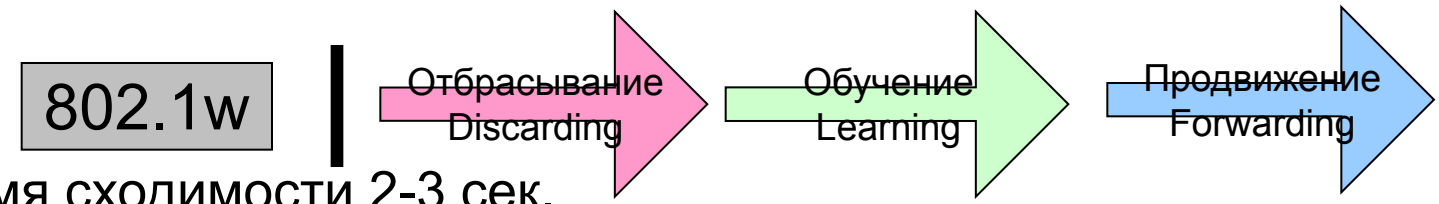
Функции повышения надежности сети

1.1 Протокол Rapid Spanning Tree Protocol

- Описывается стандартом IEEE 802.1w
- Предназначен для исключения петель в L2 сети и обеспечивает более быструю сходимость по сравнению с классическим STP
- Три состояний портов:
  - Отбрасывание (**Discarding**) - входящие пакеты отбрасываются, MAC адреса не изучаются
  - Обучение (**Learning**) - входящие пакеты отбрасываются, но изучаются MAC адреса
  - Продвижение (**Forwarding**) – пакеты коммутируются в соответствии с изученными MAC адресами

При включении порт поочередно проходит все состояния

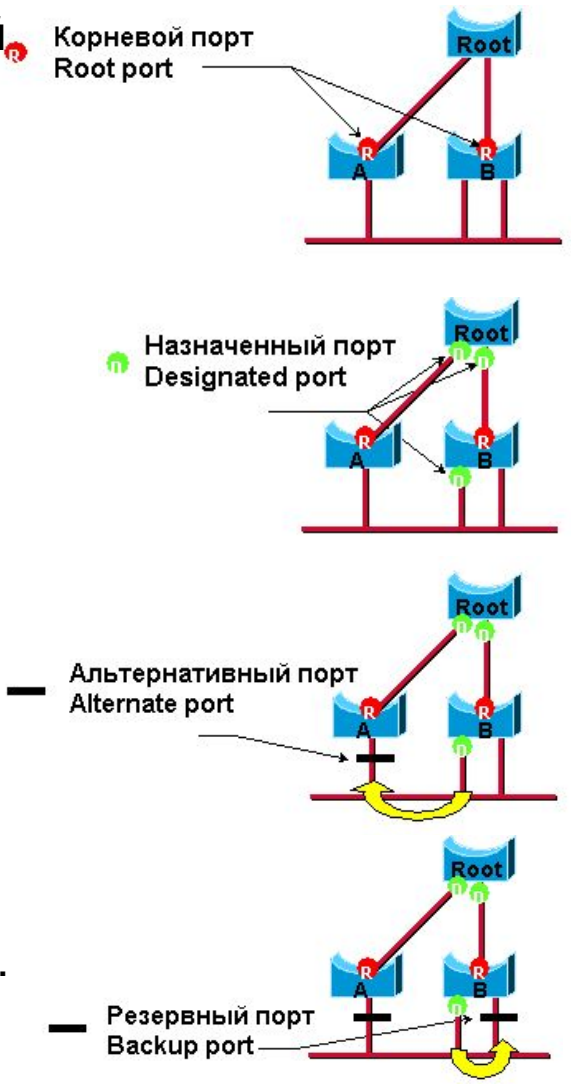


- Время сходимости 2-3 сек.
- Диаметр 18 переходов
- Ограничение: единое RSTP дерево для всех VLAN, обходится применением Multiple Spanning Tree, MSTP (IEEE 802.1s)

1.1 Протокол Rapid Spanning Tree Protocol

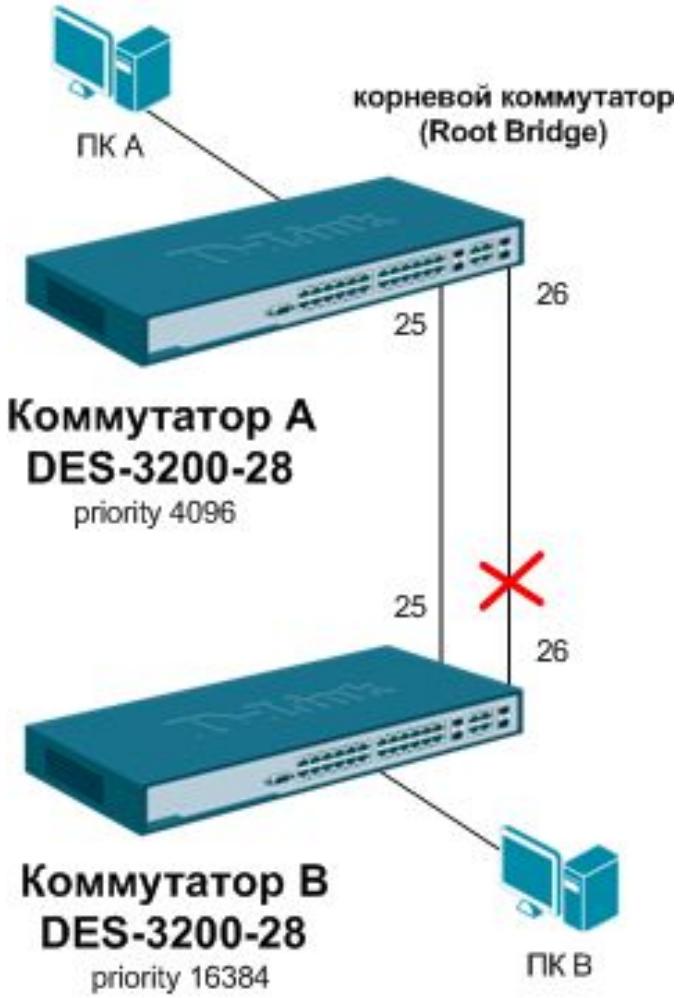
Определено четыре роли портов:

- Корневой порт (**Root port**) – порт с наименьшей стоимостью пути (Root Path Cost) до корневого коммутатора (Root Bridge). Должен быть только один у каждого коммутатора.
- Назначенный порт (**Designated port**) - порт, по которому стоимость пути до корневого коммутатора для сегмента LAN минимально. Каждый L2 сегмент должен иметь только один Назначенный порт.
- Альтернативный порт (**Alternate port**) – порт, имеющий альтернативный путь к корневому коммутатору относительно корневого порта, и заблокированный в данный момент.
- Резервный порт (**Backup port**) – порт, обеспечивающий резервное подключение к L2 сегменту, в котором уже есть порт коммутатора.



