

Методика тестирования
мультисервисных коммутаторов
QTECH QSW-2700



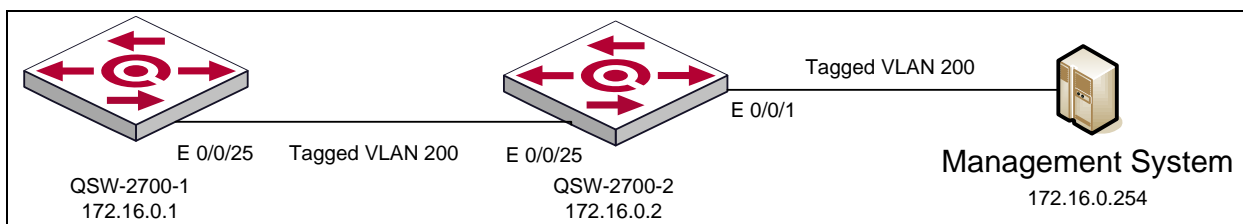
Москва 2012

Содержание

Содержание	2
I. Управление коммутатором	3
1) Управление по протоколу <i>TELNET</i>	3
2) Управление по протоколу <i>HTTP</i>	3
3) Управление по протоколу <i>SSH</i>	3
4) Управление по протоколу <i>SNMP</i>	3
II. Аутентификация пользователей на коммутаторе	4
1) Поддержка <i>RADIUS</i>	4
2) Поддержка <i>TACACS+</i>	5
III. Безопасность на портах доступа	5
1) Изоляция портов	5
2) Работа <i>ACL</i>	6
3) Обнаружение петель на стороне клиента	7
4) Ограничение количества <i>MAC</i> адресов на порту	8
IV. Синхронизация даты и времени с <i>NTP</i> сервером	8
V. Работа <i>Syslog</i>	9
VI. Работа <i>LLDP</i>	10
VII. Работа <i>LACP</i>	10
VIII. Поддержка функций <i>PPPoE Intermediate Agent</i> и <i>PPPoE snooping</i>	11
IX. Поддержка <i>DHCP-Relay</i>	13
X. Поддержка <i>DHCP Snooping</i>	14
XI. <i>IGMP Snooping</i>, <i>Multicast VLAN</i>, Списки доступа для <i>IGMP</i> запросов	15
XII. Работа протокола <i>MSTP</i>	17
XIII. Тест на производительность	19
XIV. <i>Port-based QinQ</i>	22
XV. <i>Selective QinQ</i>	23
XVI. <i>Jumbo frame</i>	25
XVII. Качество обслуживания. <i>COS</i>.	25
Приложение 1. Образец конфигурационного файла для коммутатора <i>QSW-2700</i>	28
Приложение 2. Протокол тестирования коммутатора <i>QSW-2700</i>	33

I. Управление коммутатором

Схема:



Исходное состояние: К коммутатору Ethernet подключается хост, выполняющий функции удаленного рабочего места системы управления. На данном хосте устанавливается программное обеспечение SNMP, Telnet клиент, SSH клиент и WEB браузер. IP-адрес для указанного хоста конфигурируется вручную и должен находиться в пределах той же подсети, что и IP-адрес коммутатора, используемого для функций взаимодействия с системой управления. На коммутаторе Ethernet конфигурируется возможность управления по протоколам Telnet, HTTP, SSH и SNMP.

1) Управление по протоколу TELNET

Цель теста: Проверка возможности удаленного управления оборудованием по протоколу Telnet.

Тестовая процедура: Осуществляется подключение к коммутатору по протоколу Telnet.

Ожидаемый результат: Коммутатор управляется по протоколу Telnet.

2) Управление по протоколу HTTP

Цель теста: Проверка возможности удаленного управления оборудованием по протоколу HTTP

Тестовая процедура: Осуществляется подключение к коммутатору по протоколу HTTP, через WEB браузер.

Ожидаемый результат: Коммутатор управляется по протоколу HTTP через WEB интерфейс коммутатора.

3) Управление по протоколу SSH

Цель теста: Проверка возможности удаленного управления оборудованием по протоколу SSH.

Тестовая процедура: Осуществляется подключение к коммутатору по протоколу SSH.

Ожидаемый результат: Коммутатор управляется по протоколу HTTP через WEB интерфейс коммутатора.

4) Управление по протоколу SNMP

Цель теста: Проверка возможности удаленного управления оборудованием по протоколу SNMP.

Тестовая процедура: Осуществляется подключение к коммутатору по протоколу SNMP.

Ожидаемый результат: Коммутатор управляется по протоколу SNMP.

Краткая конфигурация коммутатора QSW-2700:

```
username admin privilege 15 password 0 123456
```

```
!
```

```
authentication line console login local
```

```
!
```

```
ssh-server enable
```

```
!
```

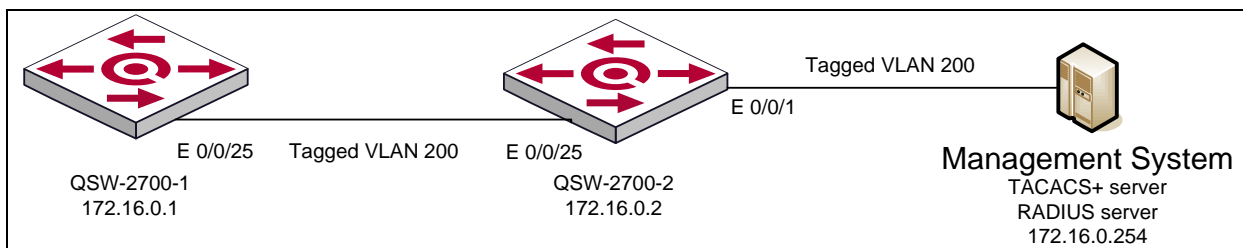
```

!
snmp-server enable
snmp-server securityip 172.16.0.254
snmp-server community rw private
snmp-server community ro public
!

```

II. Аутентификация пользователей на коммутаторе

Схема:



Исходное состояние: К коммутатору Ethernet подключается хост, выполняющий функции удаленного рабочего места системы управления. На данном хосте устанавливается программное обеспечение RADIUS сервер, TACACS+ сервер, Telnet клиент, SSH клиент и WEB браузер. IP-адрес для указанного хоста конфигурируется вручную и должен находиться в пределах той же подсети, что и IP-адрес коммутатора, используемый для функций взаимодействия с системой управления. На коммутаторе Ethernet конфигурируется возможность аутентификации и авторизации пользователей на серверах TACACS+ и RADIUS. На серверах TACACS+ и RADIUS настраиваются профайлы пользователей.

1) Поддержка RADIUS

Цель теста: Проверка возможности аутентификации и авторизации пользователя на удаленном RADIUS сервере.

Тестовая процедура: Осуществляется подключение к коммутатору по протоколам telnet, ssh, http, а так же через консольный порт.

Ожидаемый результат: Убедиться, что коммутатор аутентифицирует и авторизует пользователя заведенного на RADIUS сервере. Убедиться, что существует возможность локальной аутентификации и авторизации в случае недоступности RADIUS сервера.

Краткая конфигурация коммутатора QSW-2700:

```

authentication line console login local radius
authentication line vty login local radius
authentication line web login local radius
authentication enable local radius
authorization line console exec local radius
authorization line vty exec local radius
authorization line web exec local radius
!
radius-server key radius
radius-server authentication host 172.16.0.254
aaa enable
!

```

2) Поддержка TACACS+

Цель теста: Проверка возможности аутентификации и авторизации пользователя на удаленном TACACS+ сервере.

Тестовая процедура: Осуществляется подключение к коммутатору по протоколам telnet, ssh, http, а так же через консольный порт.

Ожидаемый результат: Убедиться, что коммутатор аутентифицирует и авторизует пользователя заведенного на TACACS+ сервере. Убедиться, что существует возможность локальной аутентификации и авторизации в случае недоступности RADIUS+ сервера.

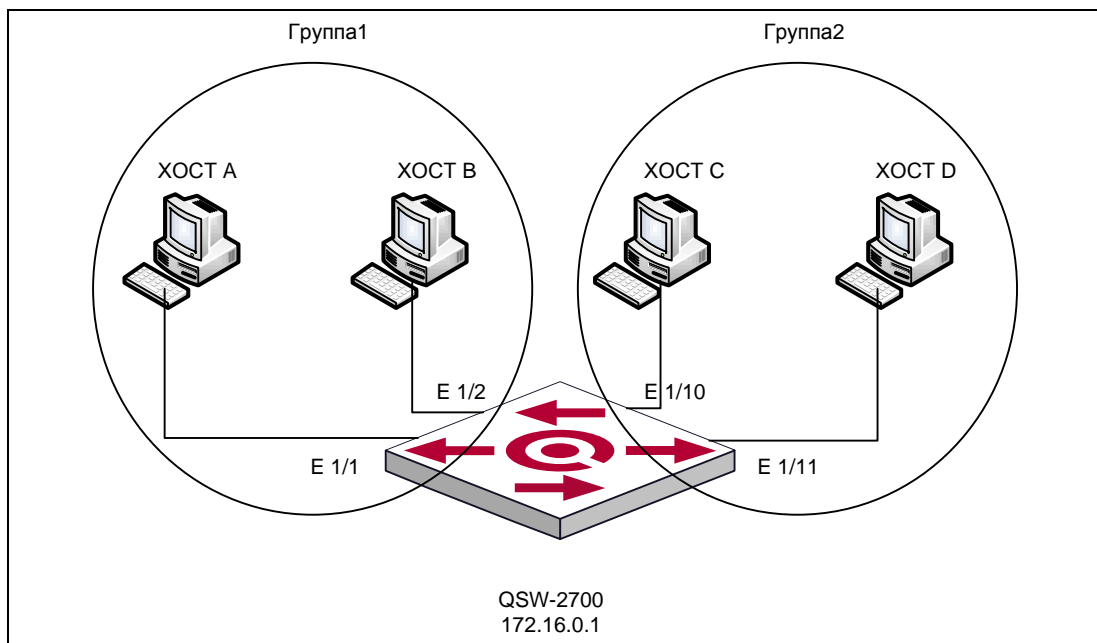
Краткая конфигурация коммутатора QSW-2700:

```
authentication line console login local tacacs
authentication line vty login local tacacs
authentication line web login local tacacs
authentication enable local tacacs
authorization line console exec local tacacs
authorization line vty exec local tacacs
authorization line web exec local tacacs
!
tacacs-server key tacacs
tacacs-server authentication host 172.16.0.254
```

