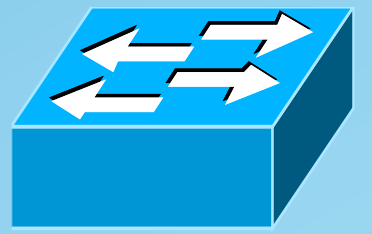
Лекция 6

# Сети на коммутаторах

# Сетевой коммутатор

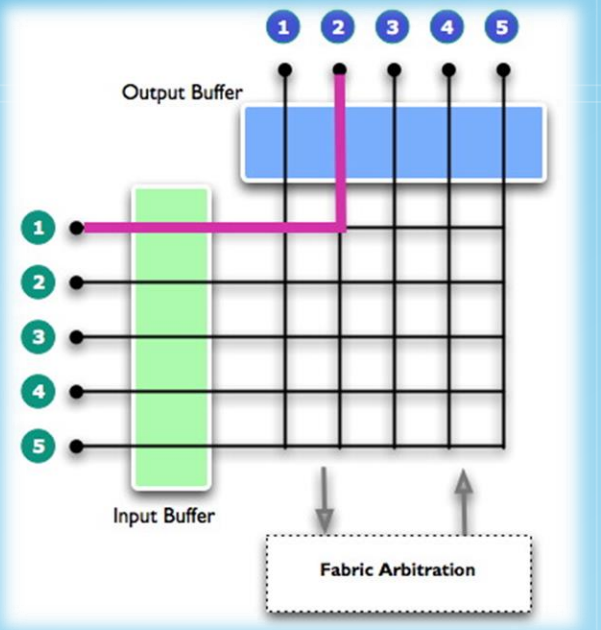
- **Сетевой коммутатор (network switch)** – сетевое устройство, предназначенное для объединения абонентских устройств в локальную сеть, а также её сегментации

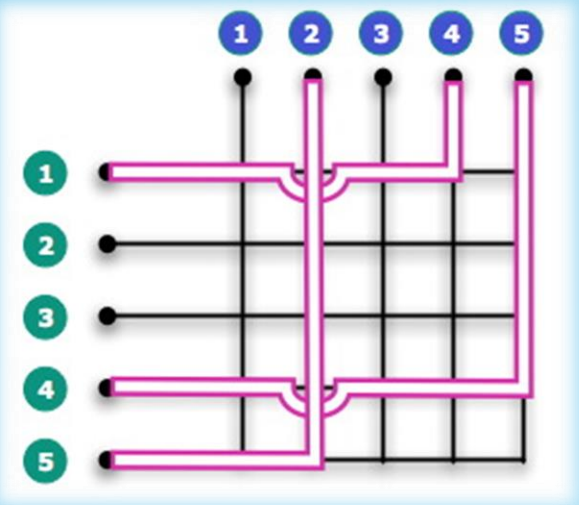



- передает данные только непосредственному получателю (таблица MAC-адресов)
- позволяет использовать полнодуплексный режим работы протоколов LAN

# Устройство коммутатора

- Основа любого современного коммутатора – **ASIC** (application specific integrated circuits), специализированные микросхемы, способные *очень быстро* делать ограниченное число операций по перекладыванию пакета из одного буфера в другой в соответствии с заданным алгоритмом

