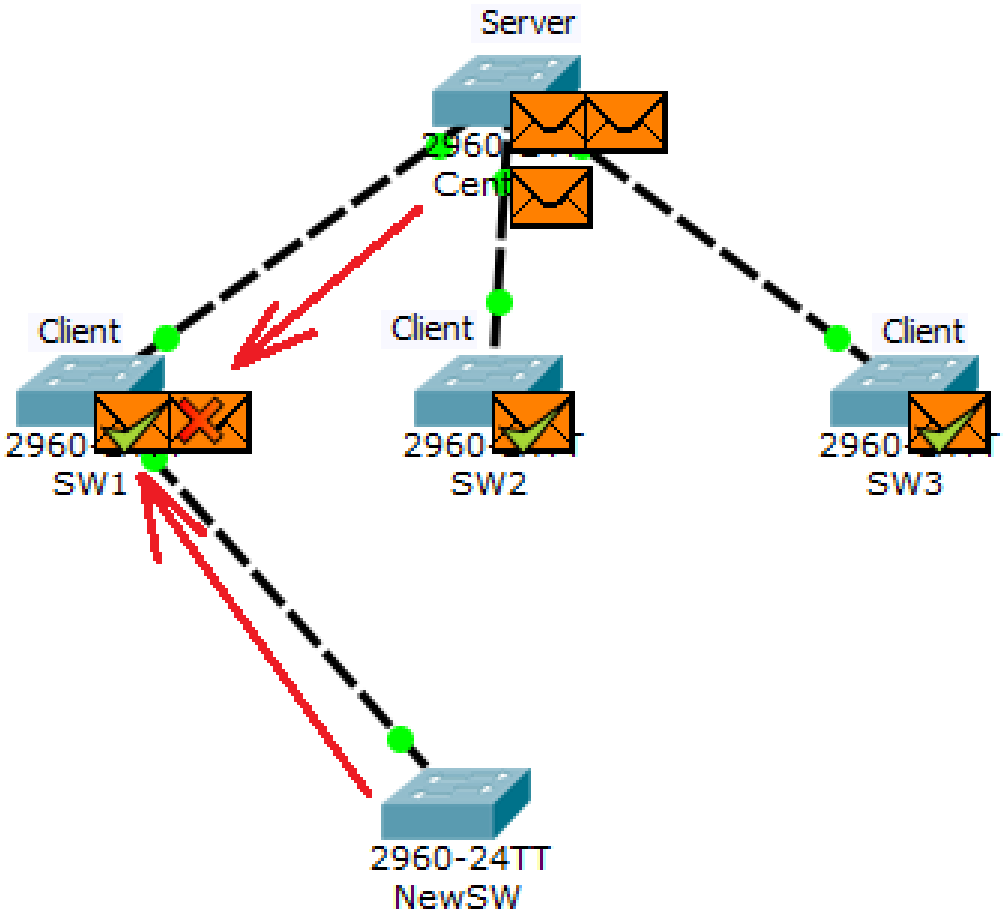
Через какое то время до NewSW доходит VTP сообщение, откуда он узнает, что в сети есть VTP-домен «cisadmin.ru». Так как он не состоял до этого в другом домене, он автоматически в него переходит. Проверим.

```
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.ru
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4C 0xD6 0x74 0x8B 0xB6 0xD5 0xBC 0x48
```

Теперь он в том же домене, но с номером ревизии выше. Он формирует VTP-сообщение, где рассказывает об этом.



Первым под раздачу попадет SW1.