III. Безопасность на портах доступа

1) Изоляция портов

Схема:



Исходное состояние: К коммутатору Ethernet подключаются четыре хоста. IP-адреса для хостов конфигурируются вручную, должны находиться в пределах одной подсети и в одном широковещательном домене. На коммутаторе Ethernet конфигурируется две группы изолированных портов, в первую группу относятся хосты А и В, во вторую хосты С и D.

Цель теста: Проверка возможности изолирования портов на коммутаторе в режимах: порт - порт, группа портов - группа портов.

Тестовая процедура: Осуществляется пинг между:

- 1) Хост А и Хост В
- 2) Хост С и Хост D
- 3) Хост А и Хост С
- 4) Хост В и Хост D

Ожидаемый результат: Убедиться, что пинг:

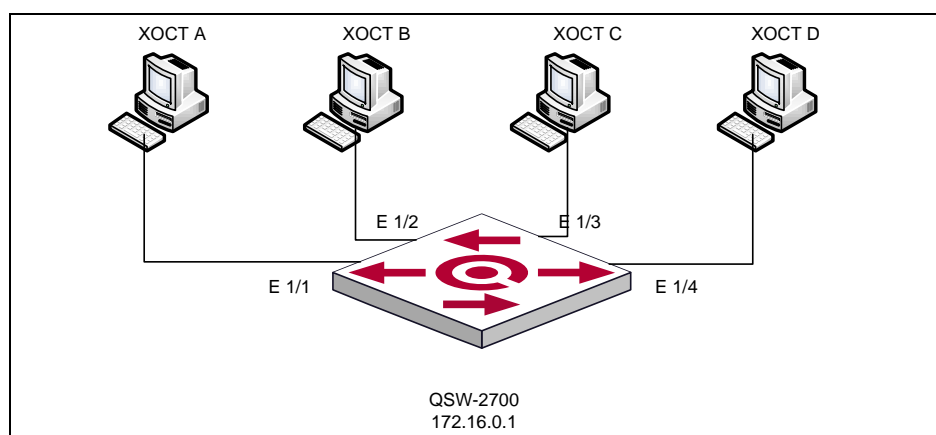
- 1) Дает отрицательный результат
- 2) Дает отрицательный результат
- 3) Дает положительный результат
- 4) Дает положительный результат

Краткая конфигурация коммутатора QSW-2700:

```
isolate-port group 1 switchport interface ethernet1/1;2  
isolate-port group 2 switchport interface ethernet1/10;11
```

2) Работа ACL

Схема:



Исходное состояние: К коммутатору Ethernet подключаются четыре хоста. IP-адреса для хостов конфигурируются вручную, должны находиться в пределах одной подсети и в одном широковещательном домене. На коммутаторе Ethernet конфигурируются следующие правила ACL:

- 1) Запрет входящего трафика с MAC адресом назначения Хоста А (на интерфейсе e 1/2)
- 2) Запрет входящего трафика с IP адресом назначения Хоста А (на интерфейсе e 1/3)
- 3) Запрет входящего трафика с IP адресом и MAC адресом источника Хоста А (на интерфейсе e 1/1)

Цель теста: Проверка работоспособности ACL следующих типов: MAC ACL, IP ACL, MAC-IP ACL.

Тестовая процедура: Осуществляется пинг между:

- 1) Хост А и Хост В
- 2) Хост А и Хост С
- 3) Хост А и Хост D
- 4) Хост В и Хост D

Ожидаемый результат: Убедиться, что пинг:

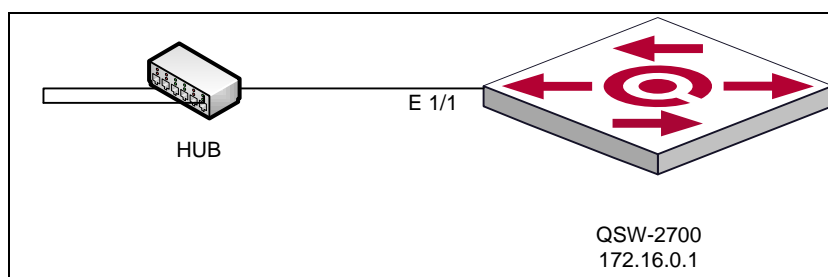
- 1) Дает отрицательный результат
- 2) Дает отрицательный результат
- 3) Дает отрицательный результат
- 4) Дает положительный результат

Краткая конфигурация коммутатора QSW-2700:

```
!  
firewall enable  
!  
access-list 100 deny ip any-source host-destination 172.16.1.194  
access-list 1100 deny any-source-mac host-destination-mac 00-24-54-b8-e9-bf  
access-list 3100 deny host-source-mac 00-24-54-b8-e9-bf any-destination-mac ip  
host-source 172.16.1.194 any-destination  
!  
Interface Ethernet1/1  
  mac-ip access-group 3100 in  
!  
Interface Ethernet1/2  
  mac access-group 1100 in  
!  
Interface Ethernet1/3  
  ip access-group 100 in
```

3) Обнаружение петель на стороне клиента

Схема:



Исходное состояние: К коммутатору Ethernet подключается HUB. На порту коммутатора Ethernet конфигурируется определение петли. При обнаружении петли, коммутатор должен физически «положить» порт.

Цель теста: Проверка работоспособности функционала обнаружения петель.

Тестовая процедура: На стороне клиента создаётся физическая петля, путем замыкания двух портов на устройстве HUB.

Ожидаемый результат: Убедиться, что коммутатор обнаружил петлю и физически «положил» порт

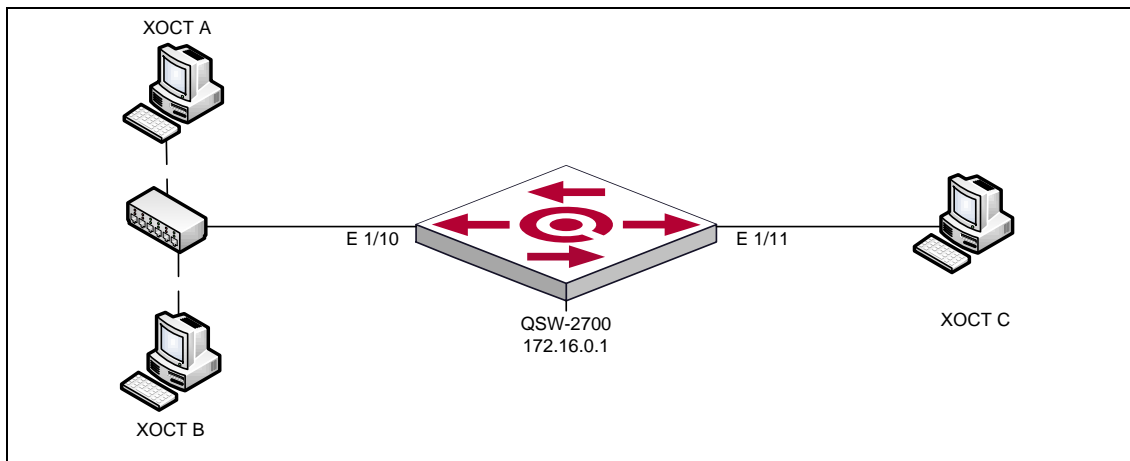
Краткая конфигурация коммутатора QSW-2700:

```
!  
Interface Ethernet1/1  
  loopback-detection specified-vlan 1
```

loopback-detection control shutdown
!

4) Ограничение количества MAC адресов на порту

Схема:



Исходное состояние: К порту коммутатора Ethernet подключается HUB, на этом порту конфигурируется ограничение количества MAC адресов за портом, устанавливается максимальное число мак адресов для данного порта равное 1. К коммутатору Ethernet подключается хост С. IP-адреса для хостов А, В и С конфигурируются вручную, должны находиться в пределах одной подсети. Хосты А, В и С находятся в одном широковещательном домене.

Цель теста: Проверка коммутатора с точки зрения возможности ограничения общего числа MAC адресов за портом.

