

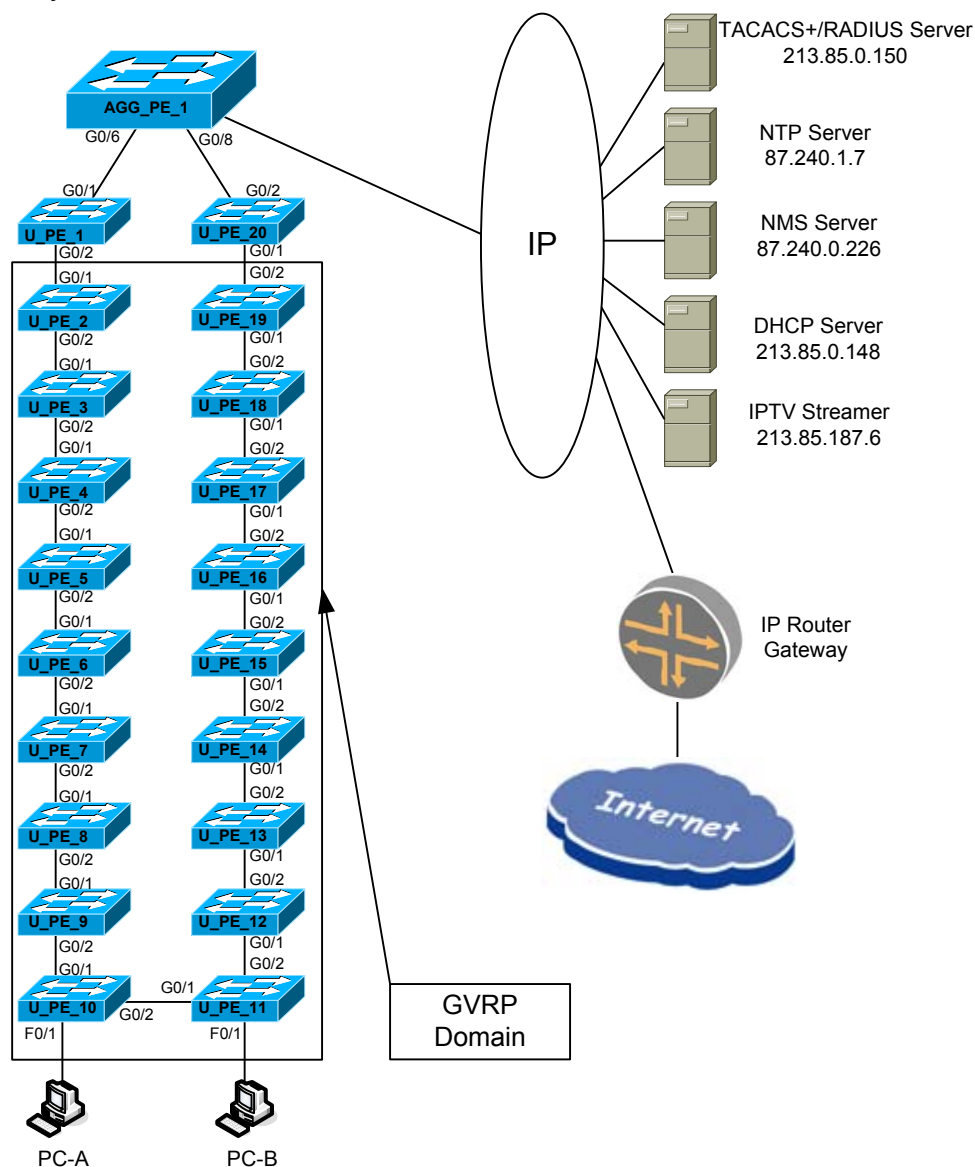
# **Тестирование коммутаторов ZES-2026C**

## Содержание:

1	Состав и схема испытательного стенда .....	3
2	Тестирование .....	5
2.1	Тест 1. Проверка работы STP .....	5
2.2	Тест 2. Проверка GVRP и IP-связности. ....	7
2.3	Тест 3. (S)NTP.....	10
2.4	Тест 4. Аутентификация по RADIUS.....	11
2.5	Тест 5. Работа syslog сервиса. ....	12
2.6	Тест 6. Работа SNMP.....	13
2.7	Тест 7. Безопасность. Переполнение MAC-таблицы.....	13
2.8	Тест 8. Безопасность. Ограничения кол-ва MAC на порту.....	15
2.9	Тест 9. Производительность и QoS. ....	15
2.10	Тест 10. Multicast IPTV.....	19
2.11	Тест 11. Списки доступа для IGMP-запросов. ....	20
2.12	Тест 12. Безопасность STP на портах доступа. ....	21
2.13	Тест 13. Поддержка функций jumbo frames и QinQ.....	23
2.14	Тест 14. Большое количество telnet сессий.....	23
2.15	Тест 15. Проверка функционала TDR.....	24
3	Сведения об оборудовании .....	25
4	Результаты тестирования.....	26

# 1 Состав и схема испытательного стенда

Рисунок 1. Схема испытательного стенда.



Стенд состоит из 20 испытуемых коммутаторов доступа ZES-2026C и 1 коммутатора агрегации. В качестве коммутатора агрегации используются и Cisco 3560.

Испытуемые коммутаторы доступа соединены в кольцо интерфейсами GE в tagged режиме (trunk).

В кольце настроен MSTP, таким образом, чтобы заблокированный линк находился между U\_PE\_10 и U\_PE\_11.

На корневом коммутаторе агрегации и ближайших к нему двух кольцевых (edge-коммутаторы), и только на них, все VLAN настроены статически. Между edge-коммутаторами и остальными включен GVRP.

К портам FastEthernet 0/1 коммутаторов U\_PE\_10 и U\_PE\_11 подключены PC-A и PC-B соответственно.

На всех коммутаторах кроме корневого настроен MVR.

В кольце настраиваются следующие VLAN:

- MC-VLAN – VLAN 222
- MNG-VLAN – VLAN 3
- C-VLAN - с номерами от 1100 до 1102.

На тестовые PC-A и PC-B назначаются адреса из подсети для клиентов.

Тестовые компьютеры:

- тестовый ПК – имя «PC-A», ip-адрес 192.168.100.1 , VLAN №1100
- тестовый ПК – имя «PC-B», ip-адрес 192.168.100.2 , VLAN №1100

Интерфейсы управления коммутаторов помещаются в MNG-VLAN и им назначаются IP-адреса из подсети управления.

При начальном тестировании в лаборатории вендора серверам назначаются «местные» IP адреса по выбору исполнителя.

NTP, NMS и AAA сервера доступны через MNG-VLAN

DHCP сервер и маршрутизатор/шлюз доступны через C-VLAN

IPTV сервер доступен через MC-VLAN

В качестве инструментария использовать аппаратные генераторы и анализаторы трафика, либо, в некоторых тестах, ПО их заменяющее.

## 2 Тестирование

### 2.1 Тест 1. Проверка работы STP.

#### Цель теста:

Проверить работу протокола STP на коммутаторах.

#### Описание теста:

- На коммутаторах кольца доступа настраивается MSTP и/или RSTP, в зависимости от типа корневого коммутатора и возможностей испытываемых коммутаторов.

```
U_PE_9(config)#spanning-tree
```

```
MSTP is starting now, please wait.....
```

```
MSTP is enabled successfully.
```

```
U_PE_9(config)#
```

- Коммутатор AGG\_PE\_1 является корневым для всего кольца.
- Представить состояние STP на каждом коммутаторе кольца в таблице.
- Разорвать кольцо между корневым коммутатором и коммутатором доступа в который включен тестовый ПК и заполнить таблицу повторно.
- Восстановить соединение и заполнить таблицу состояния STP.

