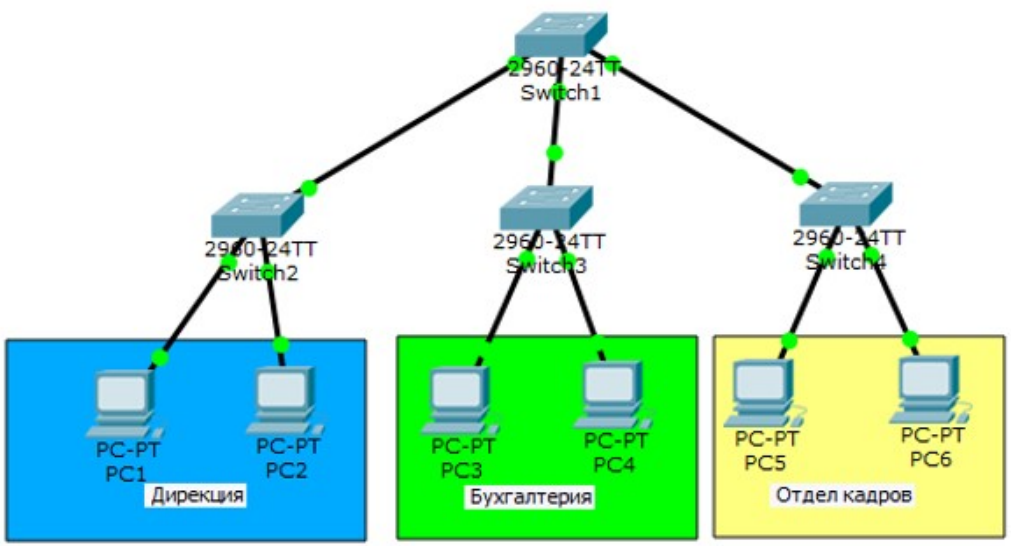
Белорусский государственный университет информатики и радиоэлектроники