Тестовая процедура:

- 1) Хост А подключается к HUB и выполняет ping на IP адрес хоста С
- 2) Хост В подключается к HUB и выполняет ping на IP адрес хоста С

Ожидаемый результат: Необходимо убедиться, что:

- 1) Пинг от хоста А дает положительный результат
- 2) Пинг от хоста В дает отрицательный результат

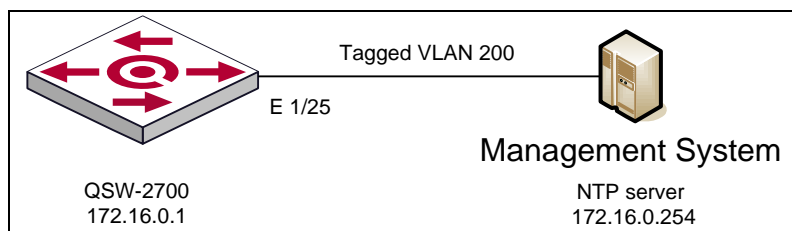
Краткая конфигурация коммутатора QSW-2700:

```
Interface Ethernet1/10  
switchport mac-address dynamic maximum 1
```

!

IV. Синхронизация даты и времени с NTP сервером

Схема:



Исходное состояние: К коммутатору Ethernet подключается хост. На данном хосте устанавливается NTP сервер. IP-адрес для указанного хоста конфигурируется вручную и должен находиться в пределах той же подсети, что и IP-адрес коммутатора. Коммутатор конфигурируется таким образом, чтобы синхронизировать дату и время с данным NTP сервером.

Цель теста: Проверка коммутатора с точки зрения возможности синхронизации даты и времени с удаленным NTP сервером.

Ожидаемый результат: Необходимо:

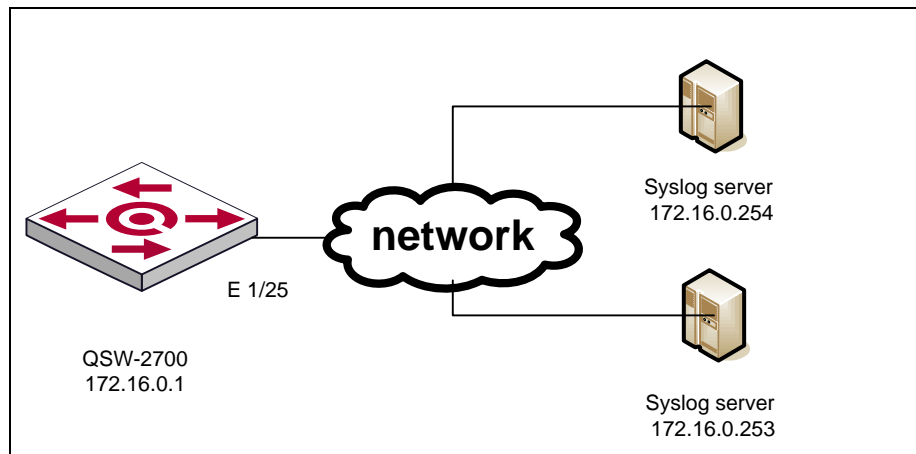
- 1) Убедиться, что коммутатор синхронизируется с источником
- 2) Проверить корректность отображения времени

Краткая конфигурация коммутатора QSW-2700:

```
sntp server 172.16.0.254
```

V. Работа Syslog

Схема:



Исходное состояние: К коммутатору Ethernet подключаются хосты. На данных хостах устанавливается Syslog сервер. IP-адреса для указанных хостов конфигурируются вручную и должны находиться в пределах той же подсети, что и IP-адрес коммутатора. На коммутаторе конфигурируется регистрация событий на данных Syslog серверах.

Цель теста: Проверка коммутатора с точки зрения возможности регистрации событий на удаленном Syslog сервере.

Тестовая процедура: Инициировать на коммутаторе отправку сообщения на Syslog сервер.

Ожидаемый результат:

Необходимо:

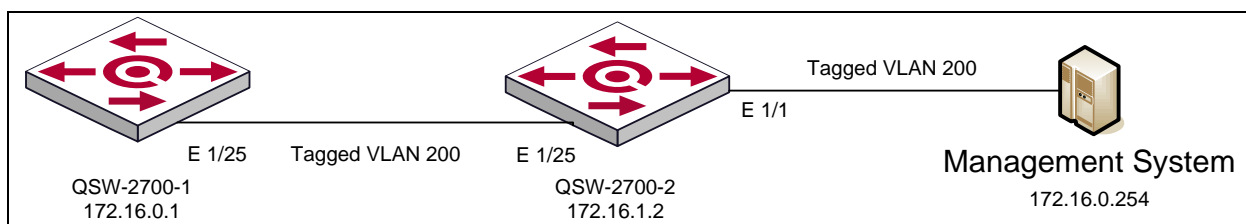
- 1) Убедиться, что коммутатор отправляет информацию о событиях на Syslog сервера
- 2) Проверить корректность отправленных данных.

Краткая конфигурация коммутатора QSW-2700:

```
logging 172.16.0.254 level debugging  
logging 172.16.30.253 level debugging
```

VI. Работа LLDP

Схема:



Исходное состояние: К коммутатору Ethernet подключается к коммутатору с поддержкой протокола LLDP, образуя, таким образом, соседние устройства. На общих портах коммутаторов настраивается протокол LLDP.

Цель теста: Проверить работу протокола LLDP на коммутаторе Ethernet.

Ожидаемый результат: Необходимо:

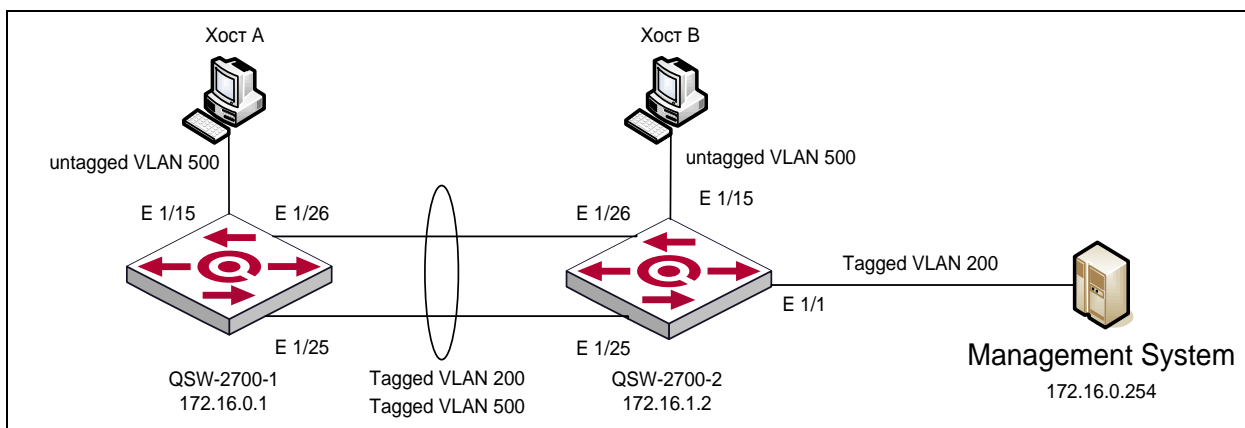
- 1) Убедиться, что устройства установили связь по протоколу LLDP
- 2) Убедиться, что информация о соседнем устройстве корректная.

Краткая конфигурация коммутатора QSW-2700:

```
lldp enable
```

VII. Работа LACP

Схема:



Исходное состояние: Два коммутатора объединены в channel-group. К каждому коммутатору подключено по одному хосту. IP-адреса для указанных хостов конфигурируются вручную. Хосты находятся в одном широковещательном домене и имеют адреса в пределах одной подсети.

Цель теста: Проверка возможности наращивание пропускной способности транспортного уровня посредством объединения интерфейсов.

Тестовая процедура:

- 1) Выполнить пинг между хостами А и В
- 2) Разъединить активный линк Channel group между коммутаторами
- 3) Выполнить пинг между хостами А и В

Ожидаемый результат: Необходимо убедиться в прохождении данных между коммутаторами как при двух линках Channel group, так и при обрыве одного из линков Channel group.

Краткая конфигурация коммутатора QSW-2700-1:

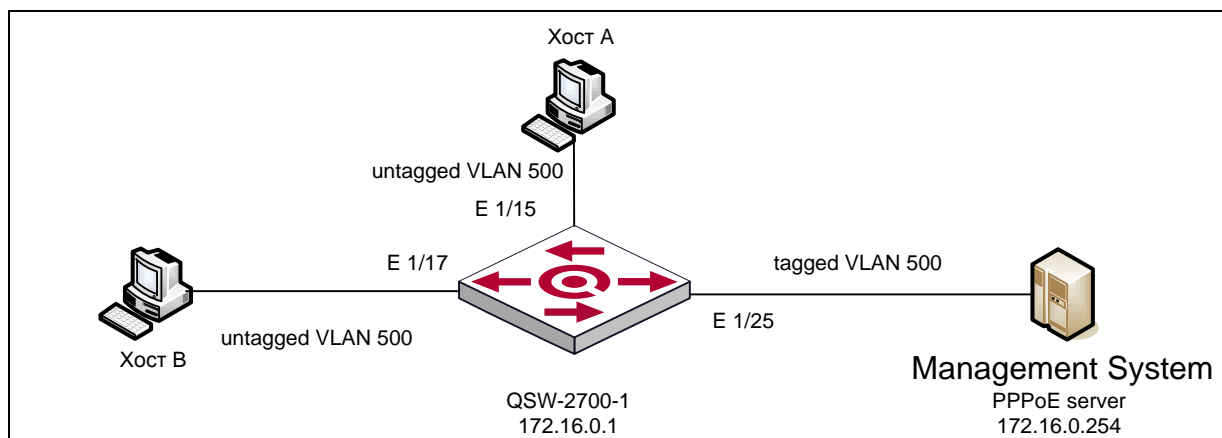
```
port-group 1
!  
Interface Ethernet1/25
  switchport mode trunk
  port-group 1 mode active
!  
Interface Ethernet1/26
  switchport mode trunk
  port-group 1 mode active
!
```