#### Результаты теста:

##### Состояние линков до разрыва кольца

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG_PE_1	00:19:06:49:0d:00	16384	FWD DSGN	FWD DSGN
U_PE_1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U_PE_2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U_PE_3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U_PE_4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U_PE_5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U_PE_6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U_PE_7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U_PE_8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U_PE_9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U_PE_10	00:1a:81:00:1b:13	32768	FWD ROOT	BLK ALTR
U_PE_11	00:1a:81:00:1b:01	32768	FWD DSGN	FWD ROOT
U_PE_12	00:1a:81:00:1a:ff	32768	FWD DSGN	FWD ROOT
U_PE_13	00:1a:81:00:1a:fd	32768	FWD DSGN	FWD ROOT
U_PE_14	00:1a:81:00:1a:fb	32768	FWD DSGN	FWD ROOT
U_PE_15	00:1a:81:00:1a:f9	32768	FWD DSGN	FWD ROOT
U_PE_16	00:1a:81:00:1b:09	32768	FWD DSGN	FWD ROOT
U_PE_17	00:1a:81:00:1b:07	32768	FWD DSGN	FWD ROOT
U_PE_18	00:1a:81:00:1b:05	32768	FWD DSGN	FWD ROOT
U_PE_19	00:1a:81:00:1b:03	32768	FWD DSGN	FWD ROOT
U_PE_20	00:1a:81:00:1a:ef	32768	FWD DSGN	FWD ROOT

**Состояние линков после разрыва кольца между коммутатором 19 и 20.**

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG PE 1	00:19:06:49:0d:00	16384	FWD DSGN	FWD DSGN
U PE 1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U PE 2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U PE 3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U PE 4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U PE 5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U PE 6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U PE 7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U PE 8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U PE 9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U PE 10	00:1a:81:00:1b:13	32768	FWD ROOT	FWD DSGN
U PE 11	00:1a:81:00:1b:01	32768	FWD ROOT	FWD DSGN
U PE 12	00:1a:81:00:1a:ff	32768	FWD ROOT	FWD DSGN
U PE 13	00:1a:81:00:1a:fd	32768	FWD ROOT	FWD DSGN
U PE 14	00:1a:81:00:1a:fb	32768	FWD ROOT	FWD DSGN
U PE 15	00:1a:81:00:1a:f9	32768	FWD ROOT	FWD DSGN
U PE 16	00:1a:81:00:1b:09	32768	FWD ROOT	FWD DSGN
U PE 17	00:1a:81:00:1b:07	32768	FWD ROOT	FWD DSGN
U PE 18	00:1a:81:00:1b:05	32768	FWD ROOT	FWD DSGN
U PE 19	00:1a:81:00:1b:03	32768	FWD ROOT	Выключен
U PE 20	00:1a:81:00:1a:ef	32768	Выключен	FWD ROOT

**Состояние линков после восстановления кольца:**

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG PE 1	00:19:06:49:0d:00	16384	FWD DSGN	FWD DSGN
U PE 1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U PE 2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U PE 3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U PE 4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U PE 5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U PE 6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U PE 7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U PE 8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U PE 9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U PE 10	00:1a:81:00:1b:13	32768	FWD ROOT	BLK ALTR
U PE 11	00:1a:81:00:1b:01	32768	FWD DSGN	FWD ROOT
U PE 12	00:1a:81:00:1a:ff	32768	FWD DSGN	FWD ROOT
U PE 13	00:1a:81:00:1a:fd	32768	FWD DSGN	FWD ROOT
U PE 14	00:1a:81:00:1a:fb	32768	FWD DSGN	FWD ROOT
U PE 15	00:1a:81:00:1a:f9	32768	FWD DSGN	FWD ROOT
U PE 16	00:1a:81:00:1b:09	32768	FWD DSGN	FWD ROOT
U PE 17	00:1a:81:00:1b:07	32768	FWD DSGN	FWD ROOT
U PE 18	00:1a:81:00:1b:05	32768	FWD DSGN	FWD ROOT
U PE 19	00:1a:81:00:1b:03	32768	FWD DSGN	FWD ROOT
U PE 20	00:1a:81:00:1a:ef	32768	FWD DSGN	FWD ROOT

## 2.2 Тест 2. Проверка GVRP и IP-связности.

**Цель теста:** Проверить IP-связанность при обрыве кольца и восстановлении. Проверить распространение информации о VLAN по GVRP.

**Описание теста:**

**Часть 1:**

- Назначить порт F0/1 коммутатора доступа U\_PE\_10 в C-VLAN-A номер 1100. К порту подключить PC\_A.
- Назначить порт F0/1 коммутатора доступа U\_PE\_11 в C-VLAN-A номер 1100. К порту подключить PC\_B.
- Утилитой iperf проверить IP-связанность между PC\_A и PC\_B.

Связь между PC\_A и PC\_B есть.

- Зафиксировать состояние протокола STP на коммутаторах кольца аналогично тесту 2.1 и занести в таблицу.

**Состояние линков до разрыва кольца**

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG_PE_1	00:19:06:49:0d:00	16384	FWD DSGN	FWD DSGN
U PE 1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U PE 2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U PE 3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U PE 4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U PE 5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U PE 6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U PE 7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U PE 8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U PE 9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U PE 10	00:1a:81:00:1b:13	32768	FWD ROOT	BLK ALTR
U PE 11	00:1a:81:00:1b:01	32768	FWD DSGN	FWD ROOT
U PE 12	00:1a:81:00:1a:ff	32768	FWD DSGN	FWD ROOT
U PE 13	00:1a:81:00:1a:fd	32768	FWD DSGN	FWD ROOT
U PE 14	00:1a:81:00:1a:fb	32768	FWD DSGN	FWD ROOT
U PE 15	00:1a:81:00:1a:f9	32768	FWD DSGN	FWD ROOT
U PE 16	00:1a:81:00:1b:09	32768	FWD DSGN	FWD ROOT
U PE 17	00:1a:81:00:1b:07	32768	FWD DSGN	FWD ROOT
U PE 18	00:1a:81:00:1b:05	32768	FWD DSGN	FWD ROOT
U PE 19	00:1a:81:00:1b:03	32768	FWD DSGN	FWD ROOT
U PE 20	00:1a:81:00:1a:ef	32768	FWD DSGN	FWD ROOT

- Разорвать соединение между коммутаторами AGG\_PE и U\_PE\_20
- Утилитой iperf продолжать проверять IP-связанность между PC\_A и PC\_B.

Связь между PC\_A и PC\_B не прерывалась, время передачи пакетов с ошибками не привисило 1 с.

- Зафиксировать состояние протокола STP на коммутаторах кольца.

**Состояние линков после разрыва кольца между коммутатором AGG\_PE 1 и 20.**

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG PE 1	00:19:06:49:0d:00	16384	FWD DSGN	выключен
U PE 1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U PE 2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U PE 3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U PE 4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U PE 5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U PE 6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U PE 7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U PE 8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U PE 9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U PE 10	00:1a:81:00:1b:13	32768	FWD ROOT	FWD DSGN
U PE 11	00:1a:81:00:1b:01	32768	FWD ROOT	FWD DSGN
U PE 12	00:1a:81:00:1a:ff	32768	FWD ROOT	FWD DSGN
U PE 13	00:1a:81:00:1a:fd	32768	FWD ROOT	FWD DSGN
U PE 14	00:1a:81:00:1a:fb	32768	FWD ROOT	FWD DSGN
U PE 15	00:1a:81:00:1a:f9	32768	FWD ROOT	FWD DSGN
U PE 16	00:1a:81:00:1b:09	32768	FWD ROOT	FWD DSGN
U PE 17	00:1a:81:00:1b:07	32768	FWD ROOT	FWD DSGN
U PE 18	00:1a:81:00:1b:05	32768	FWD ROOT	FWD DSGN
U PE 19	00:1a:81:00:1b:03	32768	FWD ROOT	FWD DSGN
U PE 20	00:1a:81:00:1a:ef	32768	FWD ROOT	выключен

- Восстановить соединение между коммутаторами AGG\_PE и U\_PE\_1
- Утилитой iperf продолжать проверять IP-связанность между PC\_A и PC\_B.

Связь между PC\_A и PC\_B не прерывалась, время передачи пакетов с ошибками не привисило 1 с.

- Зафиксировать состояние протокола STP на коммутаторах кольца.