Настройка RSTP

1. Включить RSTP на обоих коммутаторах.
2. Проверить, что порт 26 заблокирован: **show stp ports 26**
3. Запустить ping между Comp A и Comp B.
4. Отсоединить кабель 25 порта, проверить, сколько пакетов будет пропущено и через сколько восстановится связь
5. Подключить кабель обратно и посмотреть за изменениями



Настройка RSTP

Коммутатор A:

```
config ipif System ipaddress 10.90.90.90/24 vlan default
config stp ports 25-28 state enable        #включить STP на магистральных портах
config stp priority 4096 instance_id 0     #выставить меньший приоритет
config stp version rstp                    #указать версию STP
enable stp                                 #включить глобально STP
```

Коммутатор B:

```
config ipif System ipaddress 10.90.90.91/24 vlan default
config stp ports 25-28 state enable        #включить STP на магистральных портах
config stp priority 16384 instance_id 0    #выставить больший приоритет
config stp version rstp                    #указать версию STP
enable stp                                 #включить глобально STP
```

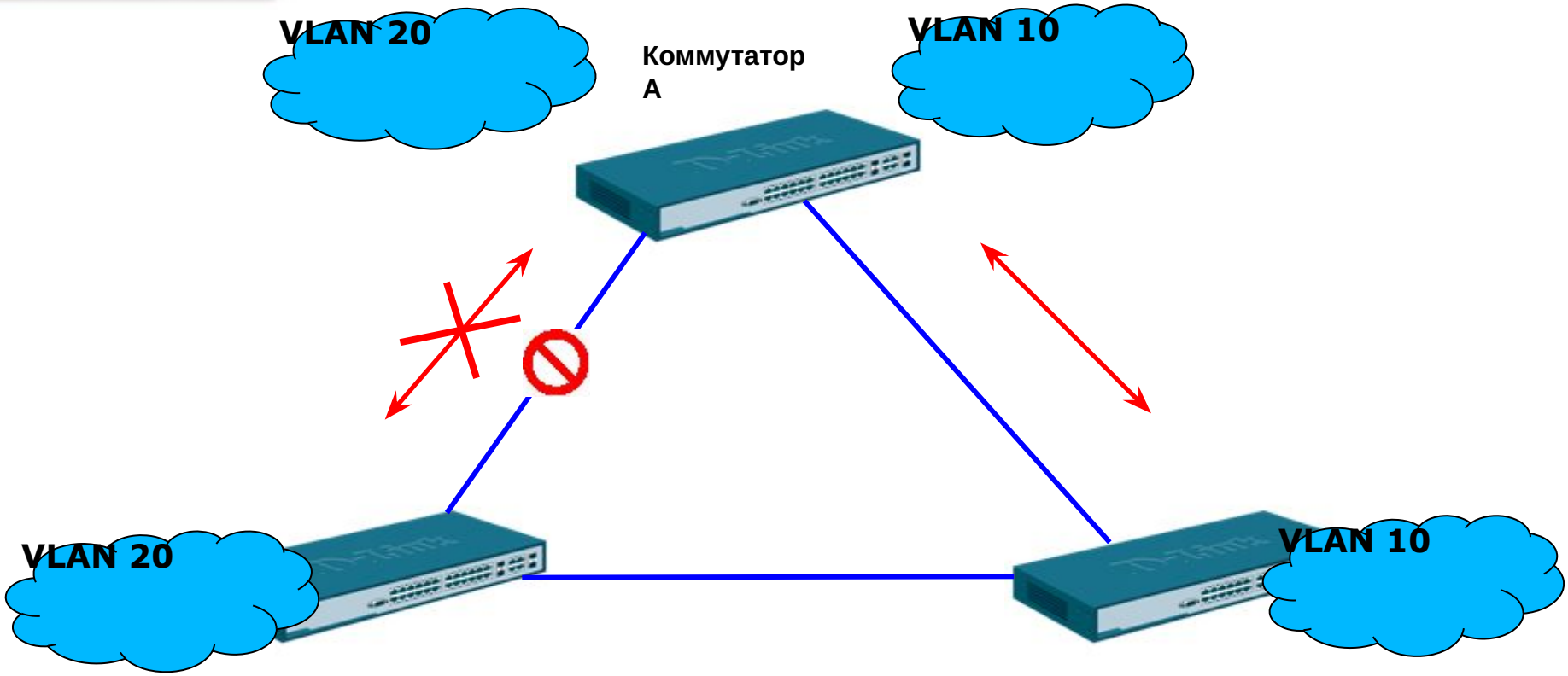
1.2 Протокол Multiple Spanning Tree Protocol

- Описывается стандартом 802.1s
- MSTP позволяет использовать более одной копии STP в сети с 802.1q VLAN. Он позволяет одни VLAN связать с одной копией STP, а другие с другой, обеспечивая несколько связей между коммутаторами.
- MSTP предоставляет возможность распределения нагрузки.
- Каждая копия (дерево) MSTP использует протокол RSTP для более быстрой сходимости сети.
- Регион MSTP это связанная группа коммутаторов с поддержкой MSTP с одинаковой конфигурацией.