Краткая конфигурация коммутатора QSW-2700-2:

```
!  
port-group 1
!  
Interface Ethernet1/25
  switchport mode trunk
  port-group 1 mode active
!  
Interface Ethernet1/26
  switchport mode trunk
  port-group 1 mode active
!
```

VIII. Поддержка функций PPPoE Intermediate Agent и PPPoE snooping

Схема:



Исходное состояние: К трем портам коммутатора подключено по одному хосту. На хост А установлено программное обеспечение - PPPoE клиент. IP-адрес для IPoE соединения данного хоста устанавливается вручную. IP-адрес для PPPoE соединения данного хоста назначается PPPoE сервером динамически. На Хост В установлено программное обеспечение Wireshark sniffer или аналогичное. IP-адрес Хоста В для IPoE соединения устанавливается вручную. Так же, к коммутатору подключен хост с установленным программным обеспечением - PPPoE сервер. IP адреса для данного хоста устанавливаются вручную. Все хосты находятся в одном широковещательном домене. Порты хостов А и В настраиваются таким образом, чтобы добавлять в PPPoE PADI пакет тег PPPoE intermediate agent. Порт, к которому подключен Хост с PPPoE сервером, объявлен доверенным для PADI пакетов от PPPoE клиентов.

Цель теста: Проверка возможности коммутатора добавлять тег PPPoE intermediate agent в PADI пакеты PPPoE клиентов. Проверка работы функционала PPPoE snooping.

Тестовая процедура: Выполнить подключение Хоста А к PPPoE серверу.

Ожидаемый результат: Необходимо убедиться в том что:

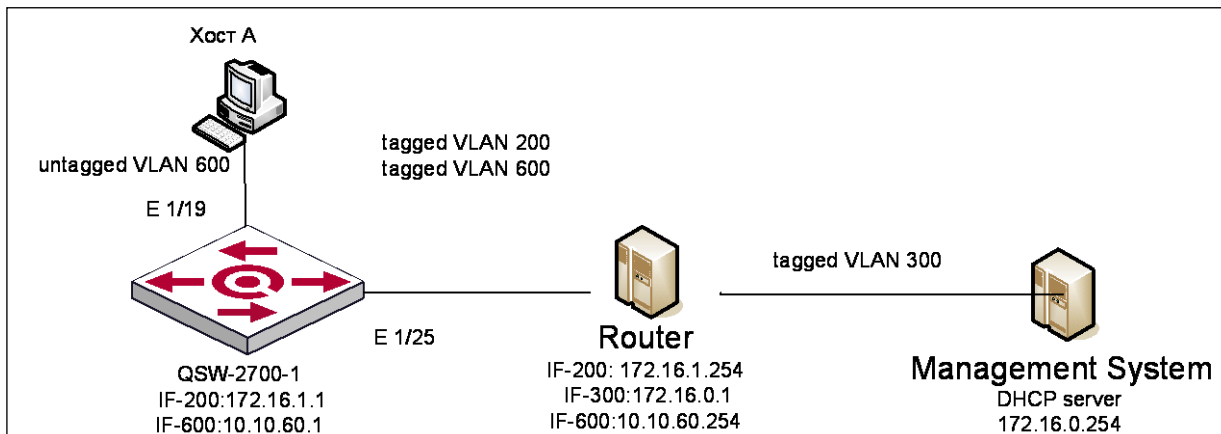
- 1) Хост В не получает PADI пакеты от Хоста А.
- 2) Коммутатор добавляет в PADI пакеты от Хоста А тег PPPoE intermediate agent.

Краткая конфигурация коммутатора QSW-2700-1:

```
pppoe intermediate-agent
!
Interface Ethernet1/15
 switchport mode hybrid
 switchport hybrid allowed vlan 500 untag
 switchport hybrid native vlan 500
 pppoe intermediate-agent
!
Interface Ethernet1/17
 switchport mode hybrid
 switchport hybrid allowed vlan 500 untag
 switchport hybrid native vlan 500
 pppoe intermediate-agent
!
Interface Ethernet1/25
 switchport mode trunk
 pppoe intermediate-agent
```

IX. Поддержка DHCP-Relay

Схема:



Исходное состояние: К коммутатору подключаются оборудование согласно схеме. На хост А установлено программное обеспечение - DHCP клиент. IP-адрес для IPoE соединения данного хоста назначается DHCP сервером динамически. Так же, к коммутатору (через маршрутизатор) подключен хост с установленным программным обеспечением - DHCP сервер. IP адрес для данного хоста устанавливается вручную. Хосты находятся в разных широковещательных доменах. Порт хоста А настраиваются таким образом, чтобы добавлять в DHCP Discover пакет тер Option 82. На коммутаторе настроена трансляция широковещательных пакетов DHCP discover в одноадресные, на DHCP сервер.

Цель теста: Проверить работу трансляции широковещательных пакетов DHCP discover в одноадресные и добавление тега Option82 в DHCP discover пакеты клиентов.

Тестовая процедура: Выполнить процедуру динамического получения IP адреса Хостом А.

Ожидаемый результат: Необходимо убедиться в том, что

- 1) Хост А получил IP адрес от DHCP сервера
- 2) Коммутатор добавляет тер Option82 DHCP Discover пакеты.

Краткая конфигурация коммутатора QSW-2700-1:

```
!
service dhcp
!
ip forward-protocol udp bootps
ip dhcp relay information option
ip dhcp relay information option subscriber-id format hex
!
Interface Ethernet1/19
switchport mode hybrid
switchport hybrid allowed vlan 600 untag
switchport hybrid native vlan 600
!
interface Vlan200
```

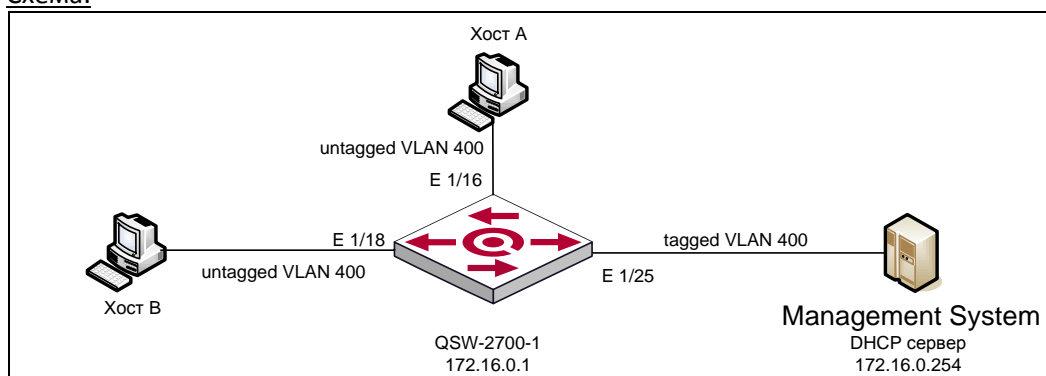
```

ip address 172.16.1.1 255.255.255.0
!
interface Vlan600
ip address 10.10.60.1 255.255.255.0
!forward protocol udp 67(active)!
ip helper-address 172.16.0.254
!
ip default-gateway 172.16.1.254
!

```

Х. Поддержка DHCP Snooping

Схема:



Исходное состояние: К трем портам коммутатора подключено по одному хосту. На хост А установлено программное обеспечение - DHCP клиент. IP-адрес для IPoE соединения данного хоста назначается DHCP сервером динамически. На Хост В установлено программное обеспечение Wireshark sniffer или аналогичное. IP-адрес Хоста В для IPoE соединения устанавливается вручную. Так же, к коммутатору подключен хост с установленным программным обеспечением - DHCP сервер. IP адрес для данного хоста устанавливается вручную. Все хосты находятся в одном широковещательном домене. Порты хостов А и В настраиваются таким образом, чтобы добавлять в DHCP Discover пакет тег Option 82. Порт, к которому подключен Хост с DHCP сервером, объявлен доверенным для DHCP Discover пакетов от DHCP клиентов. На коммутаторе включена функция контроля связи IP-MAC на основе таблицы DHCP-Snooping.

1) Работа DHCP-Snooping

Цель теста: Проверка работы функционала DHCP snooping, а именно, запрета коммутации широковещательных DHCP discover пакетов между DHCP клиентами, подключенными к разным портам.

Тестовая процедура: Выполнить процедуру динамического получения IP адреса Хостом А.

Ожидаемый результат: Необходимо убедиться в том, что коммутатор не отправляет широковещательный пакет DHCP Discover Хосту В, а отправляет только на доверенный порт.

2) Работа DHCP Snooping option82

Цель теста: Проверка возможности коммутатора добавлять тег Option82 в DHCP discovery пакеты от DHCP клиентов.

Тестовая процедура: Выполнить процедуру динамического получения IP адреса Хостом А.

Ожидаемый результат: Необходимо убедиться в том, что коммутатор добавил в DHCP Discover пакет тег Option82.