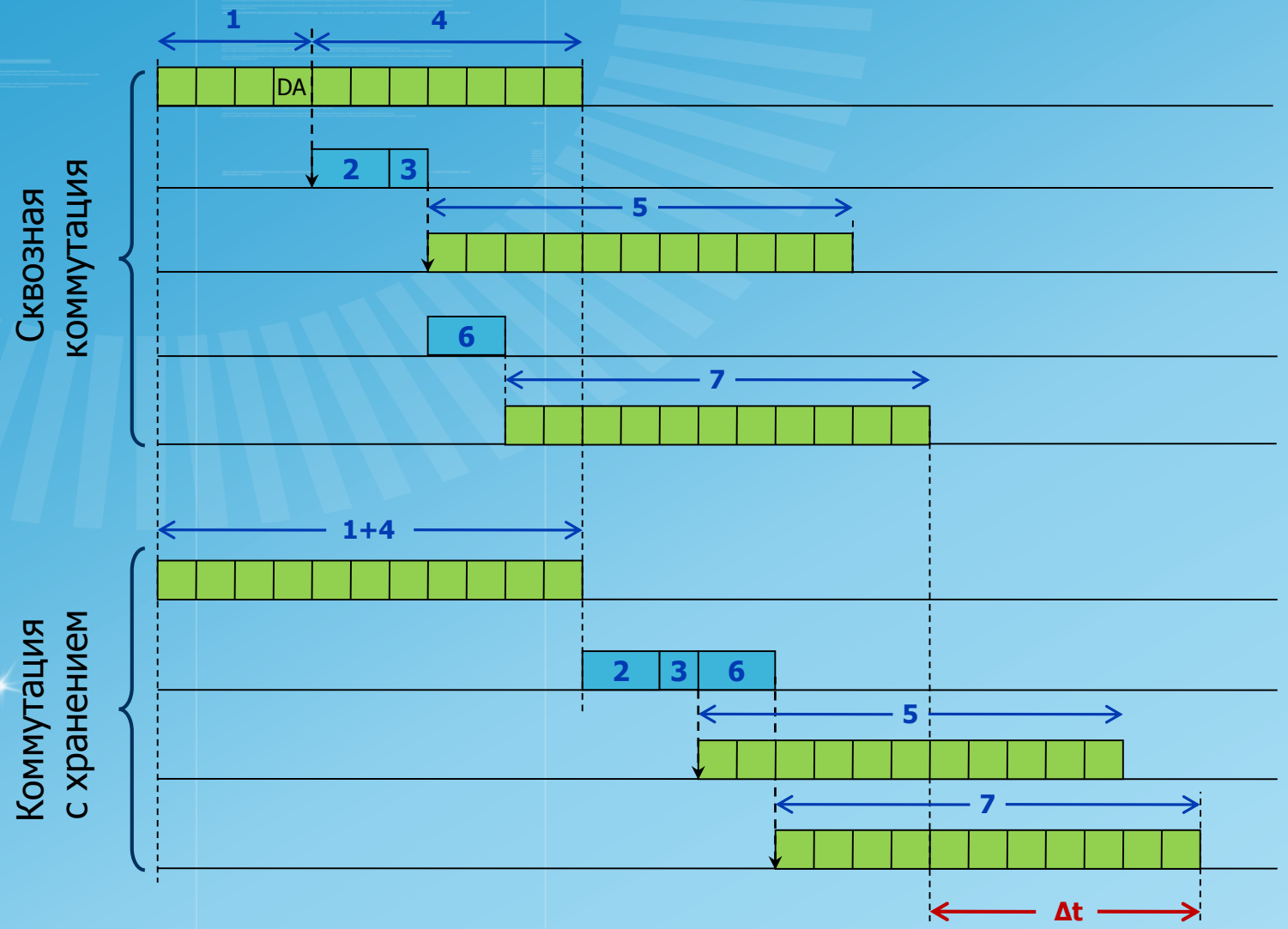


# Режимы коммутации

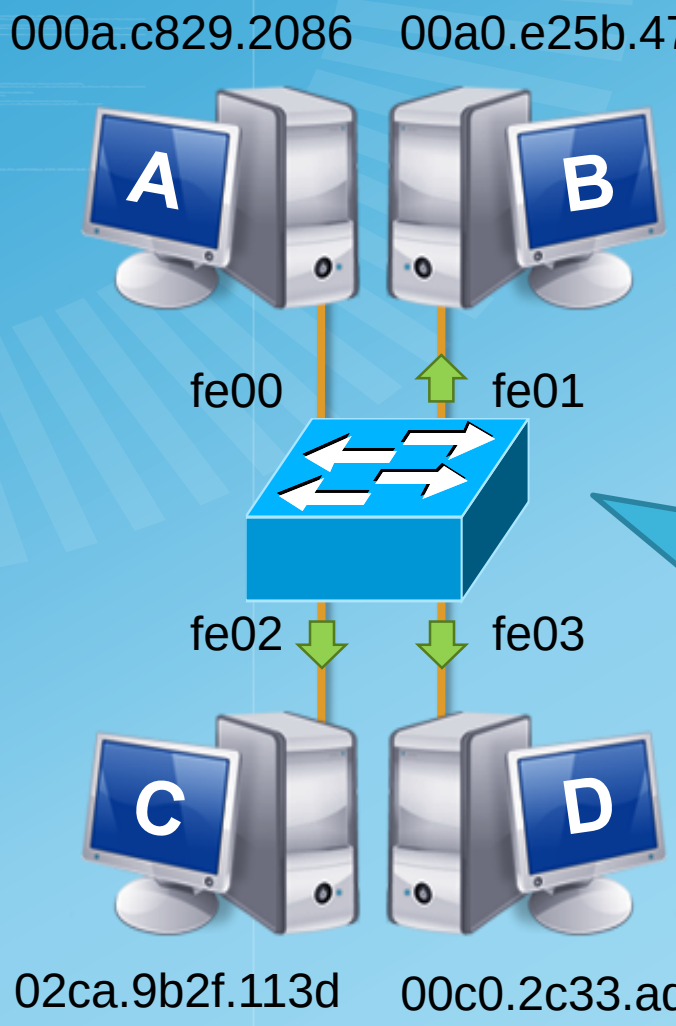
- с промежуточным хранением (store and forward):
  - приём и проверка кадра на отсутствие ошибок
  - коммутация и пересылка кадра
- сквозной (cut-through)
  - считывание  адреса назначения
  - коммутация и пересылка
- бесфрагментный (fragment-free)
  - кадры размером 64 байта – store-and-forward
  - остальные – cut-through
- адаптивная коммутация
  - автовыбор из первых трёх режимов

# Этапы работы коммутатора (2)




1. Приём первых бит кадра процессором входного порта (до адреса назначения включительно)
2. Поиск адреса назначения по адресной таблице
3. Коммутация портов
4. Приём остальных бит кадра процессором входного порта
5. Приём бит кадра процессором выходного порта через фабрику коммутации
6. Получение доступа к среде процессором выходного порта
7. Передача бит кадра процессором выходного порта в сеть