ПРИНЦИПЫ СЕГМЕНТАЦИИ СЕТИ

Доцент кафедры «Защита информации»,
к.т.н., доцент *Белоусова Елена Сергеевна*

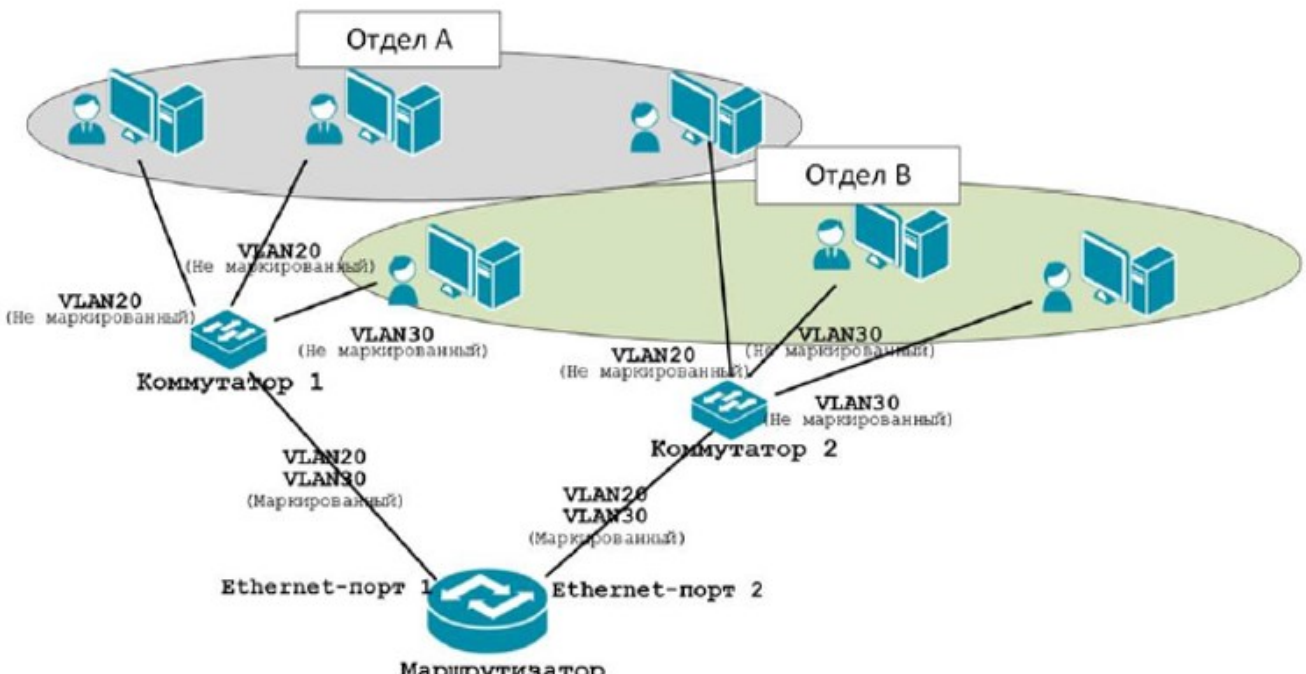
Технология VLAN

- VLAN (Virtual Local Area Network) – логическая ("виртуальная") локальная компьютерная сеть, представляет собой группу устройств с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.