3) Работа DHCP Snooping User-binding

Цель теста: Проверка возможности коммутатора блокировать трафик от клиентов которые не получили IP адрес от DHCP сервера, то есть связка IP-MAC которых не содержится в таблице клиентов DHCP-Snooping.

Тестовая процедура: Выполнить пинг Хоста с DHCP сервером от Хоста В.

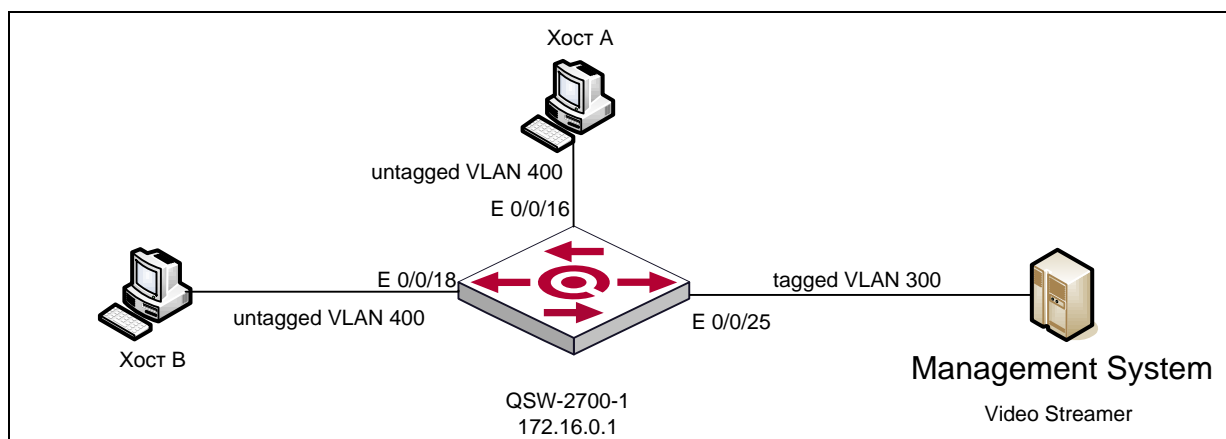
Ожидаемый результат: Необходимо убедиться в том, что пинг дает отрицательный результат.

Краткая конфигурация коммутатора QSW-2700-1:

```
!  
ip dhcp snooping enable  
ip dhcp snooping vlan 400  
  ip dhcp snooping binding enable  
!  
  ip dhcp snooping information enable  
  ip dhcp snooping information option subscriber-id format hex  
!  
Interface Ethernet1/16  
switchport mode hybrid  
  switchport hybrid allowed vlan 400 untag  
  switchport hybrid native vlan 400  
  ip dhcp snooping binding user-control  
!  
Interface Ethernet1/18  
switchport mode hybrid  
  switchport hybrid allowed vlan 400 untag  
  switchport hybrid native vlan 400  
  ip dhcp snooping binding user-control  
!  
Interface Ethernet1/25  
switchport mode trunk  
ip dhcp snooping trust
```

XI. IGMP Snooping, Multicast VLAN, Списки доступа для IGMP запросов

Схема:



Исходное состояние: К портам доступа коммутатора подключаются рабочие станции Хост А и Хост В, используемые в качестве приемников мультикаст потока, порты доступа данных Хостов находятся в PVID VLAN 400. К коммутатору подключается хост с установленным программным обеспечением Video Lan Server или аналогичным по функционалу. Источник генерирует поток на адреса 225.2.2.1-3 в VLAN 300. Коммутатор конфигурируется таким образом, чтобы транслировать мультикастовые потоки, на которые есть подписка из VLAN 300 в VLAN 400. На коммутаторе настраивается IGMP snooping и следующие правила подписки на мультикастовые группы для хостов А и В: группа 225.2.2.1 доступна только хосту А, группа 225.2.2.2 доступна только хосту В, группа 225.2.2.3 доступна обоим хостам. Коммутатор выступает в качестве источника general query v.2.

Цель теста: Проверка работы IGMP Snooping. Проверка коммутатора с точки зрения возможности трансляции Multicast трафика из одного VLAN в другой. Проверка работы списков доступа для IGMP запросов.

Тестовая процедура:

- 1) Ни один из хостов не подписан на вещаемые сервером мультикастовые группы
- 2) Хост А выполняет запрос на присоединение к группе 225.2.2.1
- 3) Хост А выполняет запрос на покидание группы 225.2.2.1
- 4) Хост В выполняет запрос на присоединение к группе 225.2.2.2
- 5) Хост В выполняет запрос на покидание группы 225.2.2.2
- 6) Хост А выполняет запрос на присоединение к группе 225.2.2.2
- 7) Хост В выполняет запрос на присоединение к группе 225.2.2.1
- 8) Хост А выполняет запрос на присоединение к группе 225.2.2.3
- 9) Хост В выполняет запрос на присоединение к группе 225.2.2.3

Ожидаемый результат:

- 1) Ни один их хостов не получает мультикастовый трафик от сервера
- 2)
 - Хост А получает мультикастовый поток для группы 225.2.2.1
 - Хост В не получает мультикастовый трафик от сервера
- 3) Ни один их хостов не получает мультикастовый трафик от сервера
- 4)
 - Хост В получает мультикастовый поток для группы 225.2.2.2
 - Хост А не получает мультикастовый трафик от сервера
- 5) Ни один их хостов не получает мультикастовый трафик от сервера
- 6) Ни один их хостов не получает мультикастовый трафик от сервера
- 7) Ни один их хостов не получает мультикастовый трафик от сервера
- 8) Хост А получает мультикастовый поток для группы 225.2.2.3
- 9) Хост А и получает мультикастовый поток для группы 225.2.2.3

Краткая конфигурация коммутатора QSW-2700-1:

```
vlan 300
 multicast-vlan
 multicast-vlan association 400
!
access-list 6000 permit ip any-source host-destination 225.2.2.1
access-list 6000 permit ip any-source host-destination 225.2.2.3
access-list 6001 permit ip any-source host-destination 225.2.2.2
```



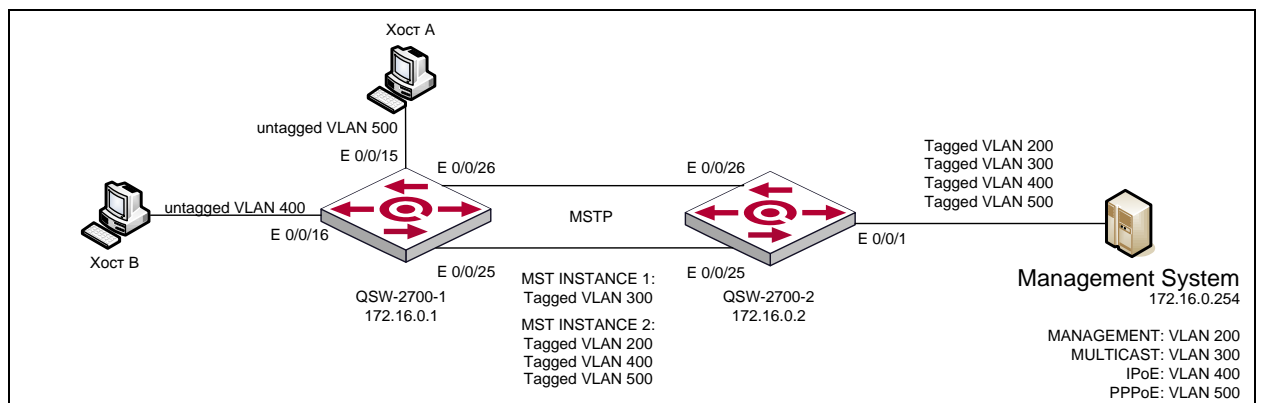
```

access-list 6001 permit ip any-source host-destination 225.2.2.3
!
multicast destination-control
!
Interface Ethernet1/16
 ip multicast destination-control access-group 6000
 switchport mode hybrid
 switchport hybrid allowed vlan 400 untag
 switchport hybrid native vlan 400
!
Interface Ethernet1/18
 ip multicast destination-control access-group 6001
 switchport mode hybrid
 switchport hybrid allowed vlan untag
 switchport hybrid native vlan 400
!
ip igmp snooping
ip igmp snooping vlan 300
ip igmp snooping vlan 300 immediately-leave
ip igmp snooping vlan 300 l2-general-querier
ip igmp snooping vlan 300 l2-general-querier-version 2
ip igmp snooping vlan 300 l2-general-querier-source 1.1.1.1
ip igmp snooping vlan 300 mrouter-port interface Ethernet 1/25
ip igmp snooping vlan 300 interface Ethernet 1/18 limit group 1 strategy replace
ip igmp snooping vlan 300 static-group 225.2.2.1 interface Ethernet 1/1

```

XII. Работа протокола MSTP

Схема:



Исходное состояние: К портам доступа коммутатора подключаются рабочие станции Хост А и Хост В. Коммутаторы подключаются согласно вышеуказанной схеме.

Цель теста: Проверить отказоустойчивость кольцевой схемы на базе протокола MSTP .

Тестовая процедура:

- 1) Разорвать соединение на порту е 1/26
- 2) Восстановить соединение на порту е 1/26
- 3) Разорвать соединение на порту е 1/25
- 4) Восстановить соединение на порту е 1/25

Ожидаемый результат: Убедиться, что после обрыва линков протокол STP активирует резервные соединения, а при восстановлении обрывов блокирует резервные соединения.