Пример работы MSTP

- Сеть состоит из 3 коммутаторов, соединенных между собой.
- В сети настроены два VLAN с VID 10 и 20.
  На коммутаторе A VLAN 10 и 20 настроены на разных портах таким образом, что трафик для обоих VLAN 10 и 20 передается по разным соединениям.
- На первый взгляд, такая конфигурация достаточно обычна и хорошо подходит для балансировки нагрузки при передаче трафика двух различных VLAN. Однако в сети настроен протокол STP.
- Если коммутатор C будет выбран корневым коммутатором для STP, то соединение между коммутаторами A и B будет заблокировано.
- В этом случае трафик из VLAN 20 не сможет передаваться по сети.
- Эта проблема возникает потому, что коммутаторы рассматривают VLAN 10 и 20 как независимые сети, в то время как протокол STP рассматривает топологию сети как одну единую сеть.

Пример работы MSTP

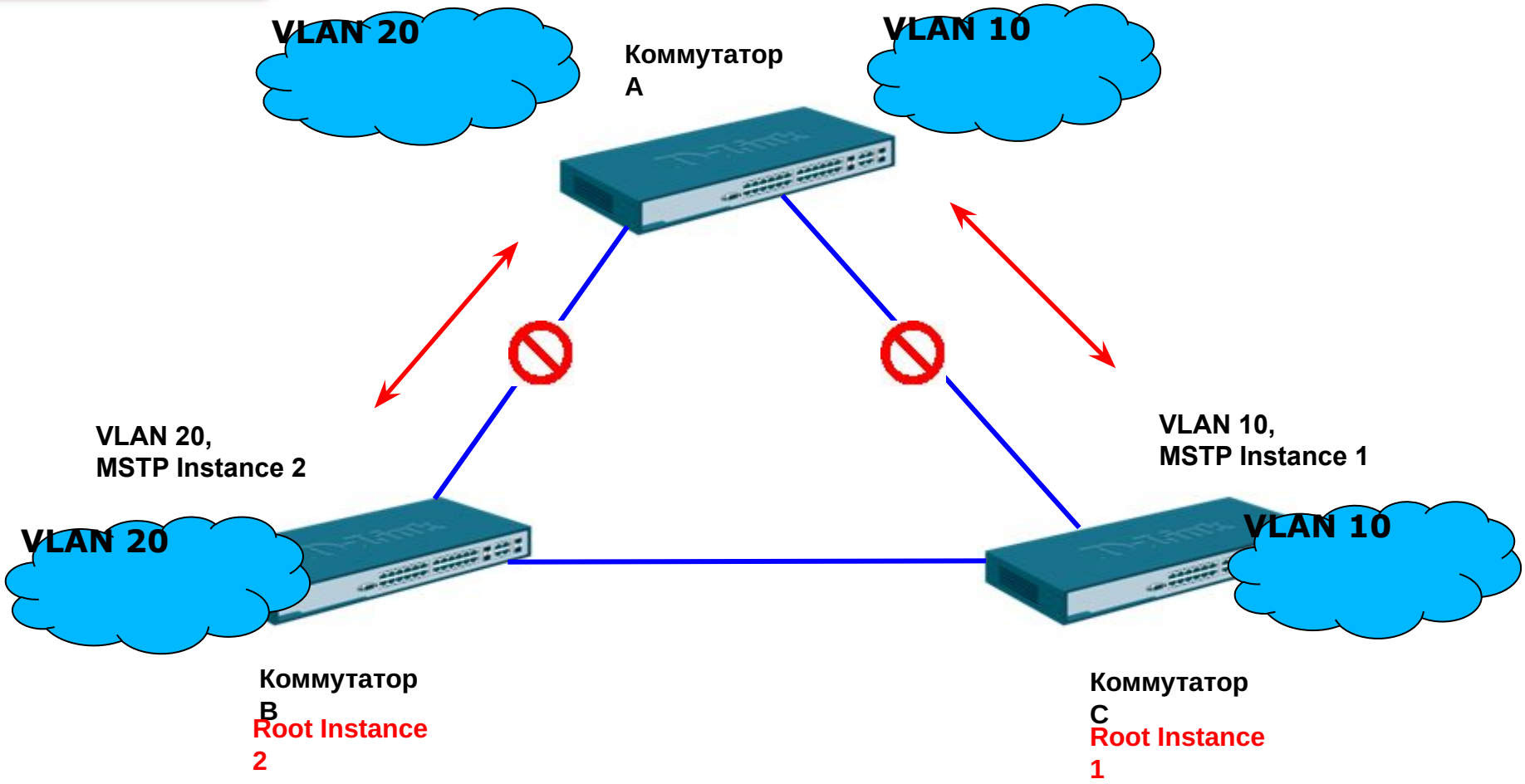


1. В результате работы STP коммутатор C выбран корневым, соединение между коммутаторами A и B было заблокировано
2. Трафик из VLAN 10 передается между коммутаторами A и C
3. Трафик из VLAN 20 блокируется и не может быть передан между коммутаторами A и B

Пример работы MSTP

- 802.1S решает поставленную задачу, если назначить VLAN 10 на копию (instance) MSTP под номером 1, а VLAN 20 сопоставить с копией 2.
- Таким образом, получится две независимых топологии дерева STP.
- Коммутатор C становится корневым для копии MSTP номер 2 и блокирует прохождение трафика между коммутаторами A и B.
- В отличие от протокола 802.1D STP, это соединение блокируется только для прохождения трафика из VLAN 10.
- Трафик из VLAN 20 будет передаваться по этому соединению.
- Аналогичным образом, копия MSTP под номером 2 выберет коммутатор B в качестве корневого и заблокирует соединение между коммутаторами A и C для трафика из VLAN 20.
- Таким образом, достигается требуемая работа сети: осуществляется баланс нагрузки при передаче трафика нескольких VLAN по разным соединениям и в то же время в сети отсутствуют логические «петли».