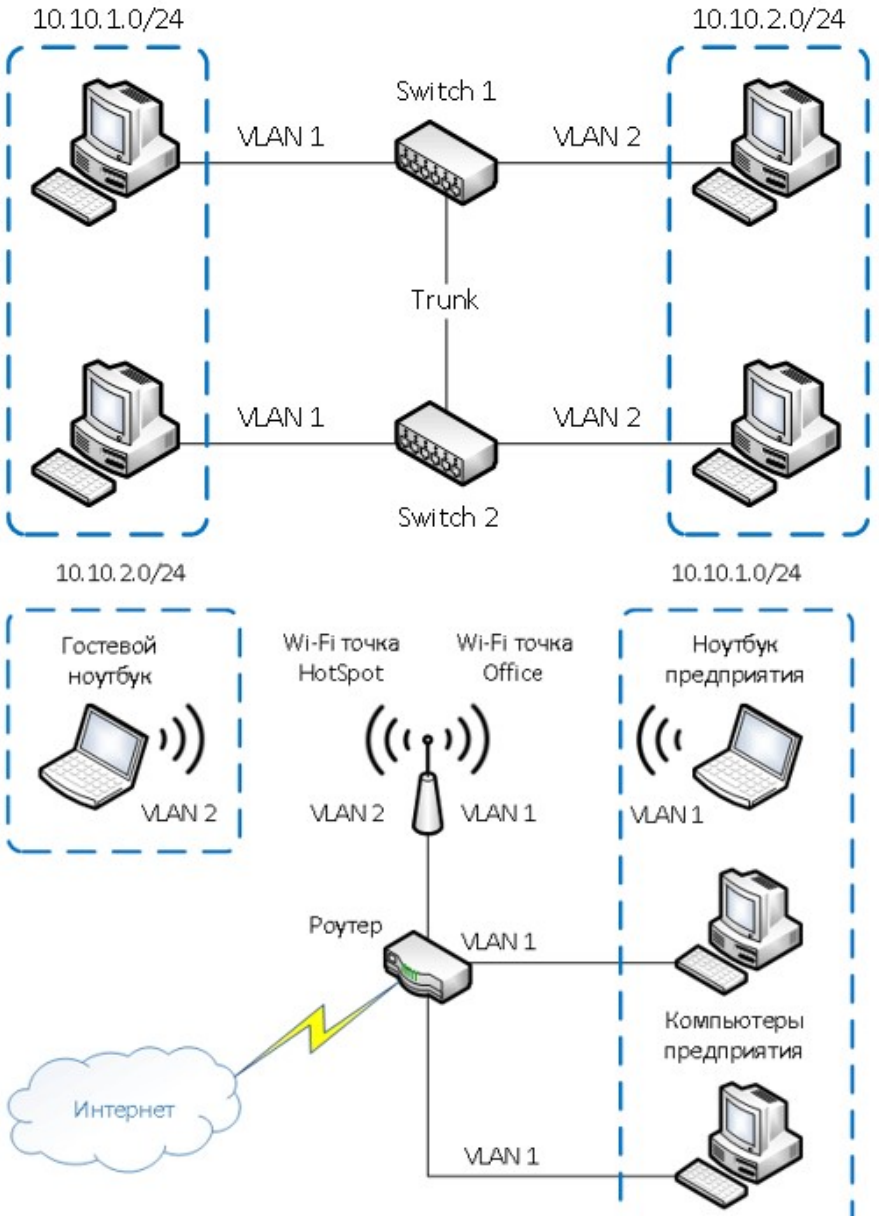
Технология VLAN

- Стандарт IEEE 802.1Q – стандарт, определяющий использование дополнительных полей кадра для хранения информации о принадлежности к VLAN при пересылке данного кадра по сети.



Примеры использования VLAN

- *Объединение в единую сеть компьютеров, подключенных к разным коммутаторам.*
- *Разделение в разные подсети компьютеров, подключенных к одному коммутатору.*
- *Разделение гостевой Wi-Fi сети и Wi-Fi сети предприятия.*

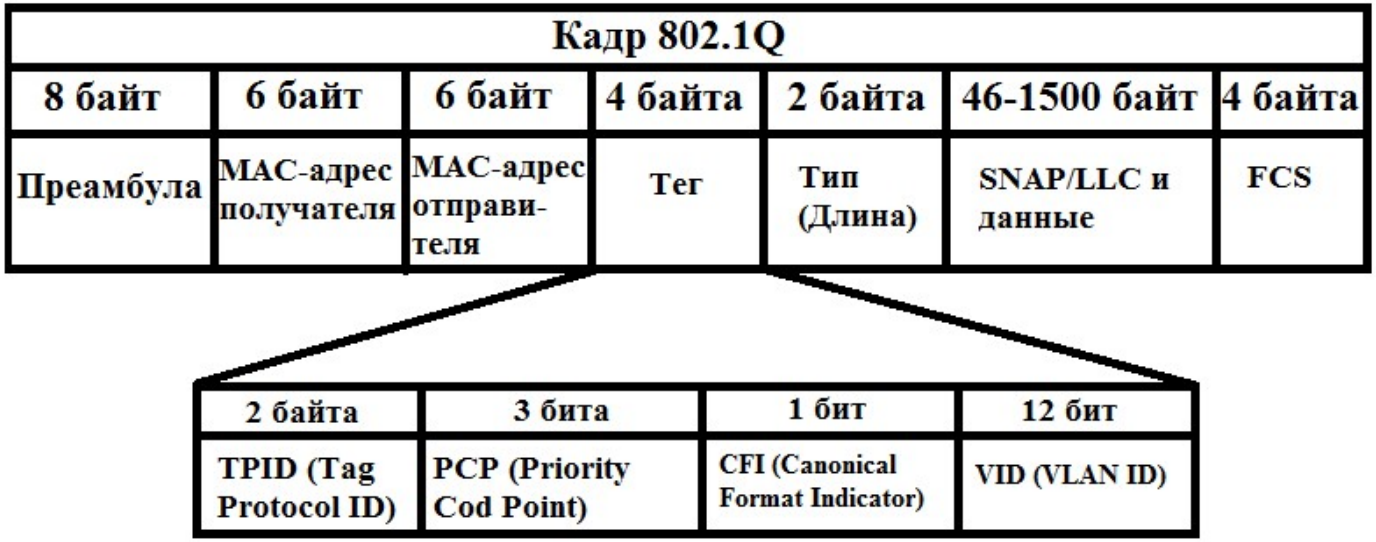


Формат Ethernet кадра по IEEE 802.3

7	1	6	6	2	46-1500	4
Преамбула	Начало разделителя кадра	Адрес источника	Адрес назначения	Длина	Заголовок и данные	Контрольная последовательность кадра

Формат Ethernet кадра по IEEE 802.1Q

8 байт	6 байт	6 байт	4 байта	2 байт	46-1500 байт	4 байт
Преамбу-ла	Адрес назначе-ния	Адрес источ-ника	Маркер 802.1Q	Тип	Данные	Контрольная последователь-ность кадра