Краткая конфигурация коммутатора QSW-2700-1:

```
!  
ip dhcp snooping enable  
ip dhcp snooping vlan 400  
  ip dhcp snooping binding enable  
!  
  ip dhcp snooping information enable  
  ip dhcp snooping information option subscriber-id format hex  
!  
spanning-tree mst configuration  
  instance 0 vlan 1-199;201-299;301-399;401-499;501-4094  
  instance 1 vlan 300  
  instance 2 vlan 200;400;500  
  exit  
!  
spanning-tree  
spanning-tree mst 1 priority 0  
spanning-tree mst 2 priority 0  
!  
vlan 300  
  multicast-vlan  
  multicast-vlan association 400;500  
!  
multicast destination-control  
pppoe intermediate-agent  
!  
Interface Ethernet1/15  
  switchport mode hybrid  
  switchport hybrid allowed vlan 500 untag  
  switchport hybrid native vlan 500  
  pppoe intermediate-agent  
!  
Interface Ethernet1/16  
  switchport mode hybrid  
  switchport hybrid allowed vlan 400 untag  
  switchport hybrid native vlan 400  
  ip dhcp snooping binding user-control  
!  
Interface Ethernet1/25  
  spanning-tree mst 2 port-priority 0  
  switchport mode trunk  
  pppoe intermediate-agent  
  pppoe intermediate-agent trust  
  ip dhcp snooping trust  
!  
Interface Ethernet1/26  
  spanning-tree mst 1 port-priority 0  
  switchport mode trunk  
  pppoe intermediate-agent
```

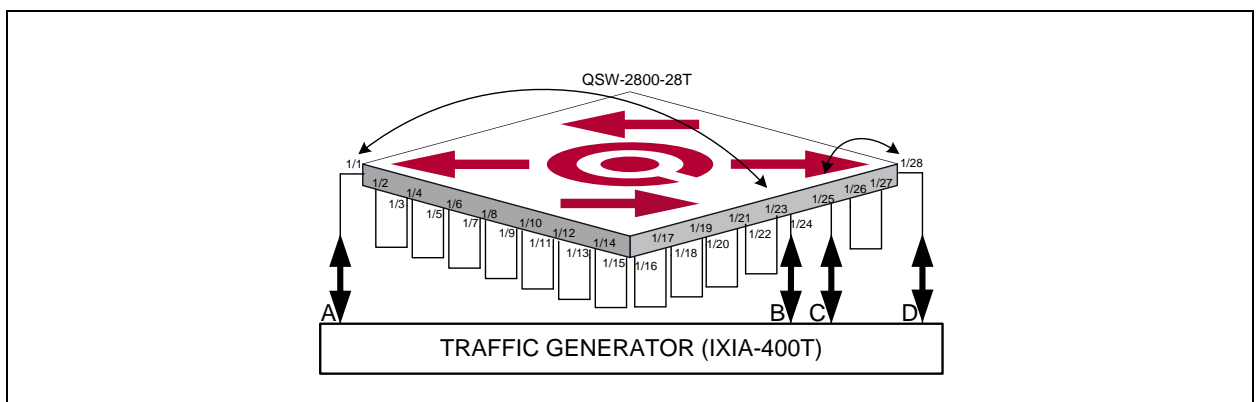
```

pppoe intermediate-agent trust
ip dhcp snooping trust
!
interface Vlan200
 ip address 172.16.0.1 255.255.255.0
!
ip igmp snooping
ip igmp snooping vlan 300
ip igmp snooping vlan 300 immediately-leave
ip igmp snooping vlan 300 l2-general-querier
ip igmp snooping vlan 300 l2-general-querier-version 2
ip igmp snooping vlan 300 l2-general-querier-source 1.1.1.1
ip igmp snooping vlan 300 mrouter-port interface Ethernet1/25
ip igmp snooping vlan 300 mrouter-port interface Ethernet1/26
!
Краткая конфигурация коммутатора QSW-2700-1:
spanning-tree mst configuration
 instance 0 vlan 1-199;201-299;301-399;401-499;501-4094
 instance 1 vlan 300
 instance 2 vlan 200;400;500
 exit
!
spanning-tree

```

XIII. Тест на производительность

Схема:



Исходное состояние: К портам e1/1, e1/24, e1/25, e1/28 коммутатора QSW-2700 подключается Генератор трфика (IXIA-400T). Порты с e1/2 по e1/23, e1/26 и e 1/27 соединяются между собой, согласно вышеуказанной схеме. Скорость сединения каждого порта коммутатора QSW-2700 максимальна (e1/1-24 – 100Mb/s, full-duplex; e1/25-28 – 1Gb/s, full-duplex).

Коммутатор настраивается таким образом, чтобы:

- 1) Траффик от порта А генератора коммутировался в порт В.
- 2) Траффик от порта В генератора коммутировался в порт А.
- 3) Траффик от порта С генератора коммутировался в порт D.
- 4) Траффик от порта D генератора коммутировался в порт С.

На траффик генераторе формируются потоки из фреймов размером 64 байта и

скоростью 100Mb/s для портов А и В, 1Gb/s для портов С и D.

Цель теста: Проверить производительность коммутационной фабрики QSW-2700.

Тестовая процедура:

- 1) Очищается статистика на портах генератора трафика
- 2) На генераторе трафика одновременно запускаются потоки на всех портах на 1 час
- 3) Потоки на генераторе останавливаются
- 4) Производится анализ статистики на портах генератора трафика

Ожидаемый результат: Убедиться, что коммутация осуществляется на скорости портов, то есть:

- 1) Статистика полученных пакетов порта А равна статистике отправленных пакетов порта В
- 2) Статистика полученных пакетов порта В равна статистике отправленных пакетов порта А
- 3) Статистика полученных пакетов порта С равна статистике отправленных пакетов порта D
- 4) Статистика полученных пакетов порта D равна статистике отправленных пакетов порта С

Конфигурация коммутатора QSW-2700:

```
!  
no service password-encryption  
!  
hostname QSW-2700  
sysLocation Russia, Moscow, Novozavodskaya st 18, bld 1  
sysContact support@qtech.ru  
!  
username admin privilege 15 password 0 admin  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
vlan 1;11-24  
!  
Interface Ethernet1/1  
    switchport access vlan 11  
!  
Interface Ethernet1/2  
    switchport access vlan 11  
!  
Interface Ethernet1/3  
    switchport access vlan 12
```

```
!  
Interface Ethernet1/4  
  switchport access vlan 12  
!  
Interface Ethernet1/5  
  switchport access vlan 13  
!  
Interface Ethernet1/6  
  switchport access vlan 13  
!  
Interface Ethernet1/7  
  switchport access vlan 14  
!  
Interface Ethernet1/8  
  switchport access vlan 14  
!  
Interface Ethernet1/9  
  switchport access vlan 15  
!  
Interface Ethernet1/10  
  switchport access vlan 15  
!  
Interface Ethernet1/11  
  switchport access vlan 16  
!  
Interface Ethernet1/12  
  switchport access vlan 16  
!  
Interface Ethernet1/13  
  switchport access vlan 17  
!  
Interface Ethernet1/14  
  switchport access vlan 17  
!  
Interface Ethernet1/15  
  switchport access vlan 18  
!  
Interface Ethernet1/16  
  switchport access vlan 18  
!  
Interface Ethernet1/17  
  switchport access vlan 19  
!  
Interface Ethernet1/18  
  switchport access vlan 19  
!  
Interface Ethernet1/19  
  switchport access vlan 20  
!  
Interface Ethernet1/20  
  switchport access vlan 20  
!  
Interface Ethernet1/21
```

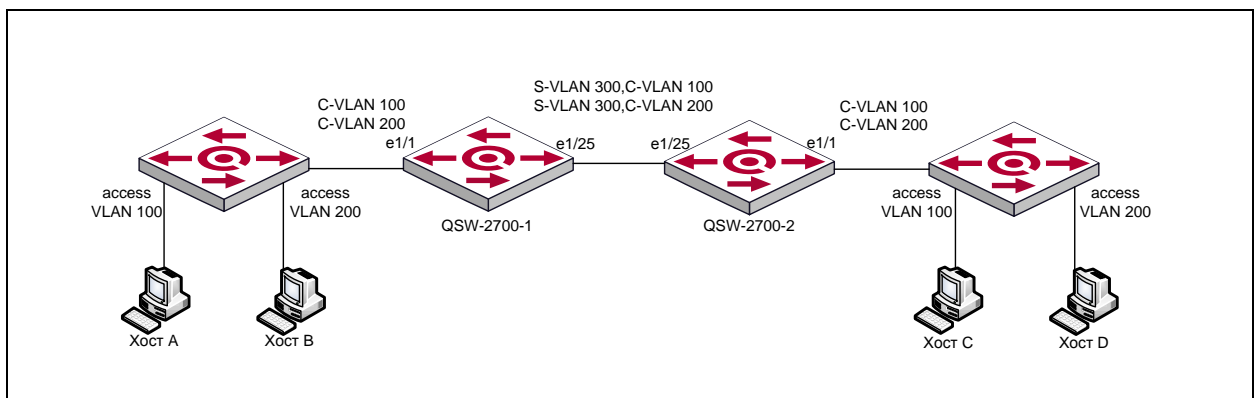
```

switchport access vlan 21
!
Interface Ethernet1/22
switchport access vlan 21
!
Interface Ethernet1/23
switchport access vlan 22
!
Interface Ethernet1/24
switchport access vlan 22
!
Interface Ethernet1/25
switchport access vlan 23
!
Interface Ethernet1/26
switchport access vlan 23
!
Interface Ethernet1/27
switchport access vlan 24
!
Interface Ethernet1/28
switchport access vlan 24
!
interface Vlan1
ip address 192.168.1.1 255.255.255.0
!
no mac-address-learning cpu-control
!
!
no login
!
end

```

XIV. Port-based QinQ

Схема:



Исходное состояние: Согласно схеме, к портам e1/1 коммутаторов QSW-2700 подключаются абонентские устройства поддерживающие стандарт 802.1Q. Трафик от хостов А и С на абонентских устройствах маркируется тегом VLAN 100. Трафик от хостов В и D на абонентских устройствах маркируется тегом VLAN 200 и отправляется на

коммутаторы QSW-2700, на порт e1/1.