Пример работы MSTP



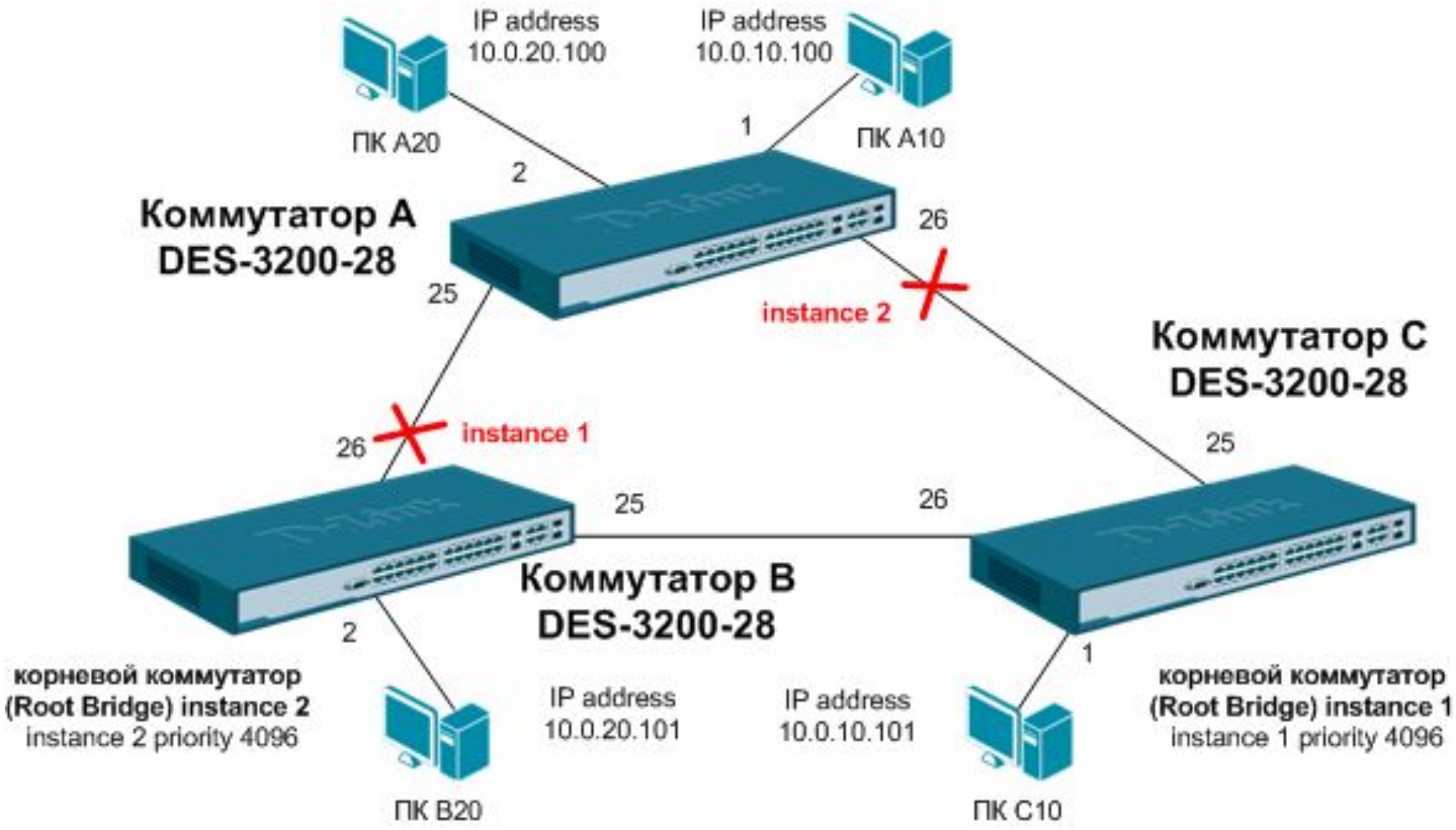
1. В копии MSTP номер 1 коммутатор C выбран корневым, соединение между коммутаторами A и B для VLAN 10 было заблокировано
2. В копии MSTP номер 2 коммутатор B выбран корневым, соединение между коммутаторами A и C для VLAN 20 было заблокировано
3. Трафик из VLAN 10 передается между коммутаторами A и C
4. Трафик из VLAN 20 передается между коммутаторами A и B

Настройка MSTP

- Внутри региона все коммутаторы должны иметь одинаковые настройки копии (instance) MSTP:
  - Конфигурационное имя MST
  - Конфигурационный номер ревизии MST (0-65535)
  - Карту привязки VLAN к экземплярам MST

1. Включить STP на каждом устройстве.
2. Изменить версию STP на MSTP (по умолчанию RSTP).
3. Задать имя региона MSTP и ревизию.
4. Создать копию (instance) и проассоциировать VLAN с ней.
5. Сконфигурировать приоритет (priority) STP так, чтобы явно задать корневой коммутатор. По умолчанию - 32768. Чем меньше номер, тем больше приоритет.
6. Задать приоритеты на портах так, чтобы задать порт в VLAN, который будет заблокирован.
7. Задать пограничный (edge) порт.

Настройка MSTP



Настройка MSTP

- Коммутатор A:

```
config vlan default delete 1,2,25,26
create vlan 10 tag 10
config vlan 10 add untag 1
config vlan 10 add tag 25-26
create vlan 20 tag 20
config vlan 20 add untag 2
config vlan 20 add tag 25-26
config stp ver mstp
create stp instance_id 1
config stp instance_id 1 add_vlan 10
create stp instance_id 2
config stp instance_id 2 add_vlan 20
config stp mst_config_id name abc
    revision_level 1
config stp ports 1-2 edge true
enable stp
```

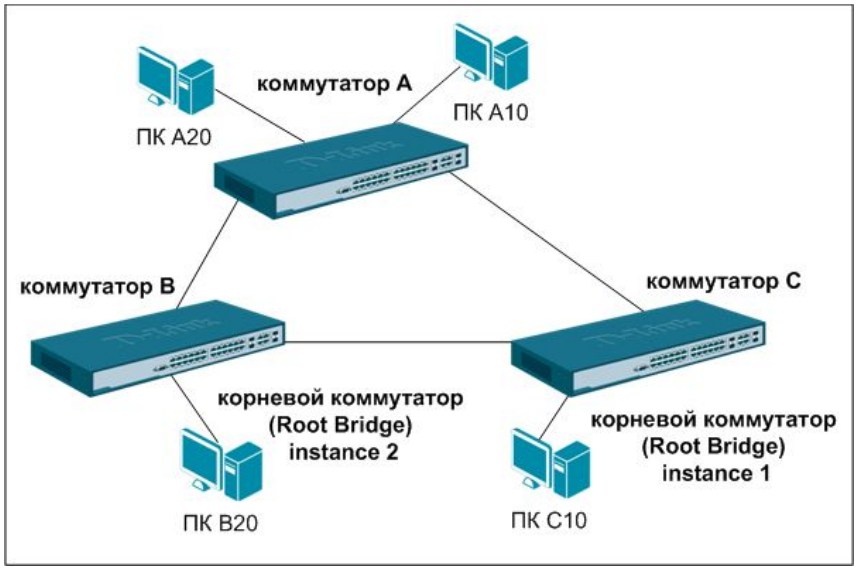
- Коммутатор B:

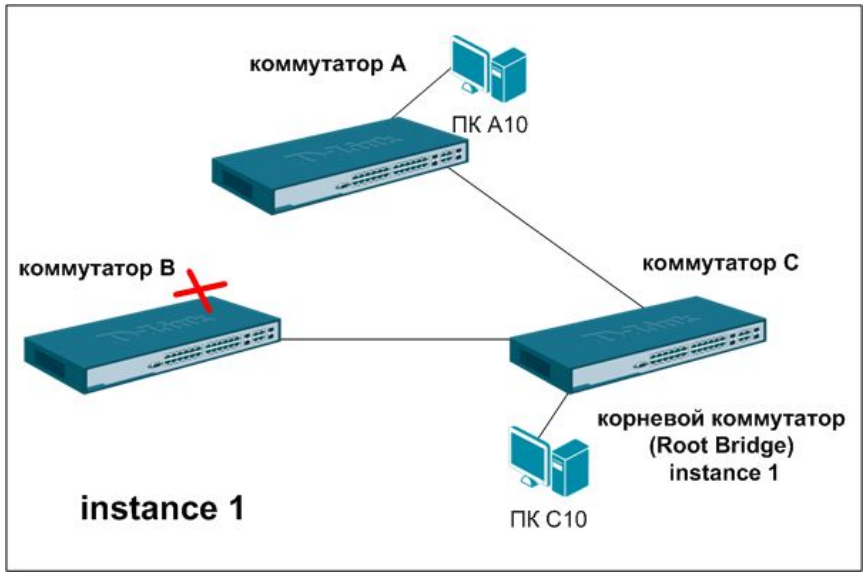
```
config vlan default delete 2,25,26
create vlan 10 tag 10
config vlan 10 add tag 25-26
create vlan 20 tag 20
config vlan 20 add untag 2
config vlan 20 add tag 25-26
config stp ver mstp
create stp instance_id 1
config stp instance_id 1 add_vlan 10
create stp instance_id 2
config stp instance_id 2 add_vlan 20
config stp mst_config_id name abc
    revision_level 1
config stp priority 4096 instance_id 2
config stp mst_ports 26 inst 2 priority 96
config stp ports 2 edge true
enable stp
```

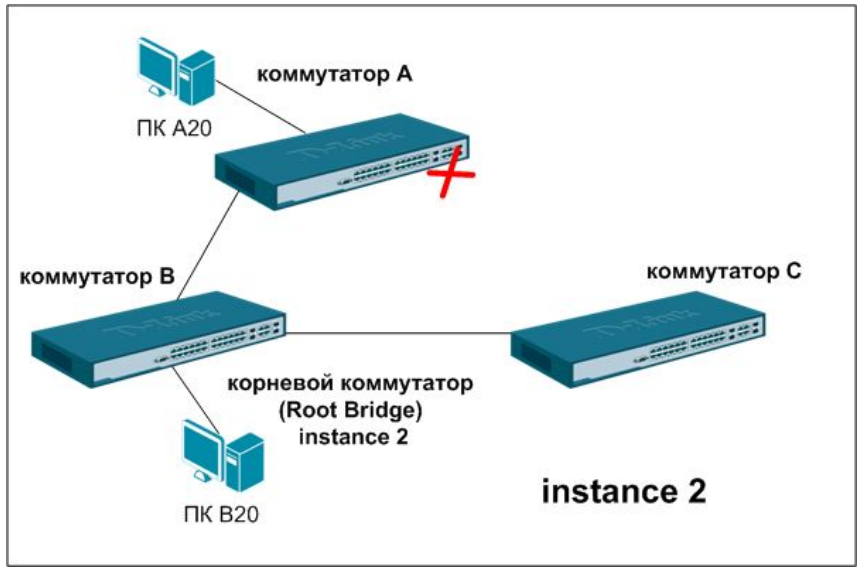
- Коммутатор C:

```
config vlan default delete 1,25,26
create vlan 10 tag 10
config vlan 10 add untag 1
config vlan 10 add tag 25-26
create vlan 20 tag 20
config vlan 20 add tag 25-26
config stp ver mstp
create stp instance_id 1
config stp instance_id 1 add_vlan 10
create stp instance_id 2
config stp instance_id 2 add_vlan 20
config stp mst_config_id name abc
    revision_level 1
config stp priority 4096 instance_id 1
config stp mst_ports 25 inst 1 priority 96
config stp ports 1 edge true
enable stp
```