**Состояние линков после восстановления кольца:**

Имя коммутатора	MAC-адрес	priority	Роль Eth 0/0/25	Роль Eth 0/0/26
AGG PE 1	00:19:06:49:0d:00	16384	FWD DSGN	FWD DSGN
U PE 1	00:1a:81:00:1a:ed	32768	FWD ROOT	FWD DSGN
U PE 2	00:1a:81:00:1a:f1	32768	FWD ROOT	FWD DSGN
U PE 3	00:1a:81:00:1a:f3	32768	FWD ROOT	FWD DSGN
U PE 4	00:1a:81:00:1a:f5	32768	FWD ROOT	FWD DSGN
U PE 5	00:1a:81:00:1a:f7	32768	FWD ROOT	FWD DSGN
U PE 6	00:1a:81:00:1b:0b	32768	FWD ROOT	FWD DSGN
U PE 7	00:1a:81:00:1b:0d	32768	FWD ROOT	FWD DSGN
U PE 8	00:1a:81:00:1b:0f	32768	FWD ROOT	FWD DSGN
U PE 9	00:1a:81:00:1b:11	32768	FWD ROOT	FWD DSGN
U PE 10	00:1a:81:00:1b:13	32768	FWD ROOT	BLK ALTR
U PE 11	00:1a:81:00:1b:01	32768	FWD DSGN	FWD ROOT
U PE 12	00:1a:81:00:1a:ff	32768	FWD DSGN	FWD ROOT
U PE 13	00:1a:81:00:1a:fd	32768	FWD DSGN	FWD ROOT
U PE 14	00:1a:81:00:1a:fb	32768	FWD DSGN	FWD ROOT
U PE 15	00:1a:81:00:1a:f9	32768	FWD DSGN	FWD ROOT
U PE 16	00:1a:81:00:1b:09	32768	FWD DSGN	FWD ROOT
U PE 17	00:1a:81:00:1b:07	32768	FWD DSGN	FWD ROOT
U PE 18	00:1a:81:00:1b:05	32768	FWD DSGN	FWD ROOT
U PE 19	00:1a:81:00:1b:03	32768	FWD DSGN	FWD ROOT
U PE 20	00:1a:81:00:1a:ef	32768	FWD DSGN	FWD ROOT

- Указать время, в течение которого связанность отсутствует для каждого из этапов

Для каждого этапа связь между PC\_A и PC\_B не прерывалась, время передачи пакетов с ошибками не превысило 1 с.

### **Часть 2:**

- Для PC\_A получить ip-адрес по DHCP.

PC\_A получил IP-адрес по DHCP

- С помощью утилиты PING постоянно проверять IP-связность с шлюзом по умолчанию.
  - Разорвать кольцо физически вынув кабель из порта G0/1 коммутатора U\_PE\_1
  - Через 1 минуту восстановить соединение.
  - Зафиксировать показатели утилиты PING.
  - Указать время, в течение которого связанность отсутствует
- Связь между PC\_A шлюзом по умолчанию не прерывалась, при изменении топологии терялся один пакет ICMP.

### **Часть 3:**

- Для PC\_A назначить ip-адрес статически, из одной подсети со шлюзом.
- С помощью утилиты PING постоянно проверять IP-связность с шлюзом по умолчанию.
- Зафиксировать состояние GVRP для всех 20 коммутаторов кольца

Таблица VLAN на всех коммутаторах одинаковая.

- Создать на корневом коммутаторе и edge-коммутаторах новый VLAN, ранее в тестах не использованный (напр. 2100)
  - Переназначить шлюз по умолчанию в другой VLAN (2100)
  - Наблюдать потерю IP-связности ПК со шлюзом
  - Переназначить PC\_A в другой VLAN (напр. 2100)
  - Наблюдать восстановление IP-связности ПК со шлюзом
- Утилита PING зафиксировала 13 сообщений “Request timed out”, после этого связь восстановилась.

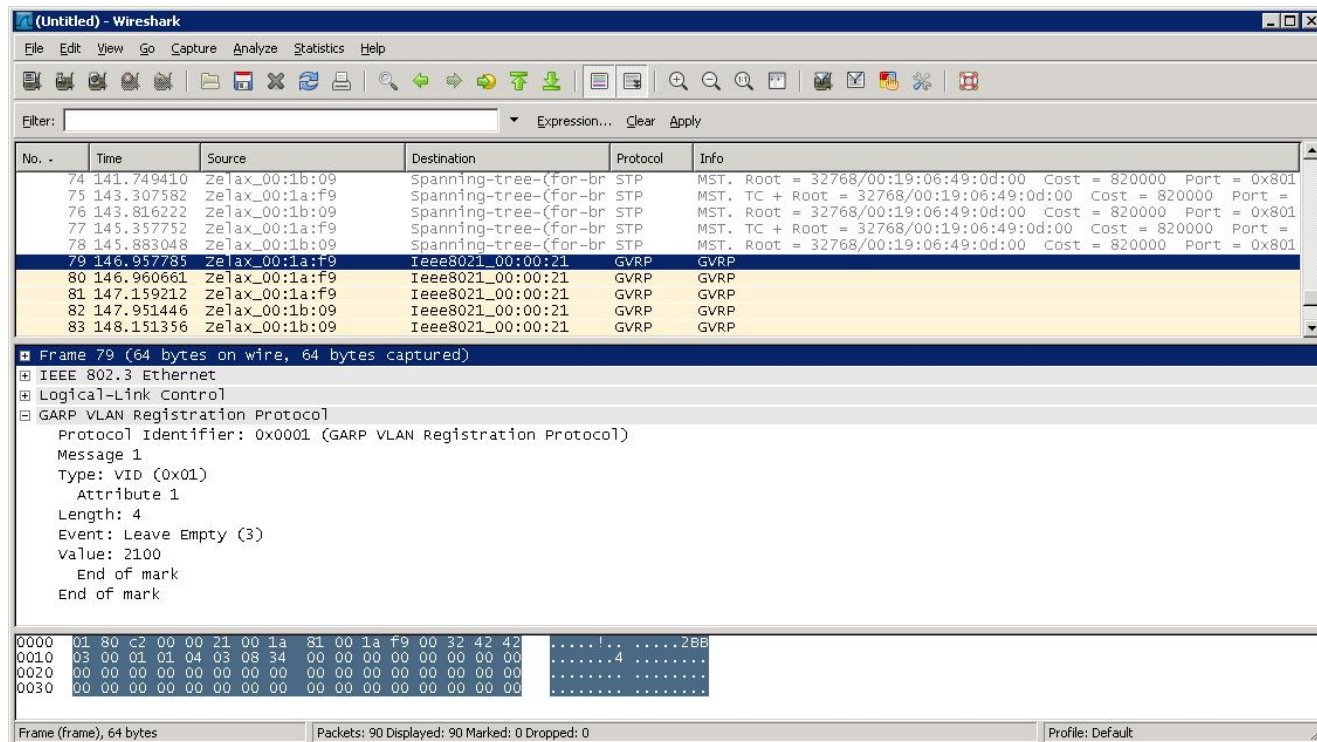
- Зафиксировать состояние GVRP для всех 20 коммутаторов кольца

В таблицах VLAN на всех коммутаторах появилась Dynamic VLAN 2100

- Разорвать кольцо, физически вынув кабель из порта G0/1 коммутатора U\_PE\_1
- Наблюдать восстановление IP-связности ПК со шлюзом
- Зафиксировать состояние GVRP для всех 20 коммутаторов кольца

В таблицах VLAN на всех коммутаторах появилась Dynamic VLAN 2100

- Через 1 минуту восстановить соединение.
- Наблюдать восстановление IP-связности ПК со шлюзом
- Зафиксировать показатели утилиты PING.
- Предоставить логи захваченного анализатором трафика GVRP



- Указать время, в течение которого связанность отсутствует для каждого из этапов. При добавлении нового VLAN утилита PING показала 13 сообщений “Request timed out”. При разрыве и восстановлении кольца утилита PING показала одно сообщение “Request timed out”.

## 2.3 Тест 3. (S)NTP.

**Цель теста:** Проверка работы протокола (S)NTP.

**Результат теста:**

Конфигурационный файл SNTP.cfg. Настроить автоматический переход на летнее и зимнее время нельзя. Максимальный оффсет -12..+12.

- Процесс синхронизации и изменения времени. Текущее время на устройстве:

```
U_PE_1#sh clock
Current time is Wed Jul 22 07:54:25 2009
```

На SNTP-сервере было изменено время на 3 часа. На устройстве для большей информативности включен debug:

```
U_PE_1#debug sntp adjust
SNTP time adjust debug is on
U_PE_1#sh clock
Current time is Wed Jul 22 07:54:55 2009
U_PE_1#%Jul 22 07:55:01 2009  slewed 4a66c5d5.0 (WED JUL 22 07:55:01 2009
)
%Jul 22 10:55:17 2009  slewed 4a66f015.0 (WED JUL 22 10:55:17 2009
)

U_PE_1#no debug sntp adjust
SNTP time adjust debug is off
U_PE_1#sh clock
Current time is Wed Jul 22 10:55:19 2009
U_PE_1#
```

- Предоставить логи захваченного анализатором трафика (S)NTP. Файл SNTP.pcap

## 2.4 Тест 4. Аутентификация по RADIUS.

**Цель теста:** Проверить работу механизма идентификации администратора при доступе к оборудованию по протоколу RADIUS.

**Описание теста:**

- Настроить на коммутаторе аутентификацию администратора с использованием сервера AAA.