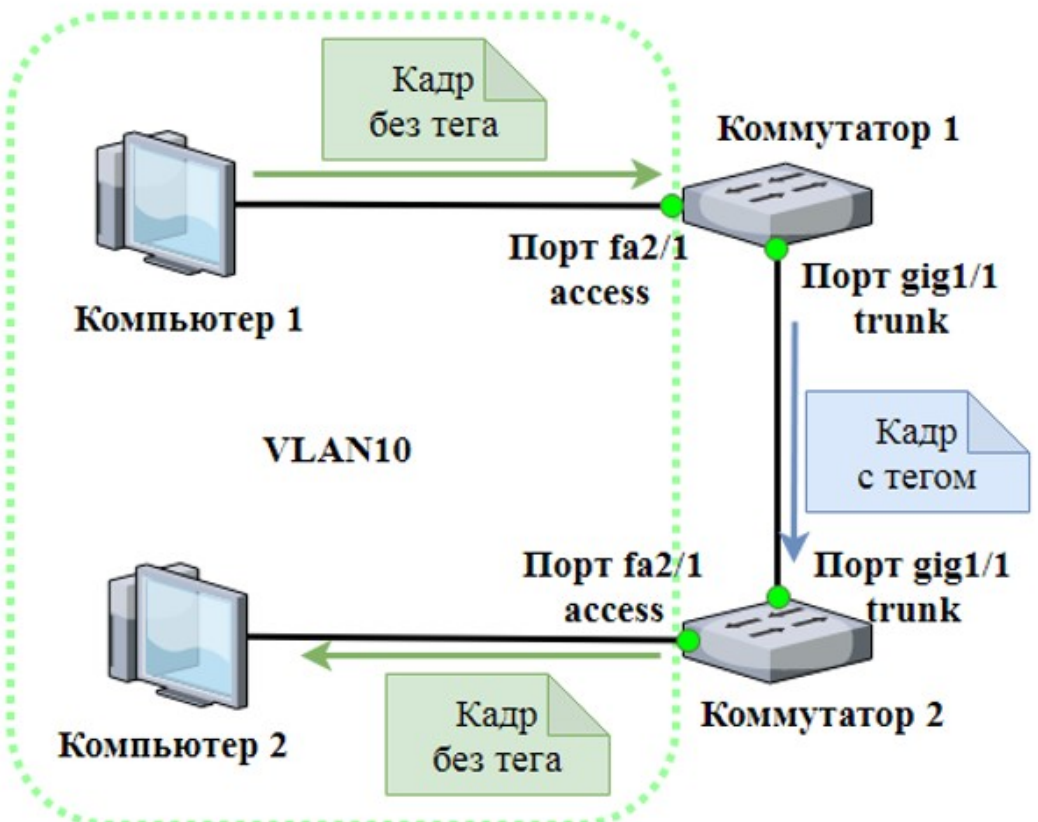
- TPID (Tag Protocol ID), идентификатор тегированного протокола (2 байта), для VLAN всегда равен 0x8100.
- PCP (Priority Code Point), значение приоритета (3 бита) используется для приоритезации трафика.
- CFI (Canonical Format Indicator), индикатор каноничного формата (1 бит), если равен 0, то это стандартный формат MAC-адреса.
- VID (VLAN ID), идентификатор VLAN (12 бит) показывает, в каком VLAN находится кадр.