# Таблица MAC-адресов (1)



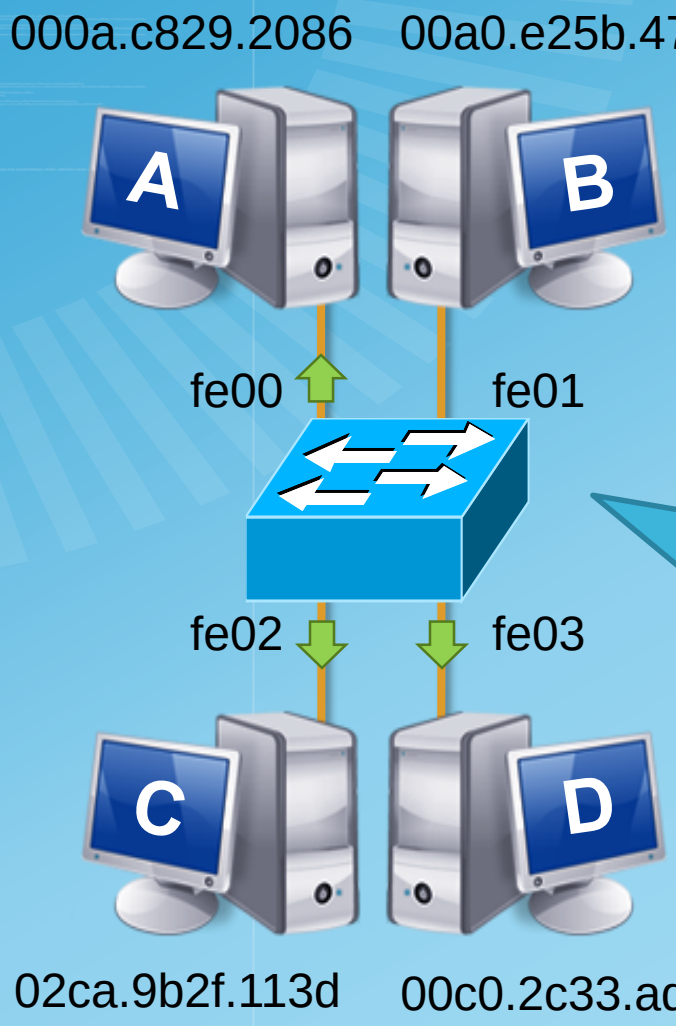

1 шаг: A → C

Таблица адресов пуста.
Коммутатор:

- разослать всем
- дополнить таблицу

| MAC-address | Port |
|---|---|
| 000a.c829.2086 | fe00 |
| | |
| | |
| | |

# Таблица MAC-адресов (2)



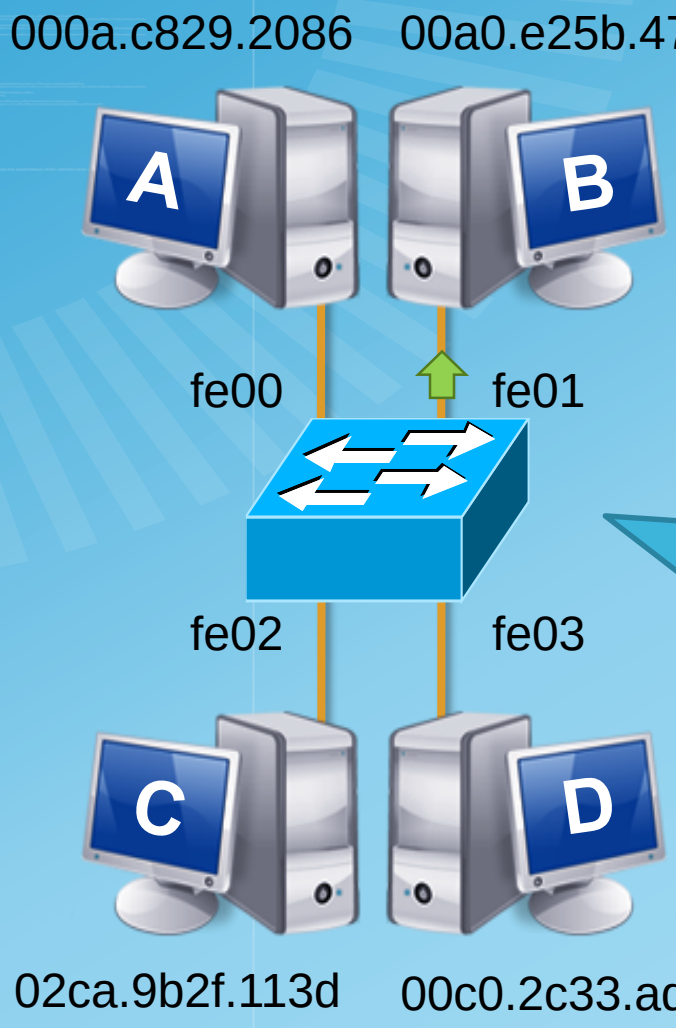

2 шаг: B  C

Соответствие не найдено.
Коммутатор:

- разослать всем
- дополнить таблицу

| MAC-address | Port |
|---|---|
| 000a.c829.2086 | fe00 |
| 00a0.e25b.47fd | fe01 |
| | |
| | |

# Таблица MAC-адресов (n)




n шаг: A  B

Таблица заполнена.
Коммутатор:

- отправить на порт адресата

| MAC-address | Port |
|---|---|
| 000a.c829.2086 | fe00 |
| 00a0.e25b.47fd | fe01 |
| 02ca.9b2f.113d | fe02 |
| 00c0.2c33.ad24 | fe03 |

# Таблица MAC-адресов – Cisco IOS

- Хранится в энергозависимой памяти (обнуляется при перезагрузке)
- Ёмкость таблицы ограничена (уязвимость!)
- Записи в таблице:
  - статические (добавляются через конфигурационный файл)
  - динамические (добавляются при обработке кадров)

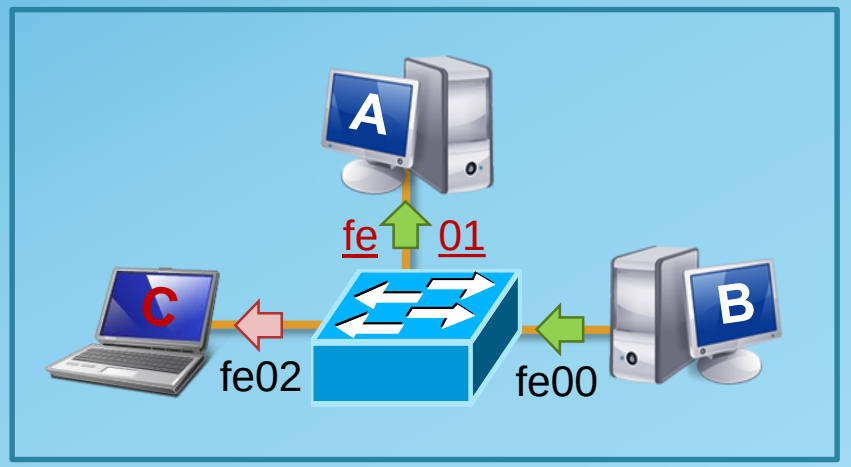

- `switch#show mac-address table`
  - выводит текущую таблицу MAC-адресов коммутатора
- `switch#show mac-address table count`
  - выводит статистику о ёмкости и заполненности таблицы MAC-адресов
- `switch#clear mac-address table`
  - очищает таблицу MAC-адресов
- `switch(config)#mac-address table static aaaa.bbbb.cccc vlan 152 interface fa0/1`
  - добавляет статическую запись в таблицу MAC-адресов