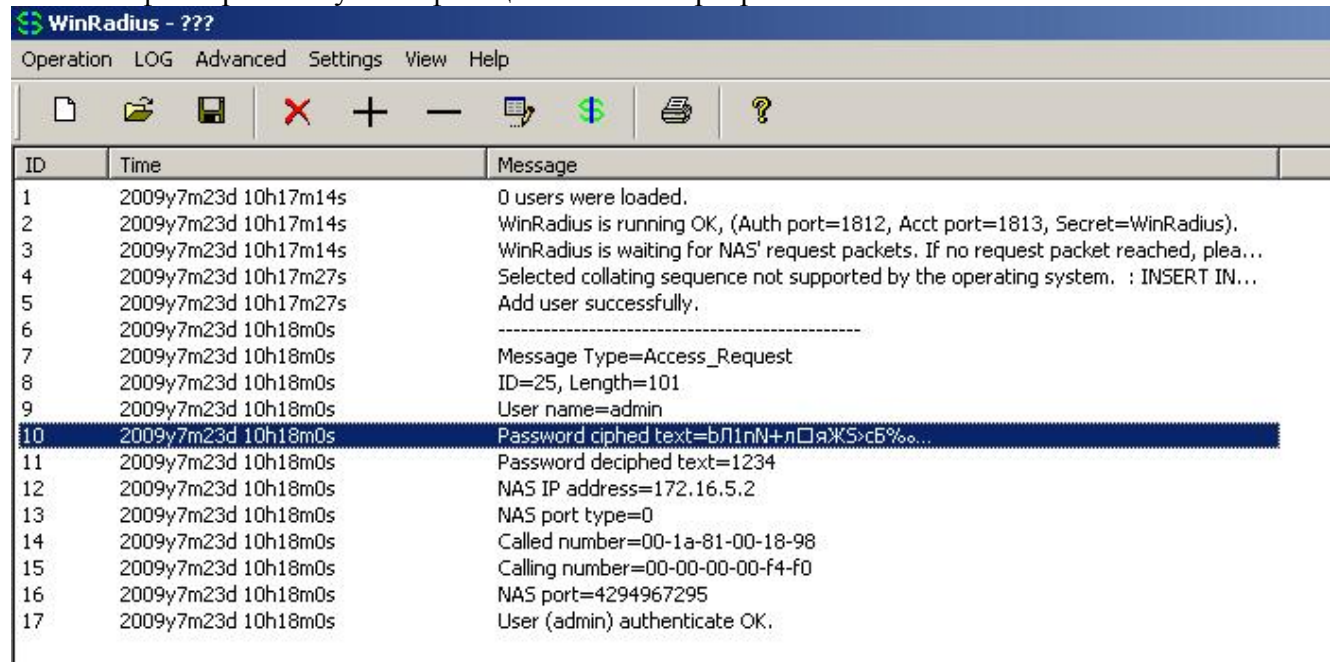
```
!  
authentication line vty login radius  
!  
radius-server key WinRadius  
radius-server authentication host 172.16.1.71  
aaa enable  
!
```

- Проверить возможность получения доступа к коммутатору.



```
C:\> Telnet 172.16.5.2  
login:admin  
Password:*****  
U_PE_1>en  
U_PE_1#exit  
  
Connection to host lost.  
Press any key to continue....
```

- Зафиксировать аутентификацию в логах сервера AAA



ID	Time	Message
1	2009y7m23d 10h17m14s	0 users were loaded.
2	2009y7m23d 10h17m14s	WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=WinRadius).
3	2009y7m23d 10h17m14s	WinRadius is waiting for NAS' request packets. If no request packet reached, plea...
4	2009y7m23d 10h17m27s	Selected collating sequence not supported by the operating system. : INSERT IN...
5	2009y7m23d 10h17m27s	Add user successfully.
6	2009y7m23d 10h18m0s	-----
7	2009y7m23d 10h18m0s	Message Type=Access_Request
8	2009y7m23d 10h18m0s	ID=25, Length=101
9	2009y7m23d 10h18m0s	User name=admin
10	2009y7m23d 10h18m0s	Password ciphered text=вЛпнМ+л□АЖS>сБ%о...
11	2009y7m23d 10h18m0s	Password deciphered text=1234
12	2009y7m23d 10h18m0s	NAS IP address=172.16.5.2
13	2009y7m23d 10h18m0s	NAS port type=0
14	2009y7m23d 10h18m0s	Called number=00-1a-81-00-18-98
15	2009y7m23d 10h18m0s	Calling number=00-00-00-00-f4-f0
16	2009y7m23d 10h18m0s	NAS port=4294967295
17	2009y7m23d 10h18m0s	User (admin) authenticate OK.

- Предоставить логи захваченного анализатором трафика RADIUS  
Файл Radius.pcap.

## 2.5 Тест 5. Работа syslog сервиса.

**Цель теста:** Проверить наличие записи событий на удалённый SYSLOG-Server

**Описание теста:**

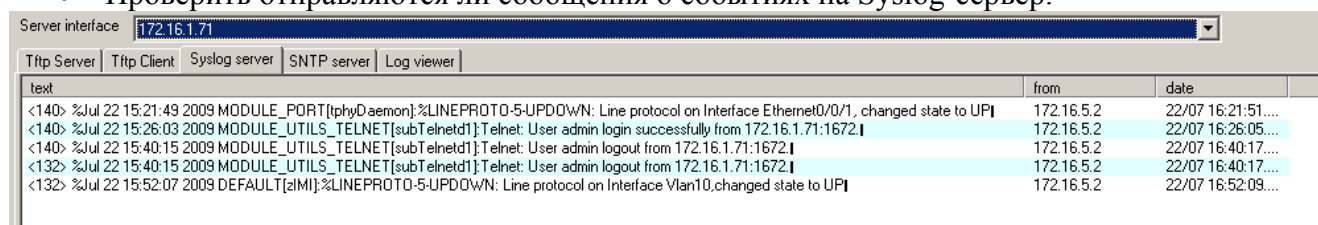
- Настроить отправку сообщений с коммутатора на Syslog-сервер.

```
!  
logging 172.16.1.71 level debugging  
!
```

- Произвести подключение PC-A в порт коммутатора, изменить конфигурацию на коммутаторе.

```
U_PE_1#%Jul 22 15:21:49 2009 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/1,  
changed state to UP
```

- Проверить отправляются ли сообщения о событиях на Syslog-сервер.



The screenshot shows a web-based Syslog server interface. At the top, there is a dropdown menu for 'Server interface' set to '172.16.1.71'. Below this are several tabs: 'Tftp Server', 'Tftp Client', 'Syslog server', 'SNTP server', and 'Log viewer'. The 'Log viewer' tab is active, displaying a table of log entries. The table has columns for 'text', 'from', and 'date'. The log entries include messages from the 'MODULE\_PORT' and 'MODULE\_UTILS\_TELNET' modules, reporting line protocol state changes and Telnet user login/logout events.

text	from	date
<140> %Jul 22 15:21:49 2009 MODULE_PORT[phyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/1, changed state to UP	172.16.5.2	22/07 16:21:51...
<140> %Jul 22 15:26:03 2009 MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 172.16.1.71:1672.1	172.16.5.2	22/07 16:26:05...
<140> %Jul 22 15:40:15 2009 MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 172.16.1.71:1672.1	172.16.5.2	22/07 16:40:17...
<132> %Jul 22 15:40:15 2009 MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 172.16.1.71:1672.1	172.16.5.2	22/07 16:40:17...
<132> %Jul 22 15:52:07 2009 DEFAULT[zlMI]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,changed state to UP	172.16.5.2	22/07 16:52:09...

- Предоставить логи этих процессов. См. выше.
- Предоставить логи захваченного анализатором трафика SYSLOG

Файл Syslog.pcap.

## 2.6 Тест 6. Работа SNMP.

**Цель теста:** Проверить работу управления коммутатора по SNMP

**Описание теста:**

- Настроить управление коммутатора по SNMP.

Настройка v2c:

```
!  
snmp-server enable  
snmp-server securityip 172.16.1.71  
snmp-server host 172.16.1.71 v2c trap  
snmp-server community ro public  
snmp-server community rw private  
snmp-server enable traps  
!
```

- Произвести подключение PC в порт коммутатора, изменение конфигурации на коммутаторе.

Произведено чтение данных с коммутатора и изменение параметра Name с U\_PE\_1 на U\_PE\_2 (см. файлы SNMPv2c.pcap).