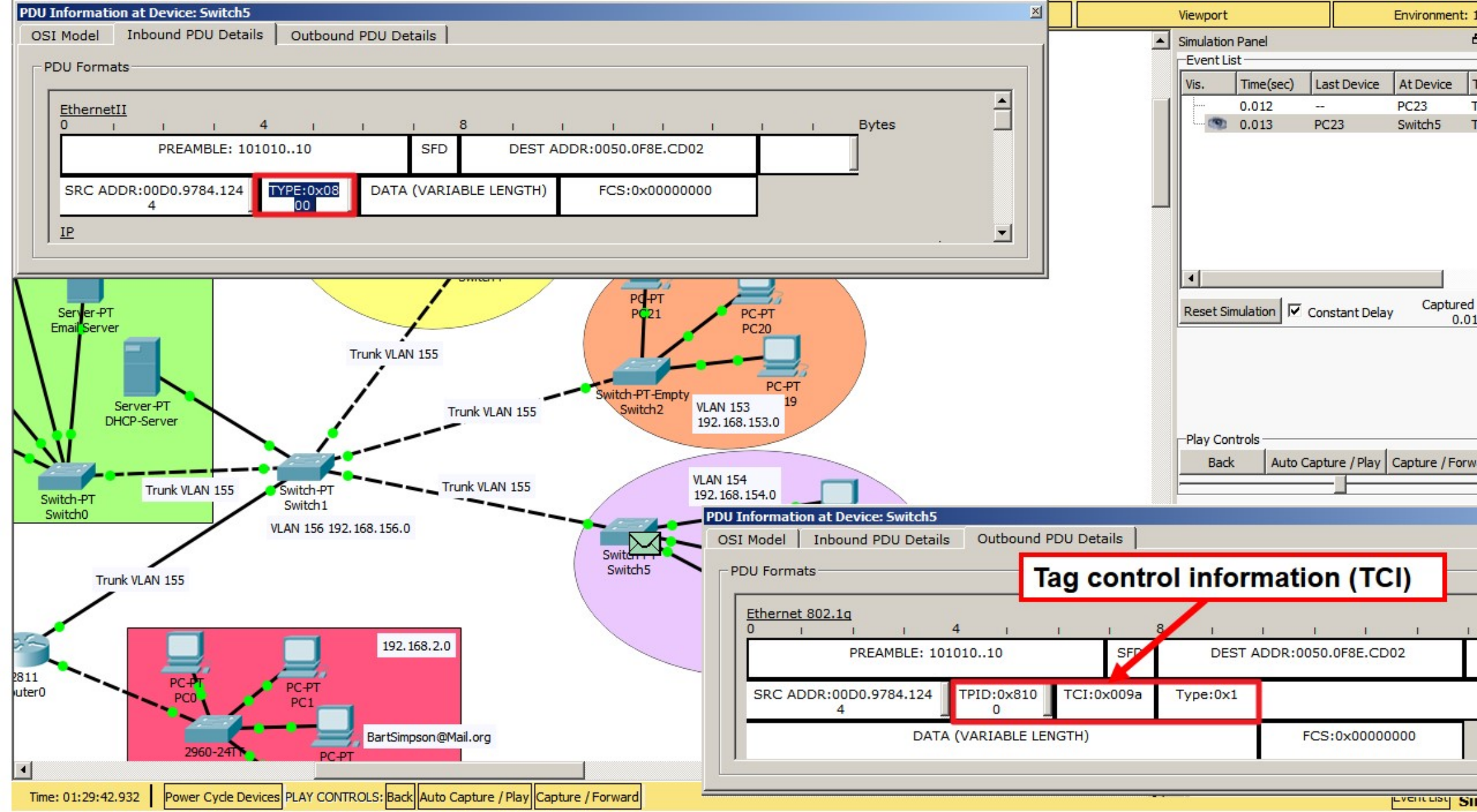
Процесс передачи кадра в сети с протоколом 802.1Q

1) При попадании кадра на порт коммутатора, в него добавляется заголовок с информацией о принадлежности к VLAN10.

2) Коммутатор1 пересылает тегированный кадр на коммутатор2 через trunk-порт.

3) Коммутатор2 получает кадр, смотрит в свою CAM-таблицу и отправляет кадр в соответствующий access-порт, заголовок снимается.