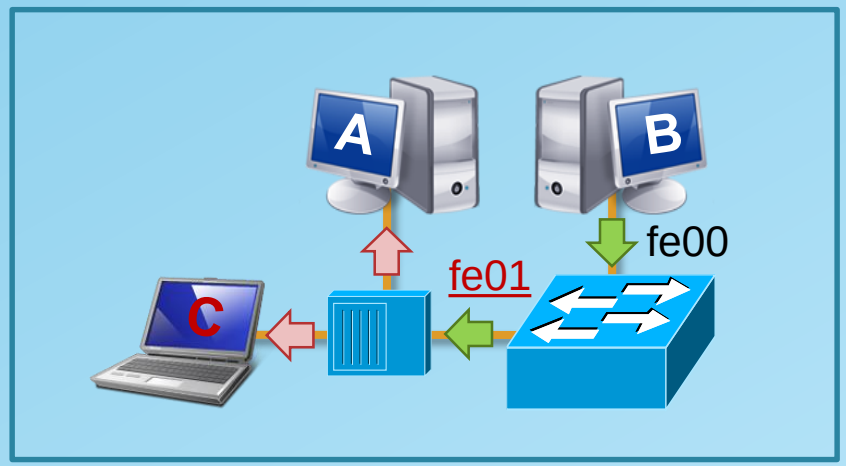
# Возможности коммутаторов

<table>
<tr><th></th><th colspan="4">Функции / Тип коммутатора</th></tr>
<tr><td rowspan="6">Гибридные</td><td rowspan="5">Управляемые</td><td rowspan="3">«умные» – smart (lightly managed)</td><td rowspan="2">неуправляемые (workgroup / unmanaged)</td><td>базовые функции коммутатора (таблица MAC-адресов, дуплексный режим, STP, PoE)</td></tr>
<tr><td colspan="2">виртуальные сети (VLAN)</td></tr>
<tr><td colspan="2">web-интерфейс управления</td></tr>
<tr><td colspan="3">CLI (интерфейс командной строки)</td></tr>
<tr><td colspan="3">advanced STP, link aggregation</td></tr>
<tr><td colspan="3">безопасность (фильтрация адресов, 802.1x)</td></tr>
<tr><td colspan="3">модульная конструкция, объединение в стек</td></tr>
<tr><td colspan="4">Технологии третьего уровня (маршрутизация, ACL, DHCP и т.п.)</td></tr>
</table>

# Мониторинг трафика

- Зеркалирование портов (только управляемые коммутаторы) – дублирование всех кадров с данного порта на порт мониторинга (зеркальный порт)
- Протокол SMON (switch monitoring) – RFC 2613
- Использование промежуточного концентратора (для тиражирования кадров на устройство мониторинга)



