Разработал: преподаватель кафедры СМС, Якушев И.Ю.

Лабораторная работа 1
Настройка STP

Цель работы: научиться настраивать STP протокол на коммутаторах.

Теория

VLAN (Virtual Local Area Network) – топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3 Ethernet.

Терминология:

- access port — порт, принадлежащий одному VLAN'у и передающий нетегированный трафик.
- trunk port — порт, передающий тегированный трафик одного или нескольких VLAN'ов.

Создание VLAN'а с идентификатором 2 и задание имени для него:

```
sw1(config)# vlan 2
sw1(config-vlan)# name test
```

Создание VLAN'ов с идентификаторами 2, 10 и 15:

```
sw3(config)# vlan 2,10,15
```

Удаление VLAN'а с идентификатором 2:

```
sw1(config)# no vlan 2
```

Настройка access портов

Назначение порта коммутатора в VLAN:

```
sw1(config)# interface fa0/1
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 2
```

Просмотр информации о VLAN'ах:

```
sw1# show vlan brief
VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                          active    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

2    test                             active    Fa0/1, Fa0/2

10   VLAN0010                         active    Fa0/4, Fa0/5

15   VLAN0015                         active    Fa0/3
```

Настройка транка (trunk)

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.

Режимы интерфейса (режим по умолчанию зависит от модели коммутатора):

- auto — Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. Т.е. если порты на обоих концах находятся в режиме "auto", то trunk применяться не будет.
- desirable — Порт находится в режиме "готов перейти в состояние trunk"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto).
- trunk — Порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим.
- nonegotiate — Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'a.

По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

VLAN можно создать на коммутаторе с помощью команды vlan. Кроме того, VLAN автоматически создается на коммутаторе в момент добавления в него интерфейсов в режиме access.

Настройка статического транка

Создание статического транка:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport mode trunk
```

На некоторых моделях коммутаторов (на которых поддерживается ISL) после попытки перевести интерфейс в режим статического транка, может появится такая ошибка:

```
sw1(config-if)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is “Auto” can not be configured to “trunk” mode.
```

Это происходит из-за того, что динамическое определение инкапсуляции (ISL или 802.1Q) работает только с динамическими режимами транка. И для того, чтобы настроить статический транк, необходимо инкапсуляцию также настроить статически.

Для таких коммутаторов необходимо явно указать тип инкапсуляции для интерфейса:

```
sw1(config-if)# switchport trunk encapsulation dot1q
```

И после этого снова повторить команду настройки статического транка (switchport mode trunk).

Разрешённые VLAN'ы

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.

Указать перечень разрешенных VLAN для транкового порта fa0/22:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan 1-2,10,15
```

Добавление ещё одного разрешенного VLAN:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN из списка разрешенных:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan remove 160
```

Native VLAN

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка VLAN 5 как native:

```
sw1(config-if)# switchport trunk native vlan 5
```

Теперь весь трафик, принадлежащий VLAN'у 5, будет передаваться через транковый интерфейс нетегированным, а весь пришедший на транковый интерфейс нетегированный трафик будет промаркирован как принадлежащий VLAN'у 5 (по умолчанию VLAN 1).

Протокол STP

STP (Spanning Tree Protocol) — сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях. Первоначальный протокол STP описан в стандарте 802.1D. Позже появилось несколько новых протоколов (RSTP, MSTP, PVST, PVST+), отличающихся некоторыми особенностями в алгоритме работы, в скорости, в отношении к VLANам и ряде других вопросов, но в целом решающих ту же задачу похожими способами. Все их принято обобщённо называть STP-протоколами.

Описание протокола STP

Протокол работает на канальном уровне. STP позволяет делать топологию избыточной на физическом уровне, но при этом логически блокировать петли. Достигается это с помощью того, что STP отправляет сообщения BPDU и обнаруживает фактическую топологию сети. А затем, определяя роли коммутаторов и портов, часть портов блокирует так, чтобы в итоге получить топологию без петель.

Для того чтобы определить какие порты заблокировать, а какие будут передавать данные, STP выполняет следующее:

- Выбор корневого моста (Root Bridge)
- Определение корневых портов (Root Port)
- Определение выделенных портов (Designated Port)

Выбор корневого моста

Корневым становится коммутатор с наименьшим идентификатором моста (Bridge ID).

Только один коммутатор может быть корневым. Для того чтобы выбрать корневой коммутатор, все коммутаторы отправляют сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID.

В итоге только один коммутатор останется корневым и будет передавать BPDU.

Изначально Bridge ID состоял из двух полей:

- Приоритет — поле, которое позволяет административно влиять на выборы корневого коммутатора. Размер — 2 байта,
- MAC-адрес — используется как уникальный идентификатор, который, в случае совпадения значений приоритетов, позволяет выбрать корневой коммутатор. Так как MAC-адреса уникальны, то и Bridge ID уникален, так что какой-то коммутатор обязательно станет корневым.

Определение корневых портов

Порт коммутатора, который имеет кратчайший путь к корневому коммутатору, называется корневым портом. У любого не корневого коммутатора может быть только один корневой порт. Корневой порт выбирается на основе меньшего Root Path Cost - это общее значение стоимости всех линков до корневого коммутатора. Если стоимость линков до корневого коммутатора совпадает, то выбор корневого порта происходит на основе меньшего Bridge ID коммутатора. Если и Bridge ID коммутаторов до корневого коммутатора совпадает, то тогда корневой порт выбирается на основе Port ID.

Определение назначенных портов

Коммутатор в сегменте сети, имеющий наименьшее расстояние до корневого коммутатора, называется назначенным коммутатором (мостом). Порт этого коммутатора, который подключен к рассматриваемому сегменту сети называется назначенным портом. Так же как и корневой порт выбирается на основе:

- Меньшего Root Path Cost.
- Меньшего Bridge ID.
- Меньшего Port ID.

Роли и состояния портов

Роли портов:

- Root Port — корневой порт коммутатора
- Designated Port — назначенный порт сегмента
- Nondesignated Port — неназначенный порт сегмента
- Disabled Port — порт который находится в выключенном состоянии.

Состояния портов:

- Blocking — блокирование
- Listening — прослушивание
- Learning — обучение
- Forwarding — пересылка

Петли в сети

Петли в коммутируемой сети могут возникнуть по нескольким причинам:

- Отключен STP;
- PVST BPDU передает идентификатор VLAN. Если на access-интерфейсе полученный идентификатор VLAN'а не совпадает с VLAN ID в котором было получено BPDU, то порт переводится в заблокированное состояние для этого VLAN;
- Различные версии STP;
- Разные native VLAN'ы на концах транка;
- Слишком маленькие таймеры STP;
- Большое количество хопов в топологии STP.

Настройка Rapid PVST+

Включение Rapid PVST:

```
sw(config)# spanning-tree mode rapid-pvst
```

Port Fast

Portfast — функция, которая позволяет порту пропустить состояния listening и learning и сразу же перейти в состояние forwarding. Настраивается на портах уровня доступа, к которым подключены пользователи или сервера.

Фактически, PortFast меняет две вещи в стандартной работе STP:

- порт пропускает состояния listening и learning

- при изменении статуса порта, не отправляется сообщение о изменении состояния порта TCN BPDU (topology change notification BPDU)

Когда на интерфейсе включен PortFast, он все равно отправляет BPDU.
Но если включить PortFast на портах, которые соединены с другими коммутаторами, то есть риск создания петли. Так как, после получения BPDU порт остается в состоянии Forwarding. За это время, уже может образоваться петля.
Поэтому, в связке с PortFast, как правило, используется BPDUGuard (хотя и это, конечно же, не даст 100% гарантии, что не будет петли).

Настройка Port Fast

Синтаксис команды для настройки Port Fast на интерфейсе:

```
sw(config-if)# spanning-tree portfast [disable | trunk]
```

Настройка Port Fast на access-интерфейсе:

```
sw(config)#interface fa0/1
sw(config-if)# spanning-tree portfast
```

Настройка Port Fast на интерфейсе, который работает в режиме trunk (тегированый порт):

```
sw(config)#interface fa0/1
sw(config-if)# spanning-tree portfast trunk
```

Если на интерфейсе, который работает в режиме транка выполнить команду без параметра trunk, то функция Port Fast не будет применена.
Функцию Port Fast можно настроить глобально на всех интерфейсах в режиме access:

```
sw(config)#spanning-tree portfast default
```

Отключить Port Fast на интерфейсе:

```
sw(config-if)# spanning-tree portfast disable
```

Просмотр информации о настройках Port Fast

Просмотр информации о статусе функции Port Fast на интерфейсе:

```
sw# show spanning-tree interface fa 0/1 portfast
VLAN0001            enabled
```

Просмотр информации о настройках spanning-tree на интерфейсе:

```
sw# show spanning-tree interface fa 0/1  detail
Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32769, address 000a.b8ab.eb80
  Designated bridge has priority 32769, address 0012.0111.e580
  Designated port id is 128.1, designated path cost 19
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
  BPDU: sent 75684, received 0
```

Если Port Fast была включена глобально на всех access-портах, то это можно посмотреть в суммарной информации о настройках STP на коммутаторе:

```
sw# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      1         0        0          3          4
```