- Проверить запись событий на удалённый SNMP-Server используя SNMP-traps.

Произведено отключение и подключение ПК в порт Ethernet 0/0/1 (см. файлы SNMPv2c.pcap).

- Прочитать и Изменить конфигурацию коммутатора с помощью SNMP-сервера управления.

См. пункты выше.

- Прочитать и Изменить конфигурацию коммутатора с помощью утилит SNMP
- Предоставить логи этих процессов

См. пункты выше.

- Предоставить логи захваченного анализатором трафика SNMP

Файл SNMPv2c.pcap.

## 2.7 Тест 7. Безопасность. Переполнение MAC-таблицы.

**Цель теста:** Проверка стабильности работы коммутатора при полном заполнении MAC-таблицы.

**Описание теста:**

- К порту F0/2 коммутатора U\_PE\_11 подключить PC\_A с программным обеспечением (VLC), позволяющем просмотр двух-трех каналов IPTV, подключиться к этим каналам и наблюдать трансляцию. Одновременно утилитой PING проверять в непрерывном режиме связанность PC\_A со шлюзом по умолчанию.

Прерывания ответа от шлюза в процессе тестирования не происходило.

- К порту F0/1 коммутатора U\_PE\_11 подключить PC\_B с программным обеспечением, или генератор трафика, с помощью которого провести атаку по заполнению MAC-таблицы коммутатора.
- Для этого циклически генерировать 10 тысяч пакетов с разными MAC-адресами источника и отсылать их в порт коммутатора.
- С сервера управления осуществить telnet-сессию на коммутатор U\_PE\_11.



- Проверить состояние MAC-таблицы, загрузку CPU, возможность отключения порта F0/1 и очистки MAC-таблицы от MAC-адресов атаки.

#### Состояние MAC-таблицы и загрузки CPU в момент атаки:

```
U_PE_1#show mac-address-t count
Compute the number of mac address....
Max entries can be created in the largest capacity card:
Total      Filter Entry Number is: 16384
Static     Filter Entry Number is: 16384
Unicast    Filter Entry Number is: 16384
Multicast  Filter Entry Number is: 255

Current entries have been created in the system:
Total      Filter Entry Number is: 12518
Individual Filter Entry Number is: 12518
Static     Filter Entry Number is: 1
Dynamic    Filter Entry Number is: 12517
Multicast  Filter Entry Number is: 0

U_PE_1#show cpu usage

Last 5 second CPU IDLE: 93%
Last 30 second CPU IDLE: 93%
Last 5 minute CPU IDLE: 79%
From running CPU IDLE: 93%
```

#### Состояние MAC-таблицы после выключения порта:

```
U_PE_1(config)#int e 0/0/1
U_PE_1(config-if-ethernet0/0/1)#shutdown
U_PE_1(config-if-ethernet0/0/1)#%Apr 23 17:58:54 1996 %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet0/0/1, changed state to DOWN
%Apr 23 17:58:54 1996 %LINK-5-CHANGED: Interface Ethernet0/0/1, changed state to
administratively DOWN

U_PE_1(config-if-ethernet0/0/1)#show mac-address-t cou
Compute the number of mac address....
Max entries can be created in the largest capacity card:
Total      Filter Entry Number is: 16384
Static     Filter Entry Number is: 16384
Unicast    Filter Entry Number is: 16384
Multicast  Filter Entry Number is: 255

Current entries have been created in the system:
Total      Filter Entry Number is: 2
Individual Filter Entry Number is: 2
Static     Filter Entry Number is: 1
Dynamic    Filter Entry Number is: 1
Multicast  Filter Entry Number is: 0
```

- Оценить влияние атаки на коммутацию IPuc и IPmc трафика. Атака не оказала влияние на вышеуказанные типы трафика.

## 2.8 Тест 8. Безопасность. Ограничения кол-ва MAC на порту.

**Цель теста:** Проверить возможность ограничения количества MAC-адресов источников на порту коммутатора.

**Описание теста:**

- Настроить порт F0/1 коммутатора U\_PE\_10 на работу максимум с 10-ю MAC-адресами источника трафика.
- К коммутатору U\_PE\_10 к порту F0/1 подключить PC\_A с программным обеспечением формирования пакетов.
- К коммутатору U\_PE\_10 к порту F0/20 подключить PC\_B с программным обеспечением анализа пакетов
- На порт F0/20 коммутатора U\_PE\_10 отзеркалировать трафик приходящий на интерфейс F0/1.
- С PC\_A циклически испускать 100 пакетов с разными MAC-адресами источника.
- Проверить что коммутатор пропускает первые 10 пакетов и не пропускает остальные.

В текущей версии программного обеспечения динамическое (без указания конкретного MAC-адреса) ограничение не реализовано. Возможно ограничение количества MAC-адресов источников с указанием конкретных адресов. Указывать можно как статические MAC-адреса так и конвертировать в статические, уже изученные коммутатором MAC-адреса.

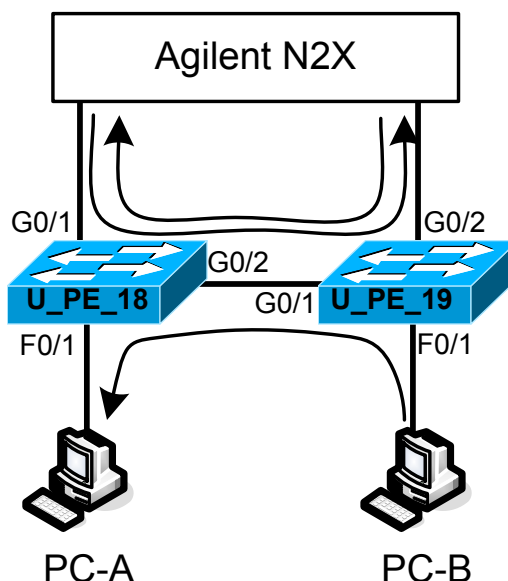
Синтаксис требуемых команд:

```
Interface Ethernet0/0/1
switchport port-security
switchport port-security maximum 10
switchport port-security lock
switchport port-security convert
```

## 2.9 Тест 9. Производительность и QoS.

**Цель теста:** Проверка коммутационной способности коммутатора доступа.

Рис.2

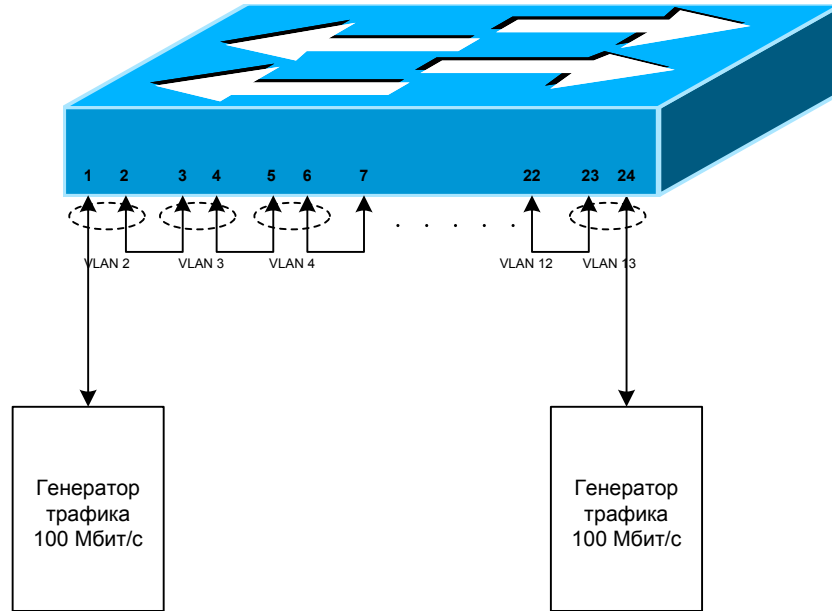


## Описание теста:

### Часть 1:

- Для проведения теста собрать схему изображенную на Рис. 2. Допускается использование генератора трафика другого типа со схожими характеристиками.