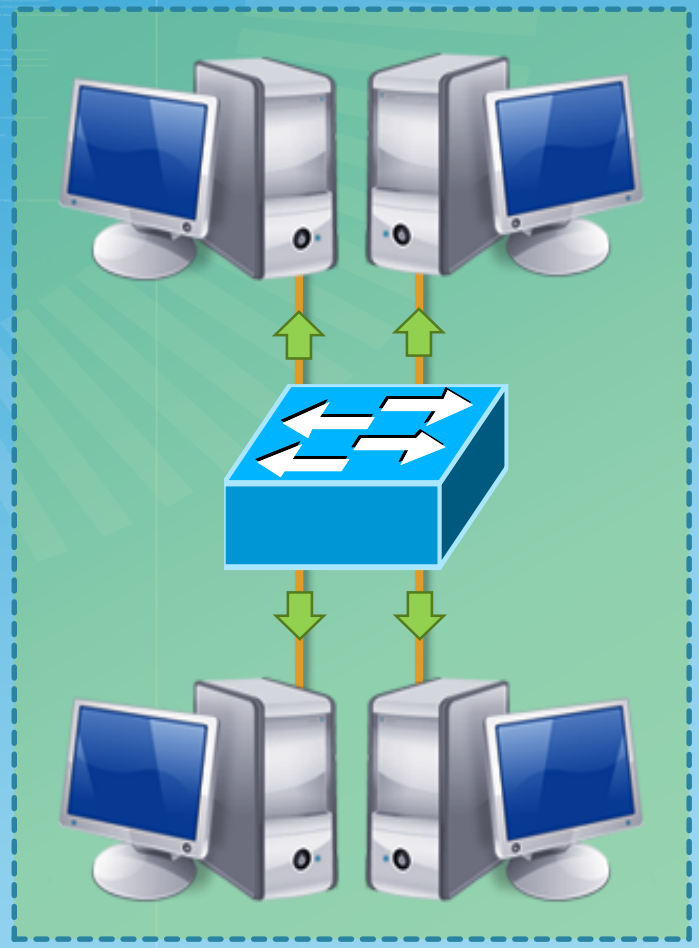



# Широковещательные кадры

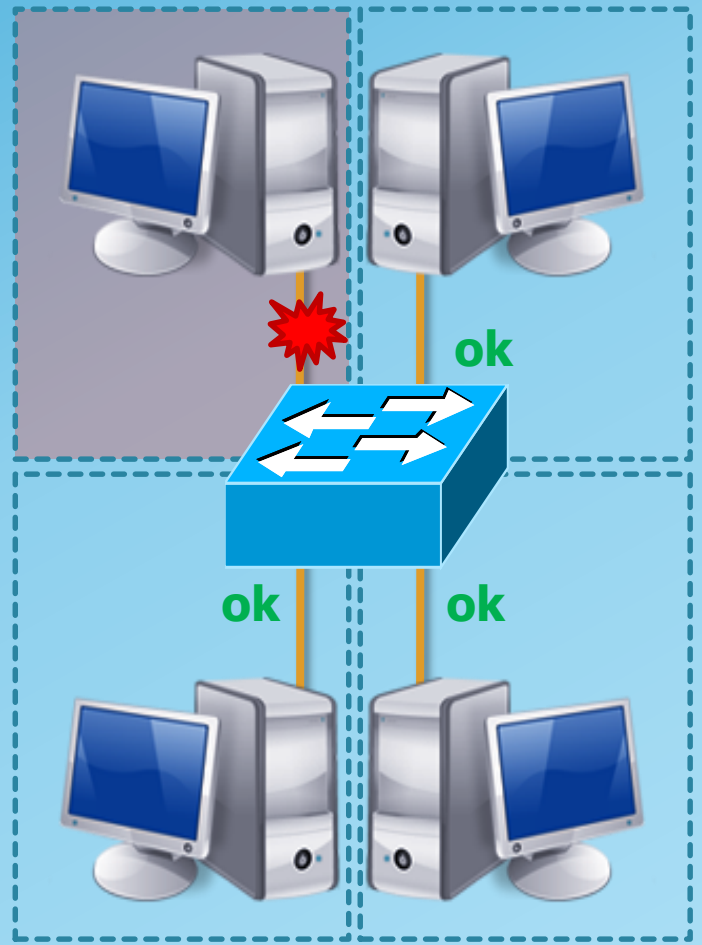
FF:FF:FF:FF:FF:FF

- **Широковещательный кадр (broadcast frame)** – кадр, адресованный всем узлам сети (MAC-адрес, состоящий из 48 единиц: ffff.ffff.ffff)
- **Домен широковещательного трафика (broadcast domain)** – совокупность узлов сети, получающих широковещательные кадры любого из указанных узлов

# Broadcast / collision domain



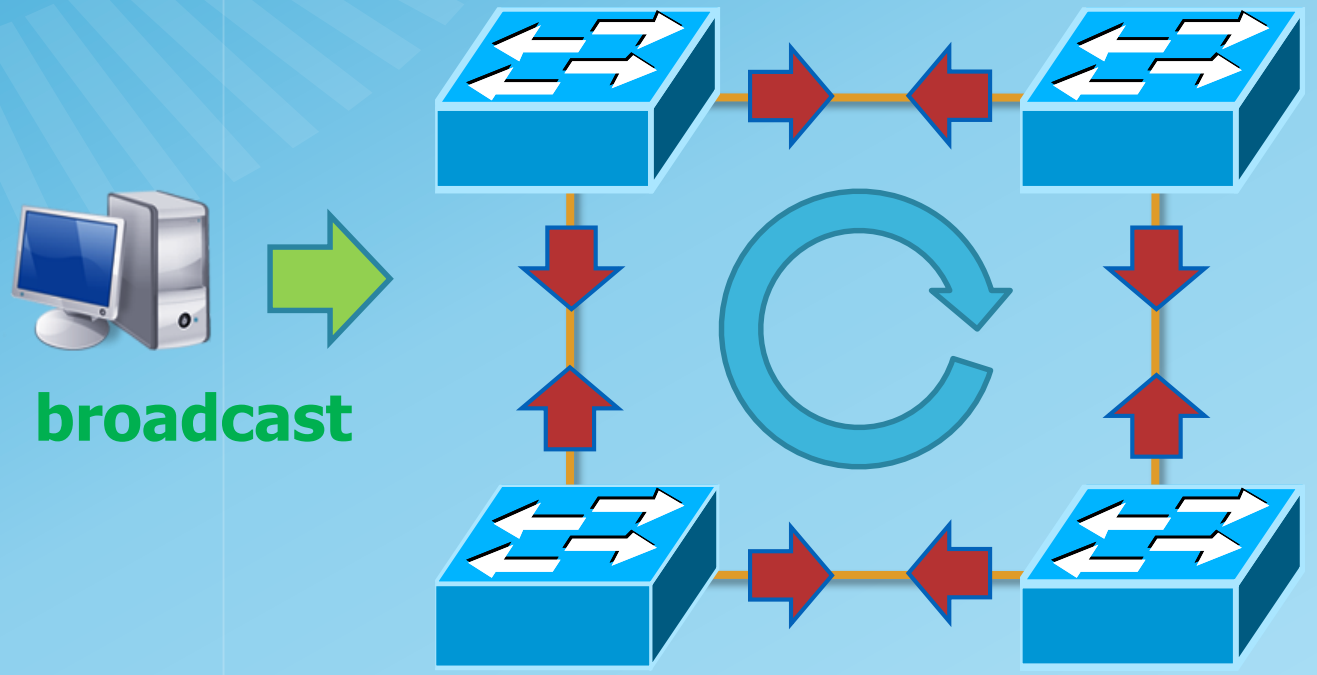
общий
broadcast-домен




раздельные домены
коллизий

# Широковещательный шторм

- **Широковещательный шторм** – зацикливание и размножение широковещательных кадров в замкнутом контуре на канальном уровне, парализующее работу сети



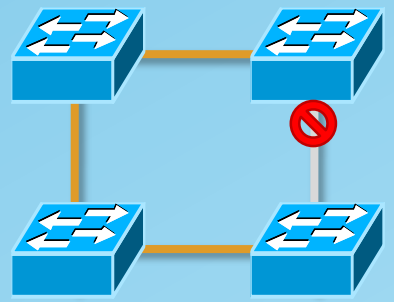
# Замкнутые контуры

## ЗАПРЕЩЕНЫ

- **Протокол STP** (spanning tree protocol) позволяет использовать замкнутые контуры для резервирования (один канал функционирует, остальные – в горячем резерве)
- **Агрегирование каналов** позволяет использовать замкнутые контуры для повышения надёжности и балансировки нагрузки (параллельная передача по всем каналам как по одному логическому)