Настройка MSTP







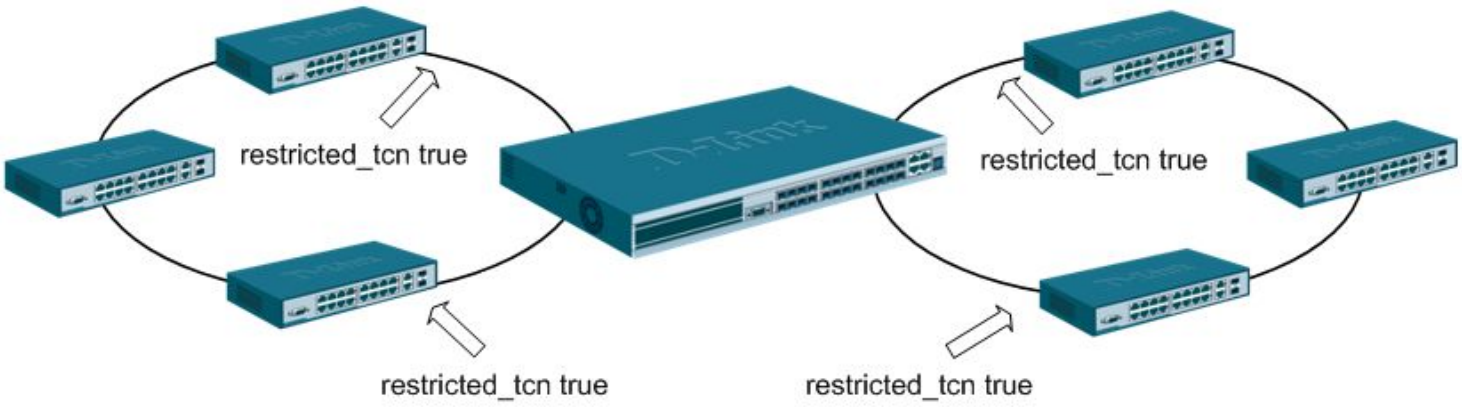
1.3 Функции безопасности STP

- Restricted role

  Запрещает порту коммутатора становиться корневым (Root port), т.е. исключает появление корневого коммутатора (Root bridge) за этим портом. По умолчанию функция выключена (значение false).

- Restricted TCN

  Запрещает на порту коммутатора прием BPDU TCN, т.о. на данном порту не будет фиксироваться изменение топологии. По умолчанию функция выключена (значение false). Рекомендуется включать на портах, смотрящих в сторону агрегатора, чтобы изменение топологии в одном кольце не сказывалось на других



Типовые настройки STP

- Коммутатор A:

config vlan default delete 21-24
create vlan v10 tag 10
config vlan v10 add tagged 21-24
config stp version rstp
config stp priority 4096
config stp ports 21-24 state enable
config stp ports 21-24 restricted_role true
enable stp

- Коммутатор B1,B3,C1,C3:

config vlan default delete 1-18
create vlan v10 tag 10
config vlan v10 add tagged 17-18
config vlan v10 add untagged 1-16
config stp version rstp
config stp ports 17-18 state enable
enable stp
config stp ports 17 restricted_tcn true
config loopdetect ports 1-16 state enabled
enable loopdetect

- Коммутатор B2,C2:

config vlan default delete 1-18
create vlan v10 tag 10
config vlan v10 add tagged 17-18
config vlan v10 add untagged 1-16
config stp version rstp
config stp ports 17-18 state enable
enable stp
config loopdetect ports 1-16 state enabled
enable loopdetect

1.4 Loopback Detection Independent STP

- Функция Loopback detection предназначена для определения возникновения петли в сети и блокирования порта, на котором эта петля обнаружена.
- Loopback Detection Independed STP использует специальные multicast пакеты для обнаружения петель
- Обнаруживает как петлю между портами, так и петлю за одним портом.
- Работа в двух режимах:
  - Port-Based – блокирует весь порт
  - Vlan-Based – блокирует трафик того vlan, в котором обнаружена петля
- Порт может быть разблокирован по прошествии определенного периода времени - recover_timer
- С версии LoopDetect 4.03 рекомендуется включаеть функцию на клиентских портах в режиме PortBased и отключать STP

Настройка Loopback Detection

- Коммутатор DES-3200-28:

enable loopdetect
config loopdetect ports 1-28 state enable
config loopdetect mode port-based
config loopdetect recover_timer 300
config loopdetect interval 5

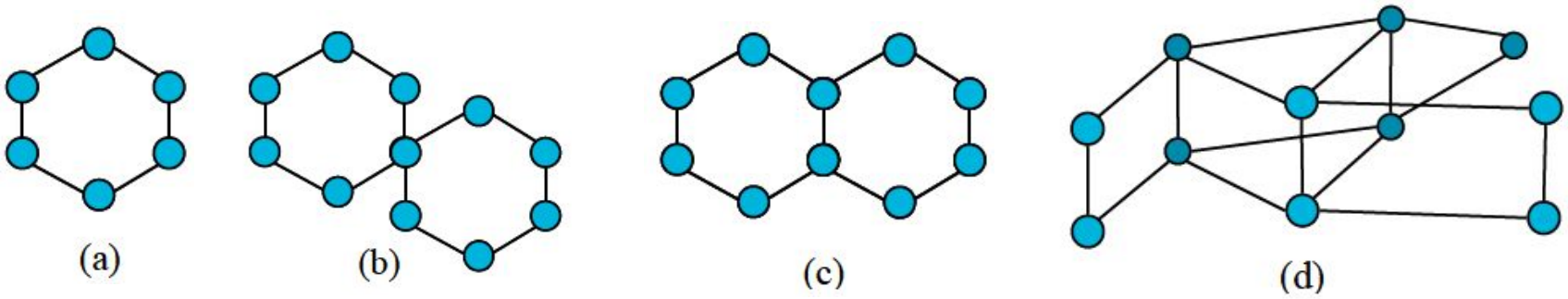
- При обнаружении петли (м-ду 1 и 2 портом):

DES-3200-28:5#show loopdetect ports 1-4
Command: show loopdetect ports 1-4

Port	Loopdetect State	Loop Status
1	Enabled	Loop
2	Enabled	Loop
3	Enabled	Normal
4	Enabled	Normal