Коммутаторы QSW-2700 настраиваются для выполнения следующих задач:

- 1) инкапсулировать весь входящий на порт e1/1 трафик в тег провайдера VLAN300
- 2) снимать на порту e1/1 с исходящего трафика тег провайдера

Коммутаторы QSW-2700 соединены портами e1/25, на этих портах настроен режим trunk и разрешен VLAN 300.

Цель теста: Проверка возможности коммутатора инкапсулировать пользовательские customer VLAN в сервисный provider VLAN на основе PVID порта.

Тестовая процедура:

- 1) Выполнить ping между хостом А и С
- 2) Выполнить ping между хостом А и D
- 3) Выполнить ping между хостом В и D
- 4) Выполнить ping между хостом В и С

Ожидаемый результат: Убедиться, что пинг:

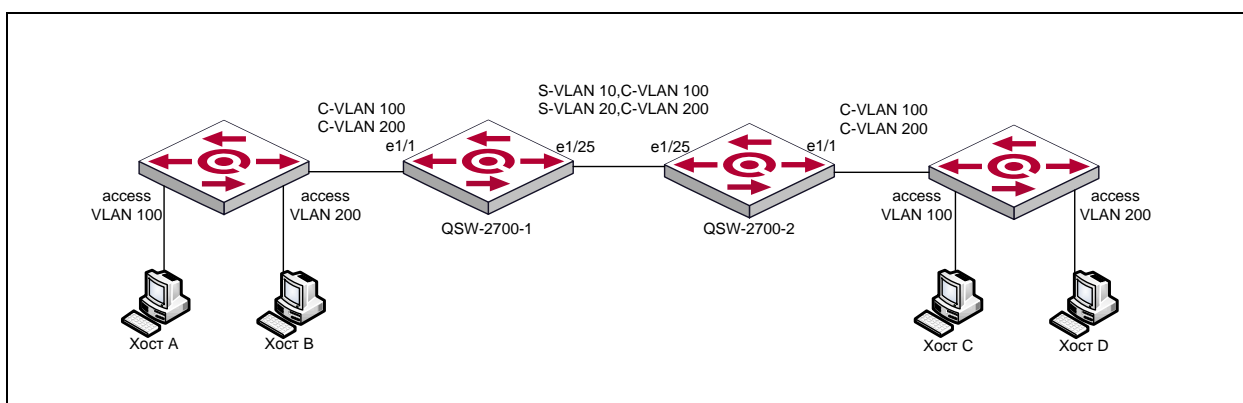
- 1) Дает положительный результат
- 2) Дает отрицательный результат
- 3) Дает положительный результат
- 4) Дает отрицательный результат

Краткая конфигурация коммутаторов QSW-2700 (конфигурация для коммутаторов 1 и 2 идентична):

```
vlan 1;300
!  
Interface Ethernet1/1
 dot1q-tunnel enable
 switchport access vlan 300
!  
Interface Ethernet1/25
 switchport mode trunk
 switchport trunk allowed vlan 300
```

XV. Selective QinQ

Схема:



Исходное состояние: Согласно схеме, к портам e1/1 коммутаторов QSW-2700

подключаются абонентские устройства поддерживающие стандарт 802.1Q. Трафик от хостов А и С на абонентских устройствах маркируется тегом VLAN 100. Трафик от хостов В и D на абонентских устройствах маркируется тегом VLAN 200 и отправляется на коммутаторы QSW-2700, на порт e1/1.

Коммутаторы QSW-2700 настраиваются для выполнения следующих задач:

- 1) инкапсулировать входящий на порт e1/1 трафик с тегом VLAN 100 в тег провайдера VLAN10
- 2) инкапсулировать входящий на порт e1/1 трафик с тегом VLAN 200 в тег провайдера VLAN20
- 3) снимать на порту e1/1 с исходящего трафика теги провайдера

Коммутаторы QSW-2700 соединены портами e1/25, на этих портах настроен режим trunk и разрешены VLAN 10 и VLAN 20.

Цель теста: Проверка возможности коммутатора инкапсулировать пользовательские customer VLAN в сервисный provider VLAN на основе тега C-VLAN абонента.

Тестовая процедура:

- 1) Выполнить ping между хостом А и С
- 2) Выполнить ping между хостом А и D
- 3) Выполнить ping между хостом В и D
- 4) Выполнить ping между хостом В и С

Ожидаемый результат: Убедиться, что пинг:

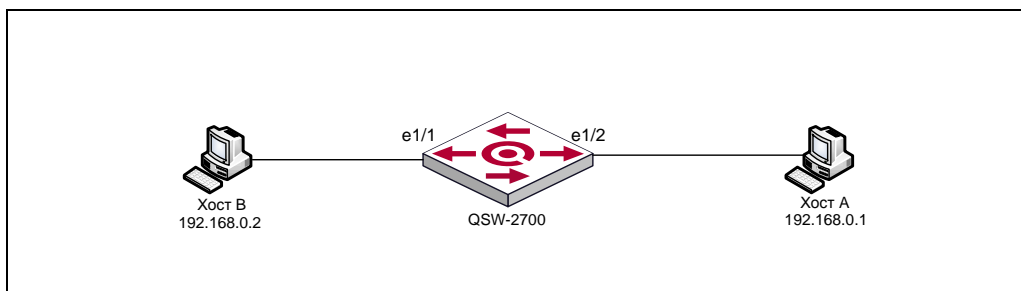
- 1) Дает положительный результат
- 2) Дает отрицательный результат
- 3) Дает положительный результат
- 4) Дает отрицательный результат

Краткая конфигурация коммутаторов QSW-2700 (конфигурация для коммутаторов 1 и 2 идентична):

```
vlan 1;10;20
!
Interface Ethernet1/1
vlan-translation enable
dot1q-tunnel selective s-vlan 10 c-vlan 100
dot1q-tunnel selective s-vlan 20 c-vlan 200
dot1q-tunnel selective enable
switchport mode hybrid
switchport hybrid allowed vlan 10;20 untag
!
Interface Ethernet1/25
switchport mode trunk
switchport trunk allowed vlan 10;20
```


XVI. Jumbo frame

Схема:



Исходное состояние: Согласно вышеуказанной схеме к портам доступа коммутатора подключаются рабочие станции Хост А и Хост В. Хост А и Хост В поддерживают обработку jumbo frame (без фрагментации). На коммутаторе включена поддержка Jumbo frame.

Цель теста: проверить возможность коммутатора обрабатывать пакеты длиной более 1500 байт.

Тестовая процедура: Выполнить ping пакетами размером MTU более 1500 байт между хостом А и С

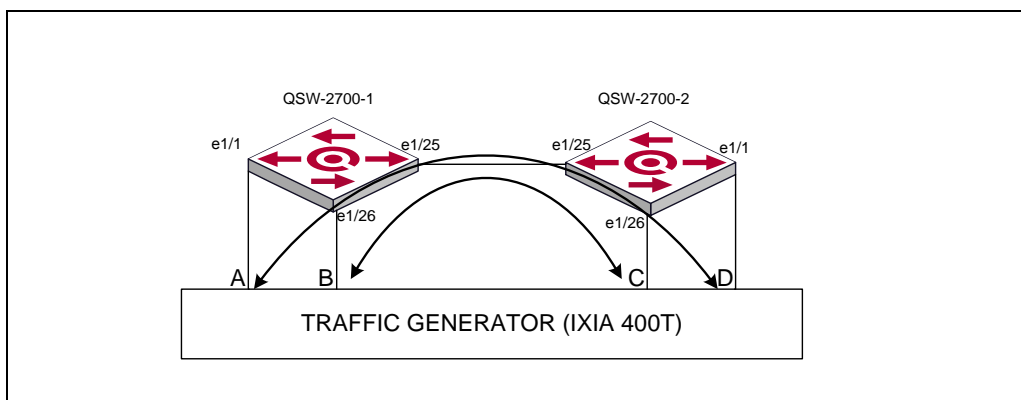
Ожидаемый результат: Результат ping положительный

Краткая конфигурация коммутатора QSW-2700-1:

```
QSW-2700(config)#mtu
```

XVII. Качество обслуживания. COS.

Схема:



Исходное состояние: Согласно вышеуказанной схеме, к портам e1/1, e1/26 коммутаторов QSW-2700 подключается Генератор трафика (IXIA-400T). Коммутаторы QSW-2700-1 и QSW-2700-2 соединяются между собой портами e1/25. Скорость соединения

каждого порта коммутаторов QSW-2700 максимальна (e1/1 – 100Mb/s, full-duplex; e1/25, e1/26 – 1Gb/s, full-duplex). Все используемые для теста порты находятся в одном широковещательном домене и режиме trunk .