# Протокол Spanning Tree (STP)

- **Назначение**: автоматический перевод в резервное состояние  всех альтернативных связей, не вписывающихся в топологию дерева
- Решает проблему альтернативных связей в сетях на основе мостов и коммутаторов
- **Принцип работы**:
  - Формализует сеть в виде графа
  - Обеспечивает поиск древовидной топологии связей естественным путём от каждого сегмента сети до «корня дерева»



Radia Perlman, 1983

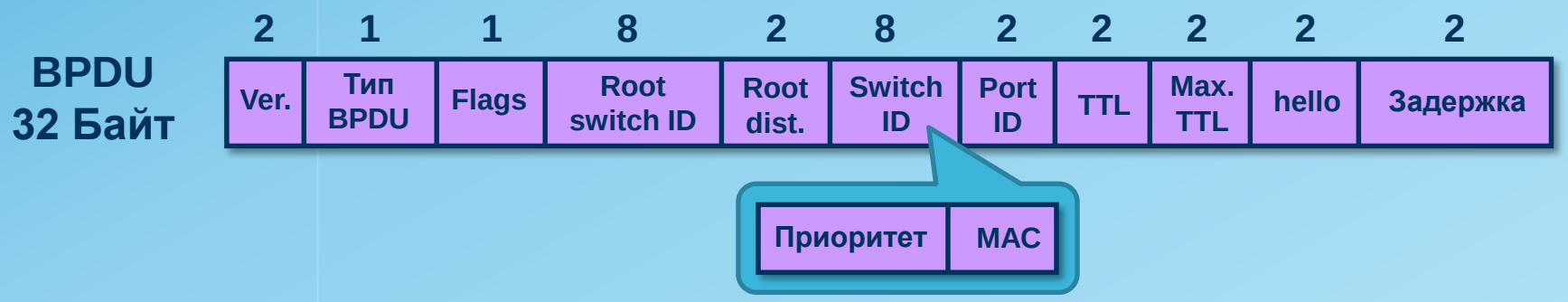
**Канальный**

# STP – принцип работы

- **1 этап. Выбор корневого коммутатора**
  - вручную администратором или автоматически (по минимальности MAC-адреса блока управления) – по пакетам BPDU (bridge protocol data unit)
- **2 этап. Выбор корневых портов** (на каждом коммутаторе)
  - на каждом коммутаторе (по ретранслируемым пакетам BPDU) выбирается порт, имеющий минимальное «расстояние» (STP Cost) до корневого коммутатора
- **3 этап. Выбор назначенных (designated) портов** (в каждом сегменте сети)
  - Из всех портов всех коммутаторов сегмента выбирается порт с минимальным «расстоянием» до корневого коммутатора
- Все остальные порты (кроме корневых и назначенных) блокируются. Математически доказано, что при таком выборе активных портов в сети исключаются петли, а оставшиеся связи образуют покрывающее дерево

# STP – выбор корневого коммутатора (автоматический)

- После инициализации каждый коммутатор считает себя корневым и генерирует кадры BPDU через все свои порты
- Получив пакет BPDU со значением идентификатора корневого коммутатора выше его собственного, коммутатор перестаёт генерировать собственные кадры BPDU и начинает ретранслировать кадры претендента на звание корневого

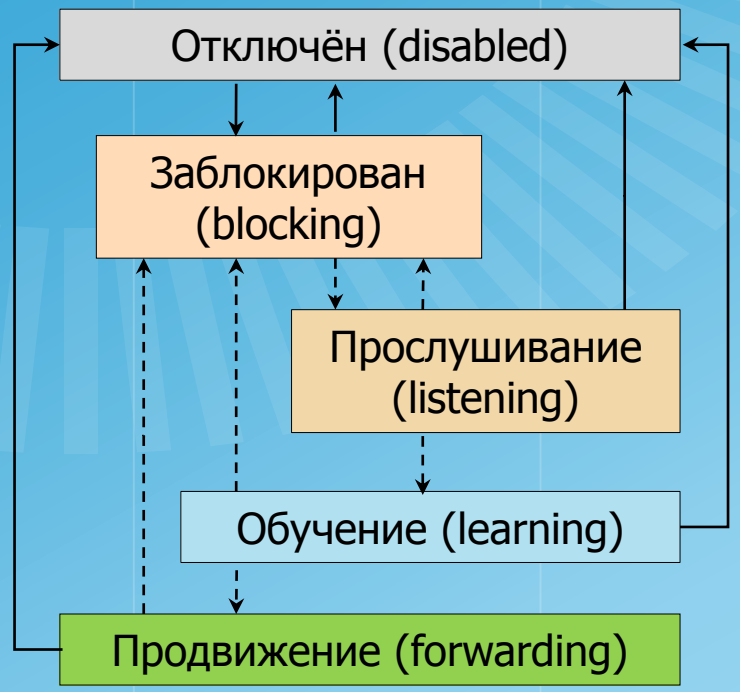


# STP – выбор корневых и назначенных портов

- При ретрансляции пакетов BPDU коммутаторы увеличивают «расстояние» до корня (STP Cost) на условное время, соответствующее сегменту, из которого пришёл пакет.
- Ретранслируя пакеты, коммутатор для каждого своего порта запоминает минимальное встретившееся «расстояние» до корня; так выбирается корневой порт.
- Для всех остальных портов выполняется сравнение принятых по ним минимальных «расстояний» до корня (до наращивания). Если все принятые на порт «расстояния» больше «расстояния» от собственного корневого порта, то этот порт – назначенный для данного сегмента.

| Битовая скорость | STP Cost |
|---|---|
| 10 Mbps | 100 |
| 100 Mbps | 19 |
| 1 Gbps | 4 |
| 10 Gbps | 2 |