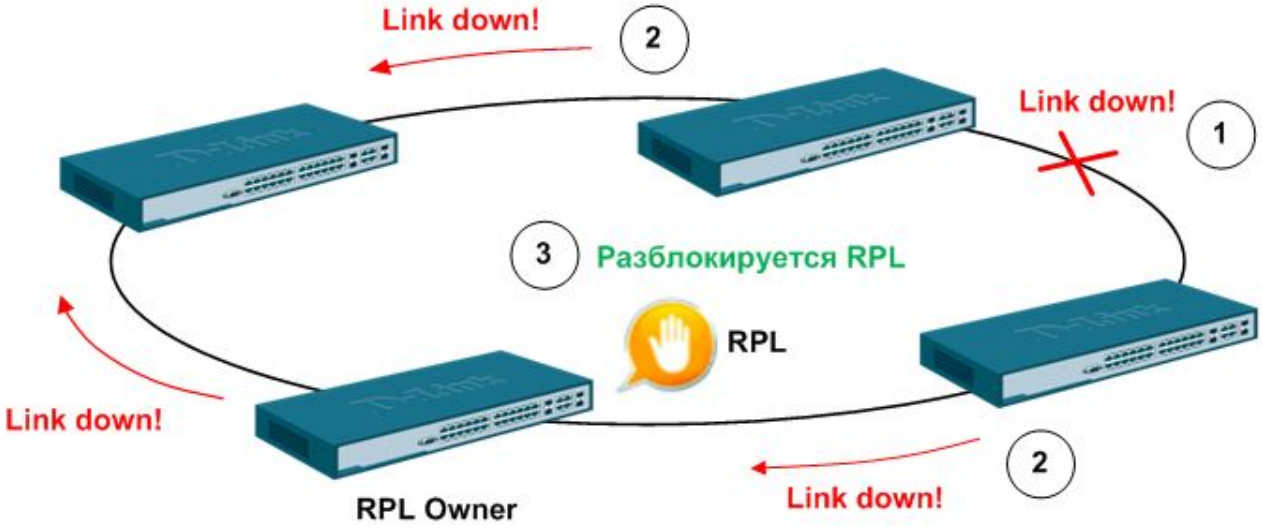
1.5 Протокол ERPS

- ERPS (Ethernet Ring Protection Switching) – протокол для обеспечения отказоустойчивости топологии «кольцо» в среде Ethernet
- Обеспечивает чрезвычайно малое (50-200 мс) время восстановления связи при отказе одной из линий в кольце
- Обеспечивает защиту от формирования петель и возникновения broadcast шторма
- Поддерживает сложные кольцевые топологии



1.5 Протокол ERPS

- Сценарий использования – кольцевая топология
- Один из портов блокируется для предотвращения петли – RPL (Ring Protection Link)
- При обрыве связи в кольце разорванный канал блокируется, и разблокируется RPL
- После восстановления связи RPL вновь блокируется.



1.5 Протокол ERPS

- **RPL (Ring Protection Link)** – соединение, определенное механизмом как заблокированное при нормальном функционировании кольца
- **RPL Owner** – узел, подключенный к RPL и блокирующий его в нормальном состоянии и разблокирующий при возникновении неисправности
- **R-APS (Ring – Automatic Protection Switching) Messages** – протокол сообщений, описанный в рекомендации G.8032:
  - **Signal Fail (SF)** - сообщение о разрыве соединения
  - **No Request (NR)** – объявляется при нормальном функционировании (нет сообщений SF и пр.)
  - **RPL Blocked (RB)** – сообщение, отправляемое узлом RPL Owner при блокировании RPL, всегда идет в паре с NR.
- **RAPS VLAN** – отдельный VLAN для передачи R-APS сообщений

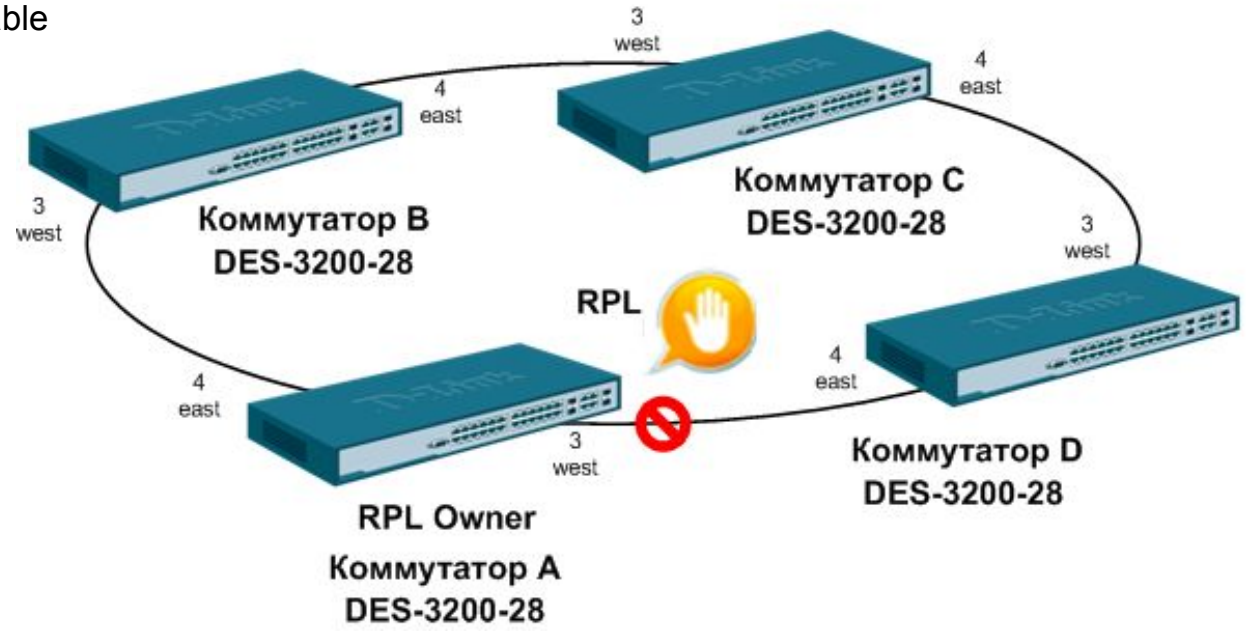
Настройка ERPS

- Коммутатор A:

create vlan vlanid 3
config vlan vlanid 3 add tagged 3-4
create vlan vlanid 5
config vlan vlanid 5 add tagged 5-6
create erps raps_vlan 3
config erps raps_vlan 3 ring_port west 3
config erps raps_vlan 3 ring_port east 4
config erps raps_vlan 3 protected_vlan add vlanid 5
config erps raps_vlan 3 protected_vlan add vlanid 1
config erps raps_vlan 3 rpl_port west
config erps raps_vlan 3 rpl_owner enable
enable erps

- Коммутатор B, C, D:

create vlan vlanid 3
config vlan vlanid 3 add tagged 3-4
create vlan vlanid 5
config vlan vlanid 5 add tagged 5-6
create erps raps_vlan 3
config erps raps_vlan 3 ring_port west 3
config erps raps_vlan 3 ring_port east 4
config erps raps_vlan 3 protected_vlan add vlanid 5
config erps raps_vlan 3 protected_vlan add vlanid 1
enable erps



1.6 Агрегирование каналов LACP

- Агрегирование каналов LACP (IEEE 802.3ad) используется для объединения нескольких портов вместе для организации одного канала с высокой пропускной способностью. Такие порты называются членами группы агрегирования (**member ports**), а один из портов назначается мастером группы (**master port)**.

- Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера группы распространяется на все порты в группе. Таким образом, при конфигурировании портов в группе агрегирования достаточно настроить мастер-порт.

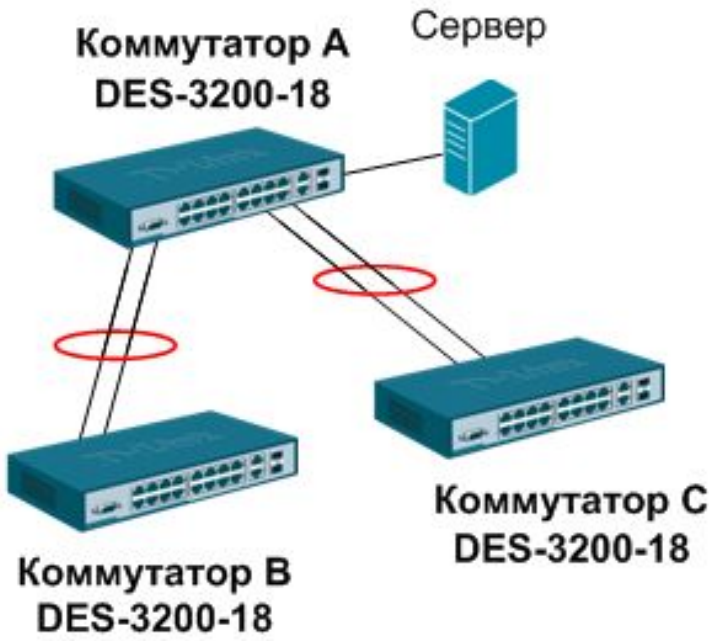
- Серия коммутаторов DES-3200 поддерживает до 15 групп агрегирования, каждая из которых может содержать от 2-ух до 8-ми портов.

1.6 Агрегирование каналов LACP

- Алгоритм LACP применяется на каждом устройстве для определения того, какой порт в группе используется для передачи определённых пакетов. Существует 6 алгоритмов (по умолчанию mac-source):
  - mac_source (по MAC-адресу источника)
  - mac_destination (по MAC-адресу назначения)
  - mac_source_dest (по MAC-адресам источника и назначения)
  - ip_source (по IP-адресу источника)
  - ip_destination (по IP-адресу назначения)
  - ip_source_dest (по IP-адресу источника и назначения)

Настройка LACP

- Замечание: порты коммутаторов должны иметь одинаковые настройки до включения в агрегированный канал
- Порты с одной стороны должны быть в состоянии active, с другой – passive (по умолчанию)



- Коммутатор A:

```
create link_aggregation group_id 1 type lacp
config link_aggregation group_id 1 master_port 1 ports 1-2
    state enable
config lacp_ports 1-2 mode active
create link_aggregation group_id 2 type lacp
config link_aggregation group_id 2 master_port 3 ports 3-4
    state enable
config lacp_ports 3-4 mode active
config link_aggregation algorithm mac_source
```

- Коммутатор B и C:

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source
config link_aggregation group_id 1 master_port 1 ports 1-2 state enable
```

1.7 Функция Storm Control

- В случае сбоя какого-либо устройства или возникновения атаки на сеть может резко увеличиться количество того или иного вида трафика в сети. Это может отрицательно сказаться на производительности и качестве предоставляемых сервисов.
- Шторм возникает при большом количестве входящих широковещательных, многоадресных или одноадресных пакетов на одном порту.
- Storm Control служит для ограничения количества пакетов определенного типа на порту, или выключения порта в случае возникновения шторма – при превышении заданного порогового значения (threshold)
- Порог (threshold) – количество широковещательных/многоадресных /одноадресных пакетов в секунду.
- Временной интервал (time_interval) – промежуток времени, через который данные по количеству пакетов на порту передаются с CPU на механизм Traffic Control

1.7 Функция Storm Control

- Возможные действия:
  - **Отбрасывание** (**Drop**) – задействует аппаратный механизм Traffic Control и отбрасывает пакеты, выходящие за рамки указанного порогового значения
  - **Отключение** (**Shutdown**) – будет отбрасываться весь трафик на порту за исключением STP BPDU пакетов, чтобы не нарушать работу механизмов Spanning Tree. Если Счетчик (Count down) отработал свое значение, а шторм продолжается, порт будет помещен в состояние Forever Shutdown и может быть выведен из него только вручную администратором.

Traffic Storm Control			
	Широковещательные (Broadcast)	**Многоадресные (Multicast)**	**Одноадресные (Unicast)**
Действие	**•Отбрасывание (Drop) •Откл. (Shutdown)**	**•Отбрасывание (Drop) •Откл. (Shutdown)**	**Отбрасывание (Drop)**
Порог (Threshold)	**Устанавливается в значение 0-255000 пакетов/сек**		
Счетчик (Count Down)	**Возможно установить 0, 5 или 30мин (Значение по умолчанию 0 означает, что порт никогда не будет отключен)**		
Интервал (Time Interval)	**Устанавливается в значение 0-30 сек (Значение по умолчанию – 5)**		

Настройка Storm Control

- Коммутатор DES-3200-28:

config traffic control 1-5 broadcast enable multicast enable
config traffic control 1-5 action drop
config traffic control 1-5 threshold 64 countdown 10 time_interval 10
config traffic trap both

- Проверка настройки:

DES-3200-28:5#show traffic control 1-5
Command: show traffic control 1-5
Traffic Storm Control Trap :[None]

Port	Thres hold	Broadcast Storm	Multicast Storm	Unicast Storm	Action	Count down	Time Interval
----	----	----	----	----	----	----	----
1	64	Enabled	Enabled	Disabled	drop	0	5
2	64	Enabled	Enabled	Disabled	drop	0	5
3	64	Enabled	Enabled	Disabled	drop	0	5
4	64	Enabled	Enabled	Disabled	drop	0	5
5	64	Enabled	Enabled	Disabled	drop	0	5

Total Entries : 5

Спасибо!