В связи с отсутствием генератора трафика 1Гбит/с, использовался генератор 100Мбит/с. Тестирование проводилось по следующей схеме:



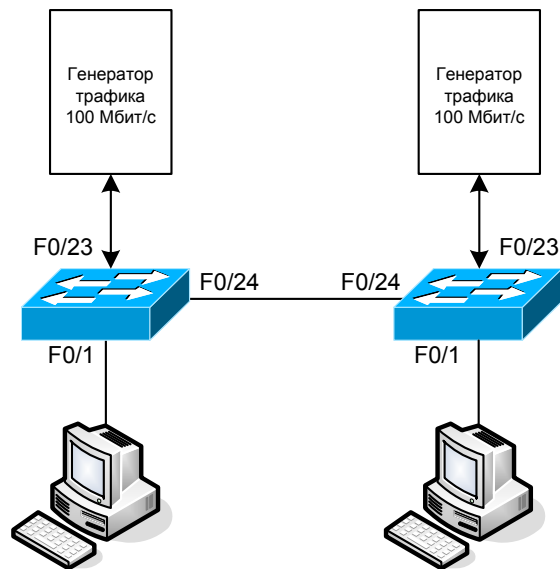
Порты попарно были изолированы с помощью VLAN, т.о. через каждый порт передавался трафик 100 Мбит/с в обоих направлениях.

- С генератора трафика сгенерировать непрерывный поток трафика объемом 1Гбит/с в обоих направлениях и проверить пропускаемый поток трафика на отсутствие потерь и ошибок.

Потери пакетов и ошибки отсутствовали.

### Часть 2:

Тестирование проводилось по следующей схеме:



- Настроить коммутаторы таким образом, чтобы трафик от PC\_A к PC\_B имел больший приоритет по сравнению с трафиком от генератора трафика.
- С генератора трафика сгенерировать поток трафика (Bulk, DSCP=0) объемом 1 Гбит/с в обоих направлениях
- Одновременно с PC\_A на PC\_B сгенерировать максимально возможный для i386 UDP поток с помощью утилиты IPERF (DSCP=EF, ~50-70 Мбит/с).
- Проверить, что UDP трафик между PC не теряется, а трафик с генератора теряется.
- Несколько раз включать-выключать поток от аппаратного генератора, фиксируя в отчете влияние на измеряемый UDP трафик.

В случае использования очереди Strict-Priority отключение и подключение генератора не влияет на трафик между компьютерами.

- Повторить тесты для трех случаев:

**А) Приоритет определяется на основе интерфейса коммутатора, UDP трафик направляется в Strict-Priority очередь.**

Трафику, пришедшему на порт Ethernet0/0/1, назначается метка CoS=5. Трафик направляется в Strict-Priority очередь:

```
!
mls qos
  priority-queue out
!
Interface Ethernet0/0/1
  mls qos cos 5
!
```

**Б) Приоритет определяется на основе разметки DSCP, UDP трафик направляется в Strict-Priority очередь.**

С нижеуказанной конфигурацией коммутатор обрабатывает пакеты на основе уже определенного поля DSCP:

```
!  
mls qos  
  priority-queue out  
!  
Interface Ethernet0/0/1  
  mls qos trust dscp  
!
```

Ниже приведена конфигурация, когда в пакетах, поступающих на порт Ethernet0/0/1 из сети 192.168.0.24, задается приоритет в поле DSCP.

```
!  
access-list 1 permit 192.168.0.0 0.0.0.255  
!  
mls qos  
class-map ZES  
  match access-group 1  
!  
policy-map ZES_policy  
  class ZES  
    set ip dscp 46  
  exit  
!  
Interface Ethernet0/0/1  
  service-policy input ZES_policy  
!
```

**В) Приоритет определяется на основе разметки DSCP, UDP трафик и BULK трафик обслуживаются по алгоритму WRR.**

Поскольку по умолчанию используется алгоритм WRR, необходимо настроить только метод обработки входящего трафика:

```
!  
mls qos  
!  
Interface Ethernet0/0/1  
  mls qos trust dscp  
!
```

В случае использования очереди WRR при подключении генераторов, трафик обслуживается в соответствии с весами очередей – 1:2:4:8.

В коммутаторе задана таблица соответствия меток DSCP, CoS очередям QoS:

```
U_PE_18(config)#show mls qos maps  
Cos-dscp map:  
      cos:   0  1  2  3  4  5  6  7  
-----  
      dscp:   0  8 16 24 32 40 48 56  
  
Cos-queue map:  
Cos   0    1    2    3    4    5    6    7  
Queue 1    1    2    2    3    3    4    4
```

Т.о., трафик с меткой DSCP=EF (46) попадает в очередь 3 с весом 4 и имеет больший приоритет по сравнению с bulk-трафиком. Возникают потери пакетов, пропорционально весам очередей.

### Часть 3:

- Отключить приоритезацию трафика на соединении между коммутаторами и проверить как это влияет на трафик UDP.

Возникают потери пакетов.

## 2.10 Тест 10. Multicast IPTV.

**Цель теста:** Проверить работу сервиса IPTV на стенде.

**Описание теста:**

- Обеспечить вещание широковещательного трафика IPTV из источника, включенного в корневой коммутатор (Dense режим)
- Настроить MC-VLAN для трафика IPTV.
- Настроить на коммутаторах кольца протокол MVR.

```
vlan 222
 name MC-VLAN
 multicast-vlan
 !
 ip igmp snooping
 ip igmp snooping vlan 222
```

- Убедится в наличии изображения на PC\_A и PC\_B.
- В табличной форме представить состояние протокола MVR на каждом коммутаторе кольца.

### Состояние протокола MVR до разрыва кольца

Имя коммутатора	Groups	Порты
U PE 1	239.1.1.3	Eth 0/0/26
U PE 2	239.1.1.3	Eth 0/0/26
U PE 3	239.1.1.3	Eth 0/0/26
U PE 4	239.1.1.3	Eth 0/0/26
U PE 5	239.1.1.3	Eth 0/0/26
U PE 6	239.1.1.3	Eth 0/0/26
U PE 7	239.1.1.3	Eth 0/0/26
U PE 8	239.1.1.3	Eth 0/0/26
U PE 9	239.1.1.3	Eth 0/0/26
U PE 10	239.1.1.3	Eth 0/0/1
U PE 11	239.1.1.3	Eth 0/0/1
U PE 12	239.1.1.3	Eth 0/0/25
U PE 13	239.1.1.3	Eth 0/0/25
U PE 14	239.1.1.3	Eth 0/0/25
U PE 15	239.1.1.3	Eth 0/0/25
U PE 16	239.1.1.3	Eth 0/0/25
U PE 17	239.1.1.3	Eth 0/0/25
U PE 18	239.1.1.3	Eth 0/0/25
U PE 19	239.1.1.3	Eth 0/0/25
U PE 20	239.1.1.3	Eth 0/0/25

- Разорвать физически кольцо между корневым коммутатором и задействованным коммутатором доступа в который включен PC\_A и заполнить таблицу состояния MVR на каждом коммутаторе кольца повторно.

**Состояние протокола MVR после разрыва кольца**

Имя коммутатора	Groups	Порты
U PE 1	-	-
U PE 2	-	-
U PE 3	-	-
U PE 4	-	-
U PE 5	-	-
U PE 6	-	-
U PE 7	-	-
U PE 8	-	-
U PE 9	-	-
U PE 10	239.1.1.3	Eth 0/0/1
U PE 11	239.1.1.3	Eth 0/0/25 Eth 0/0/1
U PE 12	239.1.1.3	Eth 0/0/25
U PE 13	239.1.1.3	Eth 0/0/25
U PE 14	239.1.1.3	Eth 0/0/25
U PE 15	239.1.1.3	Eth 0/0/25
U PE 16	239.1.1.3	Eth 0/0/25
U PE 17	239.1.1.3	Eth 0/0/25
U PE 18	239.1.1.3	Eth 0/0/25
U PE 19	239.1.1.3	Eth 0/0/25
U PE 20	239.1.1.3	Eth 0/0/25

- Оценить время перерыва в вещании при разрыве и восстановлении кольца.  
1 с.