# STP – состояние портов

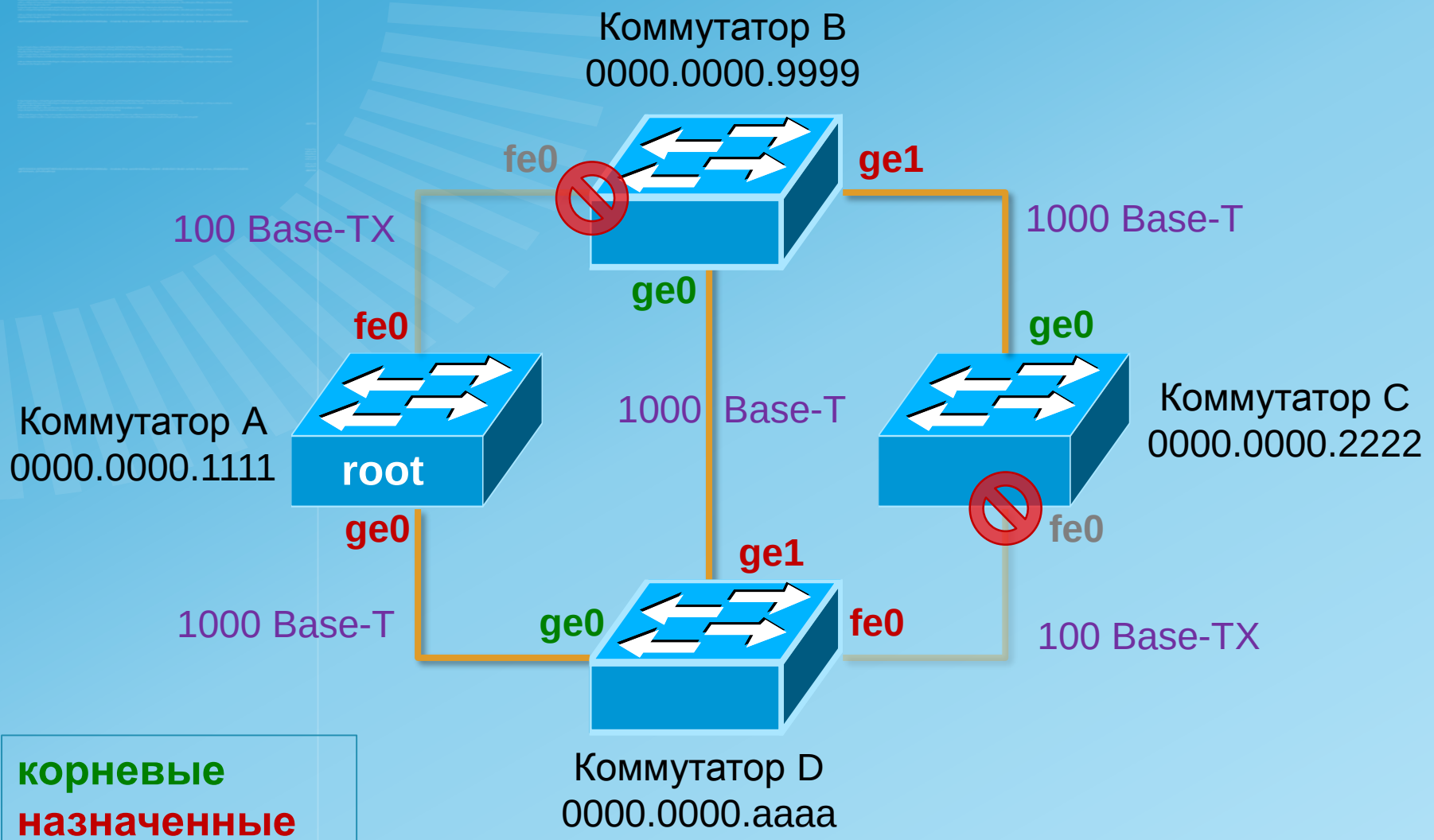



- Отключён (shutdown или err-disabled)
  - Команда конфигурирования shutdown (администратор)
  - Аварийный переход при обнаружении цикла на интерфейсе, находящемся в состоянии «продвижение»
- Заблокирован (blocking)
  - Состояние инициализации и резервное
  - Порт генерирует и ретранслирует BPDU, но не принимает и не отправляет кадры данных
- Прослушивание (listening)
  - Состояние портов, претендующих на роль корневых/назначенных. Возможен переход в «заблокирован» (при появлении лучшего претендента) и «обучение» (по таймеру)
- Обучение (learning)
  - Заполнение таблицы MAC-адресов (переход по таймеру в режим «продвижение»), приём и продвижение BPDU
- Продвижение (forwarding)
  - Приём и продвижение пакетов данных
  - Обработка BPDU и продвижение с корневых на назначенные порты; готовность стать корневым портом

# STP - версии

| Версия протокола | Стандарт | Ресурсоемкость | Сходимость | Количество деревьев |
|---|---|---|---|---|
| STP | 802.1D | Низкая | Медленная | Одно |
| **PVST+** | **Cisco** | **Высокая** | **Медленная** | **По одному на каждый VLAN** |
| RSTP | 802.1w | Средняя | Быстрая | Одно |
| Rapid PVST+ | Cisco | Очень высокая | Быстрая | По одному на каждый VLAN |
| MST | 802.1s | Высокая | Быстрая | По одному на группу VLAN-ов |