PDU Information at Device: Switch5
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
EthernetII
0
4
8
Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:0050.0F8E.CD02
SRC ADDR:00D0.9784.1244
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
Viewport
Environment:
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
At Device
0.012
--
PC23
0.013
PC23
Switch5
Reset Simulation
Constant Delay
Captured
0.01
Play Controls
Back
Auto Capture / Play
Capture / Forw
Server-PT
Email Server
Server-PT
DHCP-Server
Switch-PT
Switch0
Trunk VLAN 155
Switch-PT
Switch1
VLAN 156 192.168.156.0
Trunk VLAN 155
Trunk VLAN 155
Trunk VLAN 155
PC-PT
PC21
PC-PT
PC20
PC-PT
19
Switch-PT-Empty
Switch2
VLAN 153
192.168.153.0
VLAN 154
192.168.154.0
Switch5
192.168.2.0
PC-PT
PC0
PC-PT
PC1
2960-24TT
PC-PT
BartSimpson@Mail.org
2811
uter0
Time: 01:29:42.932
Power Cycle Devices
PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
PDU Information at Device: Switch5
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
Tag control information (TCI)
Ethernet 802.1q
0
4
8
PREAMBLE: 101010..10
SFD
DEST ADDR:0050.0F8E.CD02
SRC ADDR:00D0.9784.1244
TPID:0x8100
TCI:0x009a
Type:0x1
DATA (VARIABLE LENGTH)
FCS:0x00000000

Особенности передачи кадра в VLAN

- Пользователи ничего не знают о своей принадлежности к определенному VLAN и работают с нетегированными кадрами, заголовок появляется только при прохождении кадра через access-порт;
- Порт может быть нетегирован (access) только в одном VLAN;
- Через тегированный (trunk) порт можно передавать кадры, принадлежащие к разным VLAN.
- Существует так называемый native VLAN – при попадании на trunk-порт кадра без тега, он автоматически будет причислен к native VLAN. Как правило native VLAN по умолчанию считается VLAN1.

Процесс настройки VLAN на коммутаторах

1. Создать все сети VLAN и указать их имена

```
Switch(config)#vlan номер
Switch(config-vlan)#name имя
Switch(config-vlan)#exit
```

2. Назначить в созданные VLAN-сети физические порты коммутатора

```
Switch(config)#interface FastEthernet 2/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 151
Switch(config-if)#exit
```

Процесс настройки VLAN на коммутаторах

3. Настройка транкового порта

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 155
Switch(config-if)#exit
```

show vlan

```
Switch#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
10   direst                              active
20   bux                                 active    Fa0/2
30   kadri                               active    Fa0/3
40   server                              active
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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     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
------------------------------------------------------------------------------
```

show interfaces trunk

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      50
Fa0/2       on           802.1q         trunking      50
Fa0/3       on           802.1q         trunking      50

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40
Fa0/2       1,10,20,30,40
Fa0/3       1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40
Fa0/2       1,10,20,30,40
Fa0/3       1,10,20,30,40
```

Процесс настройки VLAN на маршрутизаторе

1. настроить sub-интерфейсы на порту, соединяющем маршрутизатор и коммутатор

```
Router (config)#interface fa0/1
Router (config-if)#no shutdown
Router (config-if)#no ip address
```

2. включить инкапсуляцию по протоколу IEEE 802.1Q.

3. Назначить в созданные VLAN-сети физические порты коммутатора

```
Router (config)# interface fa0/1.150
Router(config-subif)#encapsulation dot1q 150
Router(config-subif)#ip address 192.168.150.1 255.255.255.0
Router(config-subif)#no shutdown
```

show ip route

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0.10
C    192.168.20.0/24 is directly connected, FastEthernet0/0.20
C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
C    192.168.40.0/24 is directly connected, FastEthernet0/0.40
```

Настройка DHCP на маршрутизаторе

1. Настройка пула ip-адресов

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# dns-server 192.168.20.200
```

2. Исключения раздачи ip-адреса маршрутизатора

```
Router(config)#ip dhcp excluded-address 192.168.20.1
```

Проверка работы DHCP на маршрутизаторе

```
Router#sh ip dhcp binding
IP address       Client-ID/                Lease expiration        Type
                 Hardware address
192.168.154.2    0000.0CB4.6D65             --                     Automatic
192.168.154.3    0006.2AD4.66A9             --                     Automatic
192.168.154.4    00D0.9784.1244             --                     Automatic
192.168.2.6      0060.708C.3D2C             --                     Automatic
192.168.2.2      00D0.BAE5.28EB             --                     Automatic
192.168.2.4      0001.645A.C1C0             --                     Automatic
192.168.2.8      0060.3E5A.3644             --                     Automatic
```