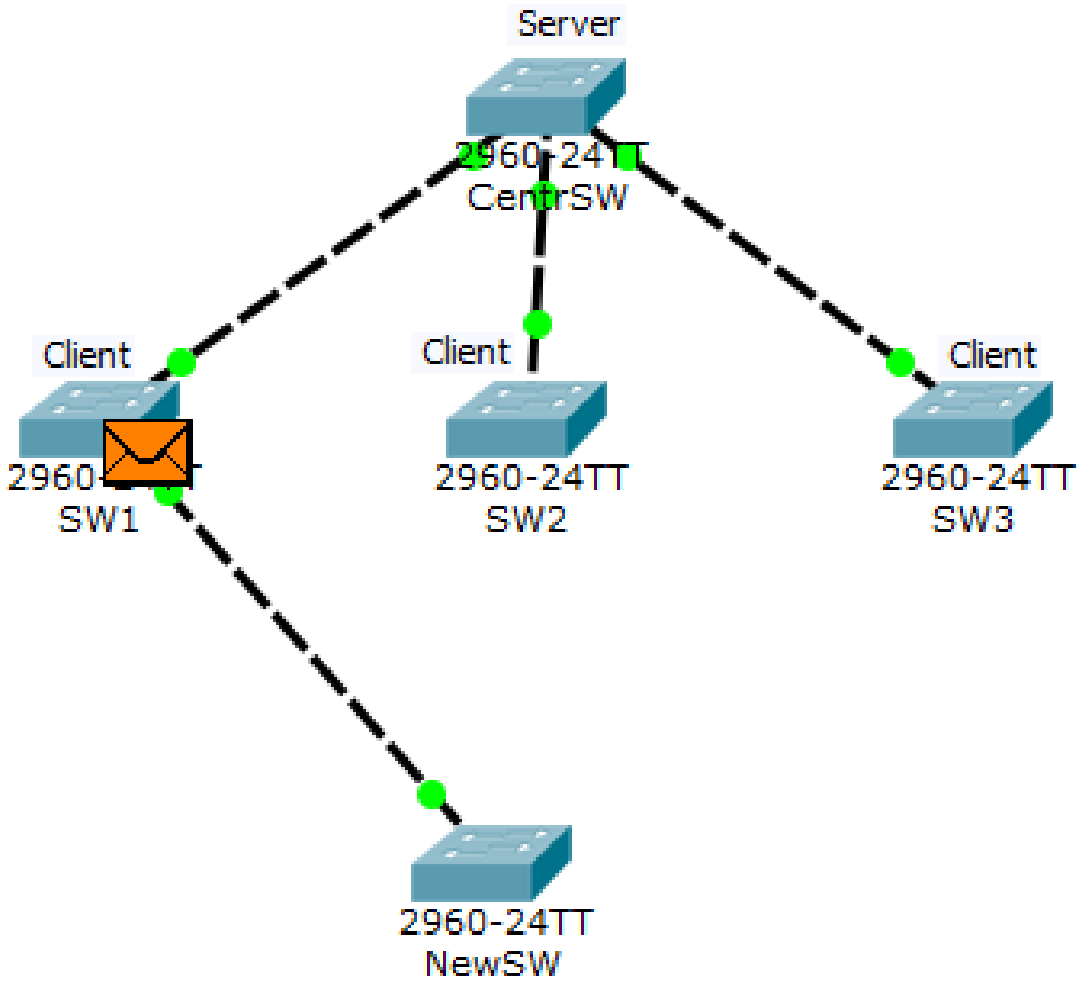


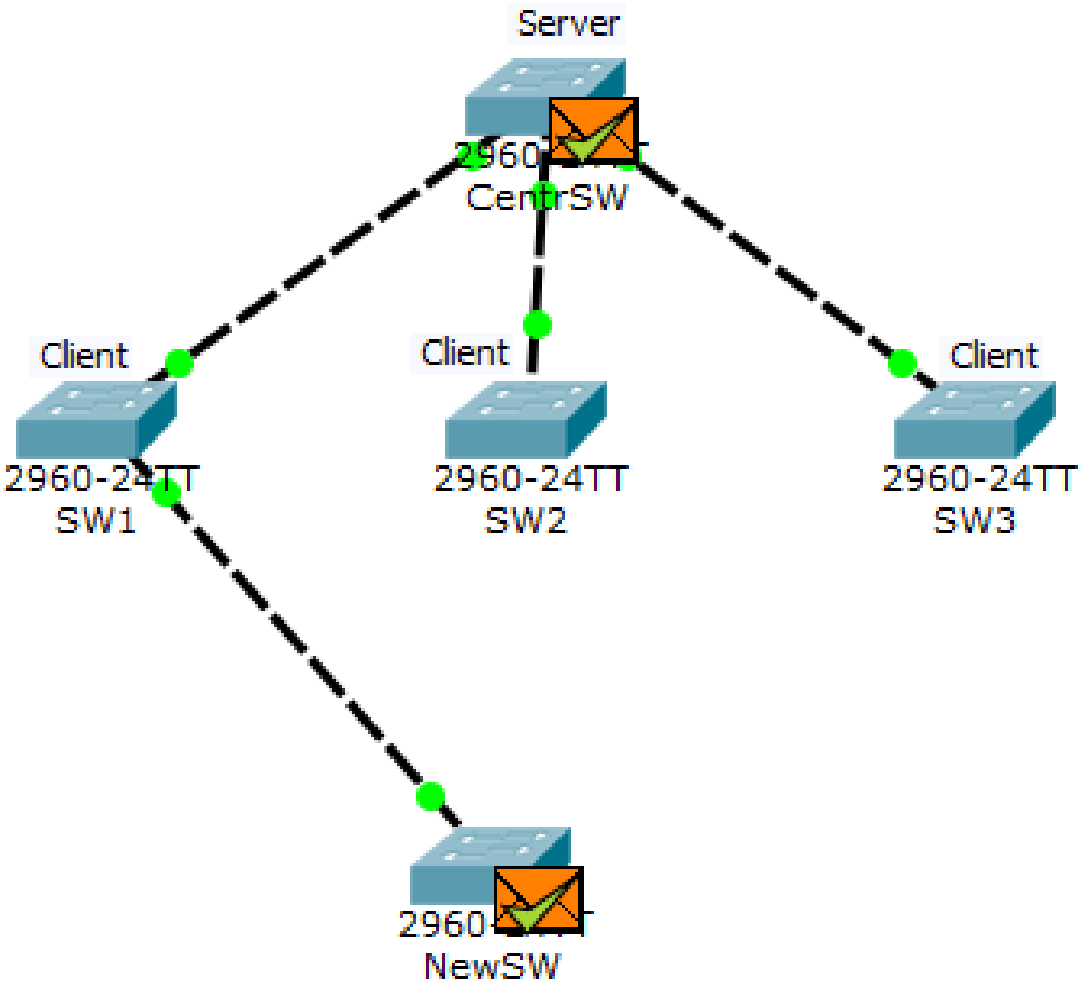
Заметьте, что на SW1 приходят сразу 2 VTP-сообщения (от NewSW и от CentrSW). В сообщении от NewSW он видит, что номер ревизии выше, чем его и синхронизирует свою базу. А вот сообщение от CentrSW для него уже устарело, и он отбрасывает его. Проверим, что изменилось на SW1.

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : cisadmin.ru
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4C 0xD6 0x74 0x8B 0xB6 0xD5 0xBC 0x48
```

```
SW1#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, 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
```

Обновился номер ревизии и, что самое интересное, база VLAN. Теперь она пустая. Смотрим дальше.





Обратите внимание. До сервера доходит VTP-сообщение, где номер ревизии выше, чем у него. Он понимает, что сеть изменилась и надо под нее подстроиться.
Проверим конфигурацию.

```
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.ru
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
```

Конфигурация центрального сервера изменилась и теперь он будет вещать именно ее.
А теперь представьте, что у нас не один VLAN, а сотни. Вот таким простым способом можно положить сеть. Конечно домен может быть запаролен и злоумышленнику будет тяжелее нанести вред. А представьте ситуацию, что у вас сломался коммутатор и срочно надо его заменить. Вы или ваш коллега бежите на склад за старым коммутатором и забываете проверить номер ревизии. Он оказывается выше чем у остальных. Что произойдет дальше, вы уже видели.

Поэтому я рекомендую не использовать этот протокол. Особенно в больших корпоративных сетях. Если используете VTP 3-ей версии, то смело переводите коммутаторы в режим «Off». Если же используется 2-ая версия, то переводите в режим «Transparent».

Кому интересно посмотреть это в виде анимации, открывайте спойлер.

Подключение коммутатора с большей ревизией

Для желающих поработать с этой лабораторкой, прикладываю ссылку.
Ну вот статья про VLAN подошла к концу. Если остались какие то вопросы, смело задавайте. Спасибо за прочтение.