```
---------------------- -------- --------- -------- ---------- ----------
1 vlan                        1         0        0          3          4
```

BPDU Guard

BPDU Guard — функция, которая позволяет выключать порт при получении BPDU.
Может быть включена глобально на коммутаторе или на интерфейсе, у этих режимов есть некоторые отличия:

- Если BPDU Guard включена глобально на коммутаторе, то для портов с включенной функцией Port Fast:
  - ✓ при корректной настройке, порты с включенным Port Fast не должны получать BPDU,
  - ✓ получение BPDU на портах с Port Fast говорит о неправильных настройках или о том, что подключено неавторизованное устройство,
  - ✓ при получении BPDU на интерфейсе, функция BPDU Guard переведет его в состояние error-disabled,
- Если BPDU Guard включена на интерфейсе (без включения функции Port Fast):
  - ✓ при получении BPDU на интерфейсе, функция BPDU Guard переведет его в состояние error-disabled.

Настройка BPDU Guard

Включение BPDU Guard глобально на коммутаторе, на портах с включенной функцией Port Fast:

```
sw(config)# spanning-tree portfast bpduguard default
```

Хотя в команде, которая включает BPDU Guard глобально на коммутаторе, есть параметр portfast, применение этой команды не включает функцию Port Fast. Она должна быть настроена отдельно.
Настройка BPDU Guard на интерфейсе:

```
sw(config)#interface fa0/1
sw(config-if)# spanning-tree bpduguard enable
```

Просмотр информации о настройках BPDU Guard

Просмотр информации о настройках spanning-tree на интерфейсе:

```
sw1#sh span int fa0/1 detail
Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32769, address 000a.b8ab.eb80
  Designated bridge has priority 32769, address 0012.0111.e580
  Designated port id is 128.1, designated path cost 19
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  Bpdu guard is enabled
  BPDU: sent 116964, received 0
```

Если функция BPDU Guard была включена глобально на коммутаторе, то это можно посмотреть в суммарной информации о настройках STP на коммутаторе:

```
sw1#sh span summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
```

VLAN0001	1	0	0	3	4
1 vlan	1	0	0	3	4

Задание

В Cisco Packet Tracer нужно промоделировать схему, изображенную на рис. 1.

Необходимо произвести настройку STP-протокола на коммутаторах с учетом указанных VLAN. Нужно настроить основной и вспомогательный корневой мост в схеме и проверить сходимость PVST+. Настройте режим Rapid PVST+ на всех коммутаторах и функции PortFast, BPDU Guard на портах доступа. При проверке работы протокола STP используйте обрыв канала между коммутаторами либо переход интерфейса коммутатора в состояние Down.

После настройки протокола STP проверить связность сети между оконечными устройствами (отправкой ICMP-пакетов) в своем VLAN. Адреса выдавать устройствам динамически и/или задавать статически. Также каждое сетевое устройство (коммутатор) должно быть доступно с сервера в Management VLAN.

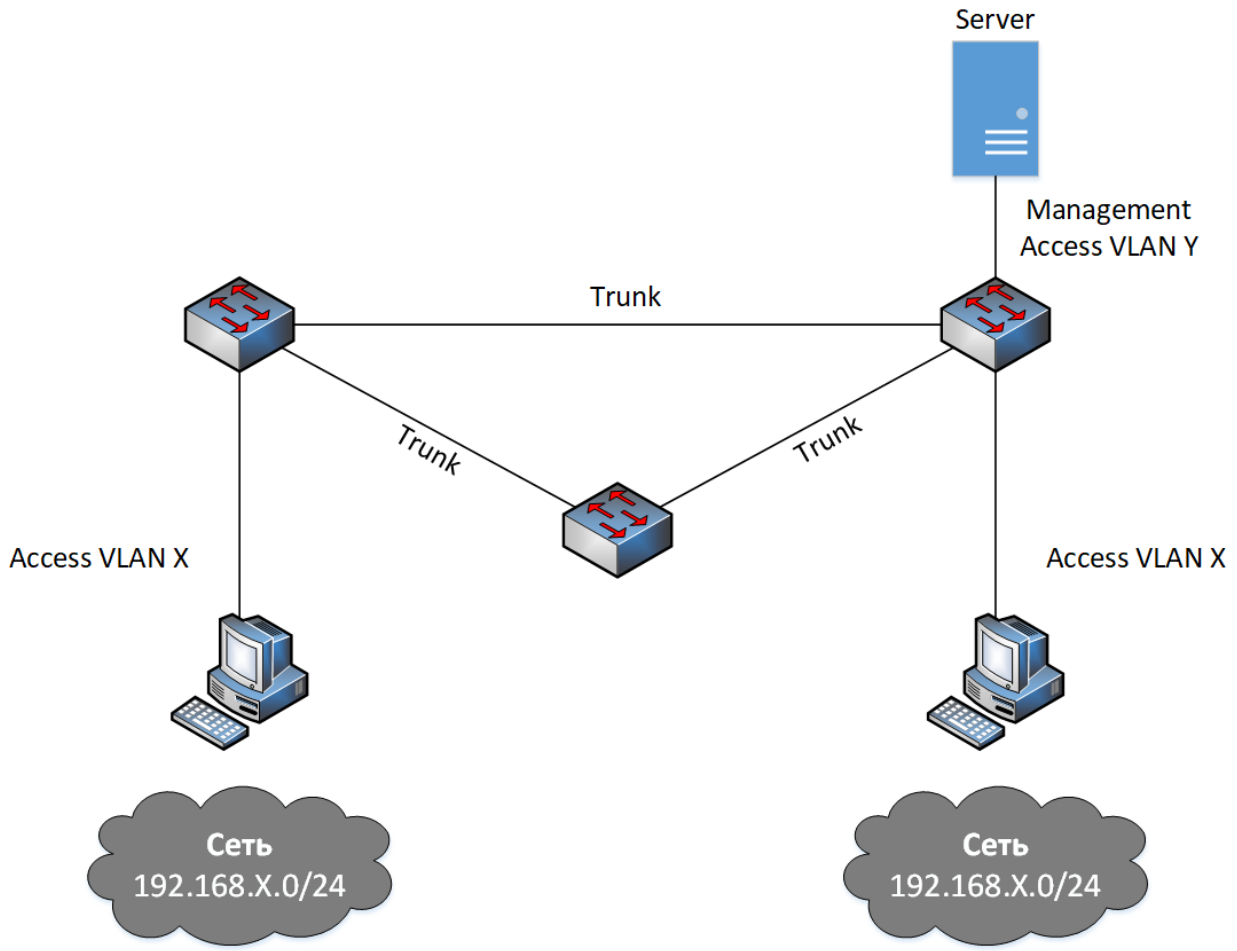

Рисунок 1 – Схема сети

Исходные данные выбирать следующим образом (вариант N выбирать по двум последним цифрам пароля): X = N, Y = N +100.

Лабораторные работы требуют для своего выполнения наличия на компьютере сетевого симулятора Cisco Packet Tracer. Ссылка на бесплатную версию CPT для студентов: http://blog.netskills.ru/2015/02/cisco-packet-tracer-62-download-cisco.html

Оформление лабораторных работ

В качестве результата выполнения лабораторной работы студент должен выслать преподавателю два файла: отчёт в формате doc/docx или pdf и файл модели в формате .pkt.

Отчёт оформляется в соответствии с требованиями ГОСТ 7.32–2017 «Отчет о научно-исследовательской работе» и ГОСТ 2.105–95 «Общие требования к текстовым документам» и состоит из следующих элементов:

1. Титульный лист.
2. Содержание (с нумерацией страниц).
3. Задание в соответствии с вариантом.
4. Структурная схема сети в соответствии с заданием.
5. Выполнение лабораторной работы в соответствии с заданием с описанием всех значащих этапов.
6. Скриншоты результатов (команд и откликов на них) выполнения пунктов задания лабораторной работы.
7. Выводы по проделанной работе.
8. Краткие ответы на контрольные вопросы.
9. Список литературы (по ГОСТ 7.1-2019).

Рисунки (графики, скриншоты, схемы, диаграммы и пр.), таблицы, формулы и другие объекты отчёта должны быть пронумерованы и подписаны в соответствии с ГОСТ 2.105-95.

Контрольные вопросы

- Коммутатор
- Access, Trunk и General VLAN
- Management VLAN
- Native VLAN
- STP
- PortFast
- BPDU Guard
- Rapid PVST+

Список литературы

1. Курс «Introduction to Packet Tracer» [Электронный ресурс] / Сетевая академия Cisco. Режим доступа: https://www.netacad.com/ru/courses/packet-tracer-download/
2. Принцип работы протокола STP [Электронный ресурс] / Режим доступа: https://habr.com/ru/post/419491/
3. Молочков В.П. Работа в программе Cisco Packet Tracer: эл.книга / ИНТУИТ, 2016.
4. Курс «Работа в программе Cisco Packet Tracer» [Электронный ресурс] / Режим доступа: https://www.intuit.ru/studies/courses/3549/791/info
5. VLAN в Cisco [Электронный ресурс] / Режим доступа: http://xgu.ru/wiki/VLAN_в_Cisco
6. STP [Электронный ресурс] / Режим доступа: http://xgu.ru/wiki/STP