## 2.11 Тест 11. Списки доступа для IGMP-запросов.

**Цель теста:** Проверить работу списков доступа для IGMP-запросов.

**Описание теста:**

- Настроить оборудование как в предыдущем тесте.
- На портах F0/1 коммутаторов U\_PE\_10 и 11 настроить IGMP-фильтры. Фильтр должен иметь разрывность (включать несколько запрещенных и разрешенных диапазонов)

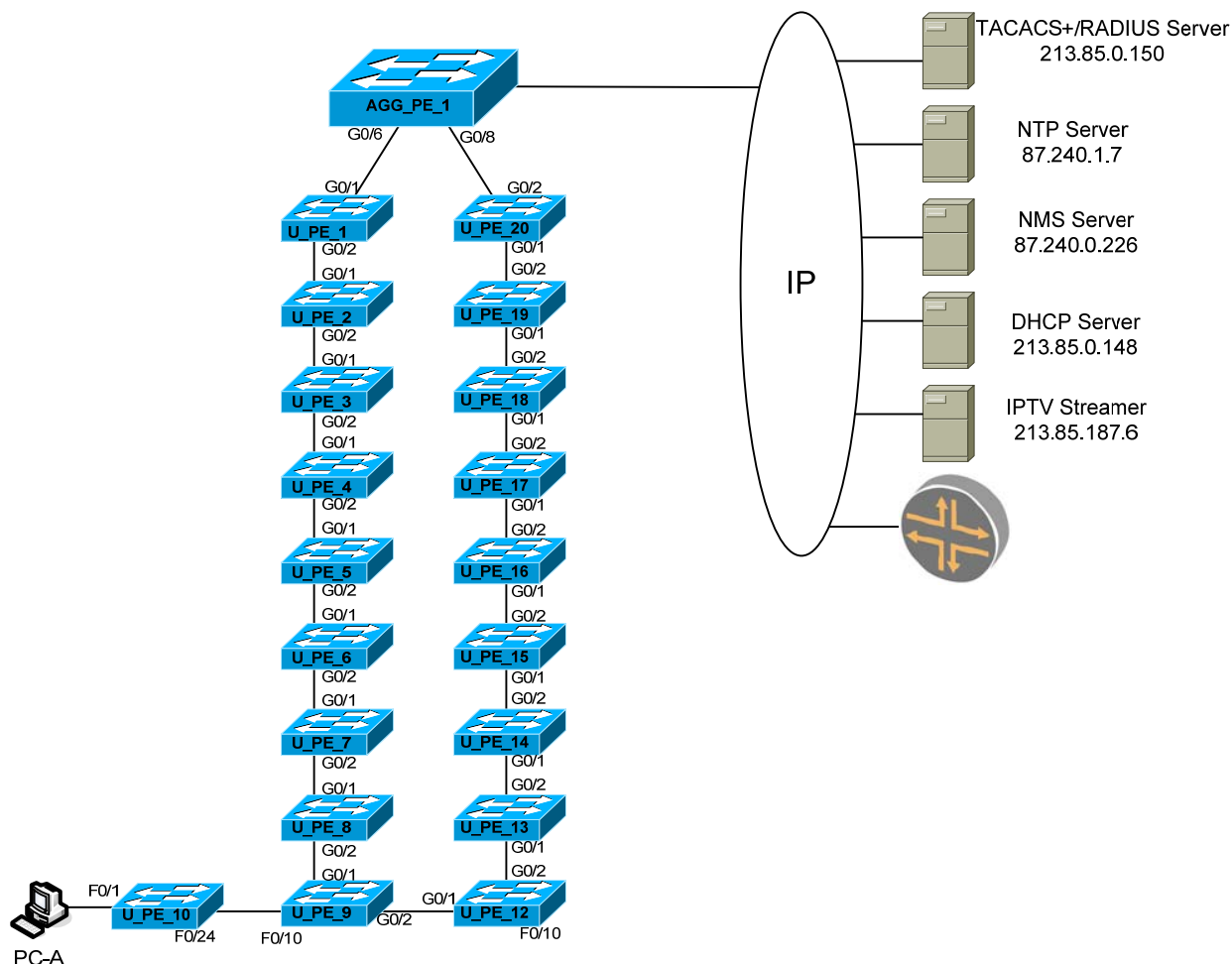
Настройка фильтра, запрещающего подключение к группе 239.1.1.1 через порт Ethernet0/0/1:

```
!
access-list 6000 deny ip any-source host-destination 239.1.1.2
access-list 6000 permit ip any-source host-destination 239.1.1.10
access-list 6000 deny ip any-source host-destination 239.1.1.1
access-list 6000 permit ip any-source any-destination
!
multicast destination-control
!
Interface Ethernet0/0/1
 ip multicast destination-control access-group 6000
```

- Убедится в невозможности просмотра потоков IPTV, внесенных в фильтр.

## 2.12 Тест 12. Безопасность STP на портах доступа.

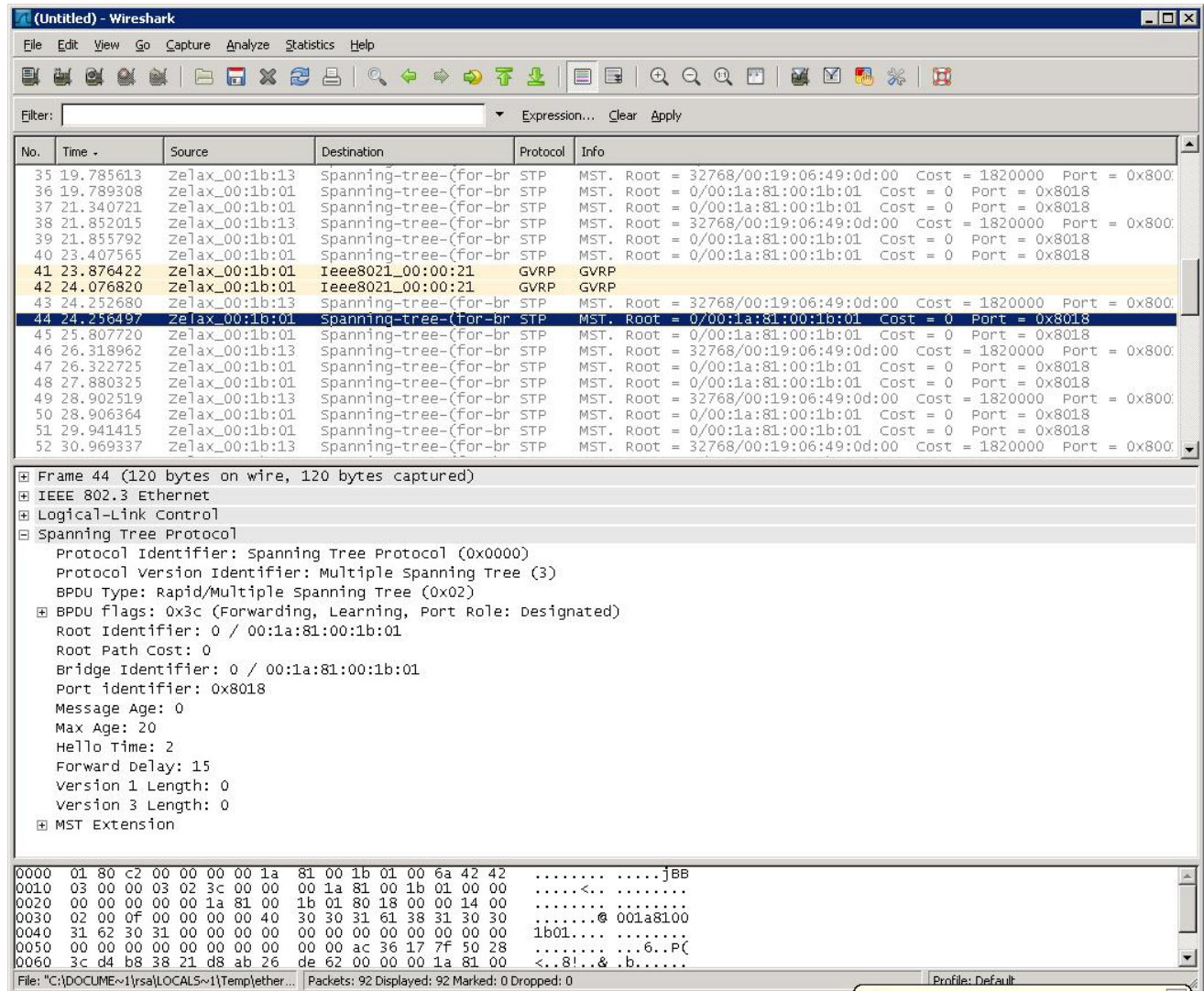
Рисунок 3. Схема станда для второй фазы тестов.



**Цель теста:** Проверить устойчивость коммутатора доступа к получению BPDU из абонентского порта, при подключении к нему нелегитимного коммутатора вместо ПК.