На трафик генераторе формируются тегированные 802.1Q потоки из фреймов размером 1300 байт и скоростью 100Mb/s для портов А и D, 1Gb/s для портов В и С. Поле COS тега 802.1Q для портов А и D = 7, для портов В и С = 0.

Адресация L2 для потоков задается таким образом, чтобы:

- 1) Трафик от порта А генератора коммутировался в порт D.
- 2) Трафик от порта D генератора коммутировался в порт А.
- 3) Трафик от порта С генератора коммутировался в порт В.
- 4) Трафик от порта В генератора коммутировался в порт С.

Цель теста: Проверка возможности коммутатора обеспечивать качество обслуживания с обработкой приоритетов в выходных очередях по алгоритму Strict Priority.

Тестовая процедура:

- 1) Очищается статистика на портах генератора трафика
- 2) На генераторе трафика одновременно запускаются потоки на всех портах на 1 час
- 3) Потоки на генераторе останавливаются
- 4) Производится анализ статистики на портах генератора трафика

Ожидаемый результат: Убедиться, что:

- 1) Статистика полученных пакетов порта А равна статистике отправленных пакетов порта D
- 2) Статистика полученных пакетов порта D равна статистике отправленных пакетов порта А
- 3) Статистика полученных пакетов порта С не равна статистике отправленных пакетов порта В (т.е. порт С получил не весь трафик отправленный с порта В)
- 4) Статистика полученных пакетов порта В не равна статистике отправленных пакетов порта С (т.е. порт В получил не весь трафик отправленный с порта С)

Краткая конфигурация коммутаторов QSW-2700 (конфигурация для коммутаторов 1 и 2 идентична):

```
vlan 1;500
!
mls qos queue algorithm sp
!
Interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 500
!
Interface Ethernet1/25
  switchport mode trunk
  switchport trunk allowed vlan 500
```

```
!  
Interface Ethernet1/26  
  switchport mode trunk  
  switchport trunk allowed vlan 500  
!
```

Приложение 1. Образец конфигурационного файла для коммутатора QSW-2700

```
!  
no service password-encryption  
!  
hostname QSW-2700-1  
sysLocation Russia, Moscow, Novozavodskaya st 18, bld 1  
sysContact www.qtech.ru  
!  
username admin privilege 15 password 0 123456  
!  
authentication line console login local tacacs  
authentication line vty login local tacacs  
authentication line web login local tacacs  
authentication enable local tacacs  
authorization line console exec local tacacs  
authorization line vty exec local tacacs  
authorization line web exec local tacacs  
!  
!  
clock timezone MOSCOW add 4 0  
!  
logging 172.16.0.254  
!  
ssh-server enable  
!  
ip http server  
!  
tacacs-server key tacacs  
tacacs-server authentication host 172.16.0.254  
!  
snmp-server enable  
snmp-server securityip 172.16.0.254  
snmp-server community rw private  
snmp-server community ro public  
!  
service dhcp  
!  
ip forward-protocol udp bootps  
ip dhcp relay information option  
ip dhcp relay information option subscriber-id format hex  
!  
ip dhcp snooping enable  
ip dhcp snooping vlan 400  
ip dhcp snooping binding enable  
!  
ip dhcp snooping information enable
```

```

ip dhcp snooping information option subscriber-id format hex
!
!
!
!
lldp enable
!
spanning-tree mst configuration
instance 0 vlan 1-199;201-299;301-399;401-499;501-4094
instance 1 vlan 300
instance 2 vlan 200;400;500
exit
!
spanning-tree
spanning-tree mst 1 priority 0
spanning-tree mst 2 priority 0
!
!
!
vlan 1;200;400;500;600
!
vlan 300
multicast-vlan
multicast-vlan association 400;500
!
firewall enable
!
access-list 6000 permit ip any-source host-destination 225.2.2.1
access-list 6000 permit ip any-source host-destination 225.2.2.3
access-list 6001 permit ip any-source host-destination 225.2.2.2
access-list 6001 permit ip any-source host-destination 225.2.2.3
access-list 100 deny ip any-source host-destination 172.16.1.194
access-list 1100 deny any-source-mac host-destination-mac 00-24-54-b8-e9-bf
access-list 3100 deny host-source-mac 00-24-54-b8-e9-bf any-destination-mac ip host-source
172.16.1.194 any-destination
!
multicast destination-control
pppoe intermediate-agent
mls qos
priority-queue out
!
radius-server key radius
radius-server authentication host 172.16.0.254
aaa enable
!
Interface Ethernet1/1
mac-ip access-group 3100 in
loopback-detection specified-vlan 1
loopback-detection control shutdown
!
Interface Ethernet1/2
mac access-group 1100 in
!

```

```
Interface Ethernet1/3
  ip access-group 100 in
  !
Interface Ethernet1/4
  !
Interface Ethernet1/5
  !
Interface Ethernet1/6
  !
Interface Ethernet1/7
  !
Interface Ethernet1/8
  !
Interface Ethernet1/9
  !
Interface Ethernet1/10
  switchport mac-address dynamic maximum 1
  !
Interface Ethernet1/11
  !
Interface Ethernet1/12
  !
Interface Ethernet1/13
  !
Interface Ethernet1/14
  !
Interface Ethernet1/15
  switchport mode hybrid
  switchport hybrid allowed vlan 500 untag
  switchport hybrid native vlan 500
  pppoe intermediate-agent
  !
Interface Ethernet1/16
  ip multicast destination-control access-group 6000
  switchport mode hybrid
  switchport hybrid allowed vlan 400 untag
  switchport hybrid native vlan 400
  ip dhcp snooping binding user-control
  !
Interface Ethernet1/17
  switchport mode hybrid
  switchport hybrid allowed vlan 500 untag
  switchport hybrid native vlan 500
  pppoe intermediate-agent
  !
Interface Ethernet1/18
  ip multicast destination-control access-group 6001
  service-policy input pppoe
  switchport mode hybrid
  switchport hybrid allowed vlan 400;500 untag
  switchport hybrid native vlan 400
  ip dhcp snooping binding user-control
  !
```

```

Interface Ethernet1/19
  switchport mode hybrid
  switchport hybrid allowed vlan 600 untag
  switchport hybrid native vlan 600
!
Interface Ethernet1/20
  switchport mode hybrid
  switchport hybrid allowed vlan 300 untag
  switchport hybrid native vlan 300
!
Interface Ethernet1/21
  switchport mode hybrid
  switchport hybrid allowed vlan 300 untag
  switchport hybrid native vlan 300
!
Interface Ethernet1/22
!
Interface Ethernet1/23
!
Interface Ethernet1/24
!
Interface Ethernet1/25
  spanning-tree mst 2 port-priority 0
  switchport mode trunk
  pppoe intermediate-agent
  pppoe intermediate-agent trust
  ip dhcp snooping trust
!
Interface Ethernet1/26
  spanning-tree mst 1 port-priority 0
  spanning-tree mst 1 cost 2000
  switchport mode trunk
!
Interface Ethernet1/27
!
Interface Ethernet1/28
!
interface Vlan200
  ip address 172.16.0.1 255.255.255.0
!
interface Vlan600
  ip address 10.10.60.1 255.255.255.0
  !forward protocol udp 67(active)!
  ip helper-address 172.16.0.254
!
ip igmp snooping
ip igmp snooping vlan 300
ip igmp snooping vlan 300 immediately-leave
ip igmp snooping vlan 300 I2-general-querier
ip igmp snooping vlan 300 I2-general-querier-version 2
ip igmp snooping vlan 300 I2-general-querier-source 1.1.1.1
ip igmp snooping vlan 300 mrouter-port interface Ethernet1/25
ip igmp snooping vlan 300 mrouter-port interface Ethernet1/26

```

```
!  
mac-address-learning cpu-control  
!  
ip default-gateway 172.16.0.254  
!  
snmp server 172.16.0.254  
!  
no login  
!  
!  
end
```


Приложение 2. Протокол тестирования коммутатора QSW-2700

Тест №	Наименование теста	Результат	Примечание
Управление коммутатором			
1)	<i>Управление по протоколу TELNET</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
2)	<i>Управление по протоколу HTTP</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
3)	<i>Управление по протоколу SSH</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
4)	<i>Управление по протоколу SNMP</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Аутентификация пользователей на коммутаторе			
1)	<i>Поддержка RADIUS</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
2)	<i>Поддержка TACACS+</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Безопасность на портах доступа			
1)	<i>Изоляция портов</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
2)	<i>Работа ACL</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
3)	<i>Обнаружение петель на стороне клиента</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
4)	<i>Ограничение количества MAC адресов на порту</i>	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Синхронизация даты и времени с NTP сервером		прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Работа Syslog		прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Работа LLDP		прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Работа LACP		прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Поддержка функций PPPoE Intermediate Agent и PPPoE snooping		прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	

Поддержка DHCP-Relay	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Поддержка DHCP Snooping	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
IGMP Snooping, Multicast VLAN, Списки доступа для IGMP запросов	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Работа протокола MSTP	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Тест на производительность	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Port-based QinQ	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Selective QinQ	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Jumbo frame	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	
Качество обслуживания. COS.	прошел: <input type="checkbox"/> не прошел: <input type="checkbox"/>	

Комментарии к результату теста:

Подпись:	Представитель QTECH:	Представитель _____:
	_____	_____
	_____	_____