**Описание теста:**

- Коммутатор **U\_PE\_10** отключить от кольца – это будет эмуляция коммутатора злонамеренного пользователя.
- Порт **G0/2** коммутатора **U\_PE\_9** соединить с портом **G0/1** коммутатора **U\_PE\_11** – замкнуть кольцо доступа.
- К коммутатору **U\_PE\_9** к порту **F0/10** подключить порт **F0/24** коммутатора **U\_PE\_10**.
- На коммутаторе **U\_PE\_10** для VLAN 1100 настроить протокол STP с значением **Bridge priority = 0**.
- Отзеркалировать трафик приходящий на порт **F0/10** коммутатора **U\_PE\_9** на сетевой анализатор и проверить наличие BPDU-пакетов приходящих от коммутатора **U\_PE\_10**.



- Проверить состояние протокола STP коммутатора U\_PE\_9, которое должно остаться неизменным и не реагировать на BPDU-пакеты от коммутатора U\_PE\_10.

**Состояние STP коммутатора U PE 9 с подключенным коммутатором U PE 10.**

PortName	Role
Ethernet0/0/1	FWD DSGN
Ethernet0/0/25	FWD DSGN
Ethernet0/0/26	FWD ROOT

**Состояние STP коммутатора U PE 9 без коммутатором U PE 10.**

PortName	Role
Ethernet0/0/25	FWD DSGN
Ethernet0/0/26	FWD ROOT

## 2.13 Тест 13. Поддержка функций jumbo frames и QinQ.

**Цель теста:** Проверить возможности коммутатора по инкапсуляции трафика с одной меткой 802.1q в трафик с дополнительной меткой 802.1q и возможность коммутаторов обрабатывать пакеты длиной более 1500 байт.

**Описание теста:**

- Собрать схему стенда как показано на Рис. 3
- Подключить к портам F0/1 коммутатора U\_PE\_10 PC\_A.
- На коммутаторе U\_PE\_10 настроить VLAN 200 и порт F0/1 назначить в VLAN 200, Inner-TAG. На порту F0/24 настроить trunk.
- На коммутаторе U\_PE\_9 на порту F0/10 настроить режим QinQ, (произвести инкапсуляцию трафика с коммутатора U\_PE\_10 в VLAN 1101, Outer-TAG).

```
!  
vlan 1101  
!  
dot1q-tunnel enable  
dot1q-tunnel tpid 9100  
!  
Interface Ethernet0/0/10  
  switchport dot1q-tunnel mode customer  
  switchport access vlan 1101  
!  
Interface Ethernet0/0/18  
  switchport dot1q-tunnel mode uplink  
  switchport mode trunk  
!
```

- Настроить интерфейс шлюза IP на обработку стекированных VLAN
- Проверить связность PC\_A с интерфейсом шлюза утилитой PING с размером пакета 1900 байт. При этом должна быть запрещена фрагментация пакета, и установлен соответствующий MTU для физического интерфейса PC\_A и шлюза.

Тест проводился с помощью аппаратного генератора-анализатора трафика, который формировал пакет длиной 1600 байт. См. файл jumbo.pcap.

- Отзеркалировать трафик на U\_PE\_9 на анализатор и удостовериться в наличии двух VLAN-тегов у трафика с PC\_A до BRASa.

См. файлы Dot1q-tunnel\_8100.pcap и Dot1q-tunnel\_9100.pcap.

- В случае невозможности настроить шлюз на обработку стекированных VLAN, сделать тест с использованием PC\_B (сетевой адаптер в tagged режиме), когда Outer-TAG снимается соответствующим коммутатором доступа, или провести тест при помощи аппаратного генератора-анализатора.
- Повторить тесты для различных значений TPID.

См. файлы Dot1q-tunnel\_8100.pcap и Dot1q-tunnel\_9100.pcap.

## 2.14 Тест 14. Большое количество telnet сессий.

**Цель теста:** Проверить возможность работы коммутатора по работе с 8-ю telnet-сессиями одновременно.

**Описание теста:**

- С помощью автоматического скрипта одновременно установить 8 сессий telnet на коммутатор U\_PE\_1 и одновременно выдать команды по настройке разных портов коммутатора во всех восьми сессиях.

Максимальное количество одновременно установленных telnet-сессий может быть равно 16. Вход в режим глобальной конфигурации можно осуществить только из одной сессии (включая консоль), доступ для остальных сессий блокируется.

- Проверить сколько успешно настроенных портов на коммутаторе мы получим.

## 2.15 Тест 15. Проверка функционала TDR.

**Цель теста:** Проверить возможность коммутатора по диагностике UTP-кабеля подключенного к портам FastEthernet.

**Описание теста:**

- Подключить к порту F0/20 коммутатора U\_PE\_9 кабель достаточно большой длины.
- С помощью коммутатора измерить длину кабеля.

```
U_PE_1(config-if-ethernet0/0/20)#virtual-cable-test

Interface Ethernet0/0/20:
-----
Cable pairs      Cable status      Error lenth (meters)
-----
(1, 2)           open              15
(3, 6)           open              15
```

- Подключить к порту PC\_A.
- С помощью коммутатора измерить длину кабеля при подключенном PC.

Измерение длины кабеля можно производить только при неподключенном, на удаленной стороне, кабеле. При подключении оборудования, на удаленной стороне, коммутатор отображает текущее состояние кабеля (cable status):

```
U_PE_1(config-if-ethernet0/0/20)#virtual-cable-test

Interface Ethernet0/0/20:
-----
Cable pairs      Cable status      Error lenth (meters)
-----
(1, 2)           well              --
(3, 6)           well              --
```

- Продемонстрировать функциональность при подключении «неправильных (с перепутанными парами) кабелей».

Проводники с номерами 3 и 6 не скоммутированы, проводники с номерами 1 и 2 скоммутированы правильно.

```
U_PE_1(config-if-ethernet0/0/20)#virtual-cable-test

Interface Ethernet0/0/20:
-----
Cable pairs      Cable status      Error lenth (meters)
-----
(1, 2)           well              --
(3, 6)           open              15
```

### 3 Сведения об оборудовании

1) Предоставить изображение внешнее.



2) Предоставить изображение внутреннее (фото со снятой крышкой).



3) Предоставить паспортный диапазон рабочих температур.

0°C – 50°C

4) Предоставить паспортное значение MTBF.

80,000 часов

5) Описать систему охлаждения, наличие вентиляторов.

Вентиляторы не применяются. Используется пассивное охлаждение.

## 4 Результаты тестирования.

№ теста	Название теста	Результаты
Тест 1.	Проверка работы STP.	Протокол STP успешно обрабатывает случаи обрыва и восстановления соединения кольца доступа.
Тест 2.	Проверка IP-связности.	Связность между тестовыми компьютерами не нарушается при обрыве и восстановлении кольца доступа.
Тест 3.	NTP.	Протокол синхронизации времени NTP работает корректно.
Тест 4.	Аутентификация по RADIUS.	Успешная авторизация с использованием внешнего сервера RADIUS выполняется.
Тест 5.	Работа syslog сервиса.	Сервис syslog работает корректно.
Тест 6.	Работа SNMP.	Сервис SNMP работает корректно.
Тест 7.	Безопасность. Переполнение MAC-таблицы.	При переполнении MAC-таблицы коммутатор работает устойчиво и корректно
Тест 8.	Безопасность. Ограничения кол-ва MAC на порту.	Функции по ограничению количества MAC-адресов на порту работают. Необходимо указывать разрешенные MAC-адреса.
Тест 9.	Производительность и QoS.	Производительность коммутатор достаточна для того, чтобы обслуживать порты на полной скорости и выполнять функции QoS для приоритетного обслуживания трафика.
Тест 10.	Multicast IPTV.	Функции по предоставлению услуги IPTV работают корректно, позволяя безболезненно переносить случаю обрыва связи в кольце доступа.
Тест 11.	Списки доступа для IGMP-запросов	Списки доступа для IGMP-запросов есть и работают правильно, позволяя ограничивать возможность пользователей подписываться на те или иные IPTV программы
Тест 12	Безопасность STP на портах доступа.	Функции по обеспечению безопасности на портах доступа делают сеть провайдера защищенной от атак на протокол STP.
Тест 13	Поддержка функций jumbo frames и QinQ.	Коммутаторы поддерживают QinQ и пакеты повышенной длины, функционал работает правильно.
Тест 14	Большое количество telnet сессий.	Проверенно установление 8 telnet-сессий. Доступ в режим глобальной конфигурации был доступен только из одной из них. Доступ из остальных был заблокирован.
Тест 15	Проверка функционала TDR.	Коммутатор позволяет с помощью функций TDR измерять длину UTP-кабеля подключенного к порту доступа. Работает на всех портах RJ-45.
Тест 16	Проверка работы IP SLA агента.	IP SLA аген на коммутаторе не реализован.