# STP – пример



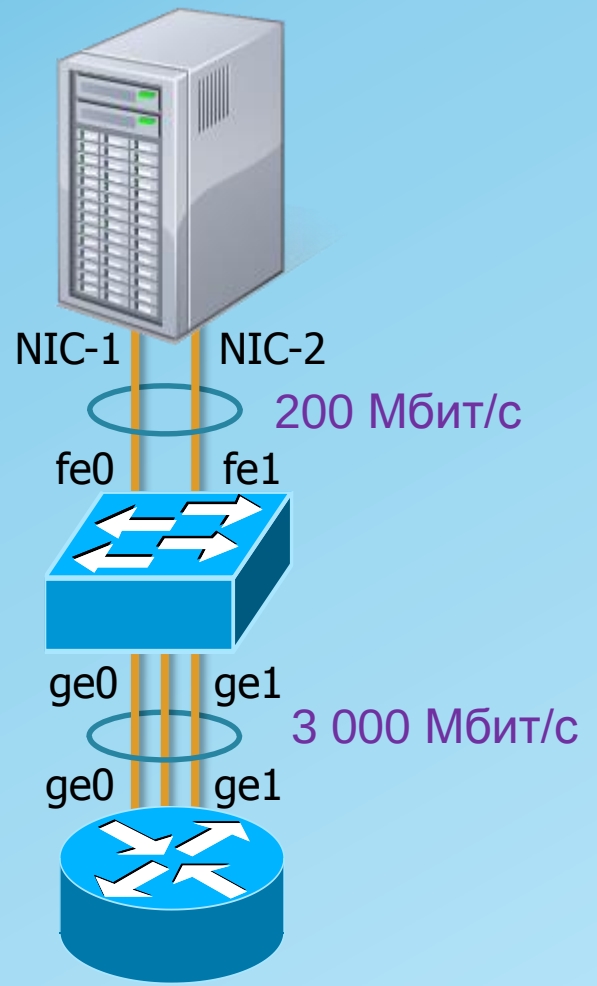

**корневые**
**назначенные**
**отключённые**

# STP – Cisco IOS


- `switch#show spanning-tree […]`
  - выводит сведения о состоянии STP
- `switch(config)#spanning-tree mode { rstp | rapid-pvst | … }`
  - переключает режимы работы STP
- `switch(config)#spanning-tree vlan 152 priority 4096`
  - устанавливает приоритет коммутатора для STP в соответствующем vlan (значение приоритета должно быть кратно 4096)
- `switch(config)#spanning-tree vlan 152 root primary`
  - назначает данный коммутатор корневым для STP в соответствующем vlan
- `switch(config-if)#spanning-tree portfast`
  - включает режим portfast на данном интерфейсе (фактически отключает STP – порт пропускает состояния listening и learning, мгновенно переходя в forwarding)

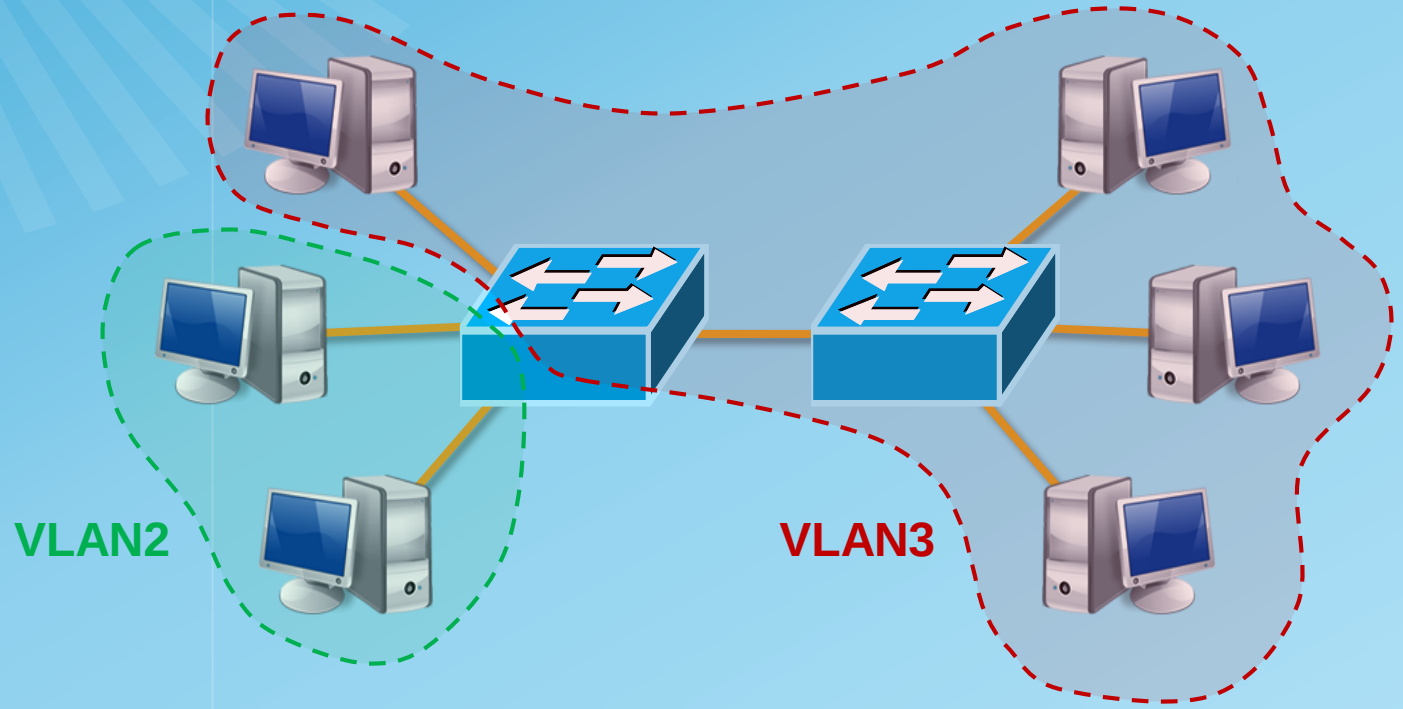
# Агрегирование каналов

- **Агрегирование каналов –** объединение нескольких физических каналов в один логический
  - повышение пропускной способности
  - повышение отказоустойчивости
- IEEE802.3ad, IEEE802.1AX
- Реализации:
  - Port Aggregation Protocol (PAgP)
  - Link Aggregation Control Protocol (LACP)
  - Ручной режим



# Виртуальные локальные сети

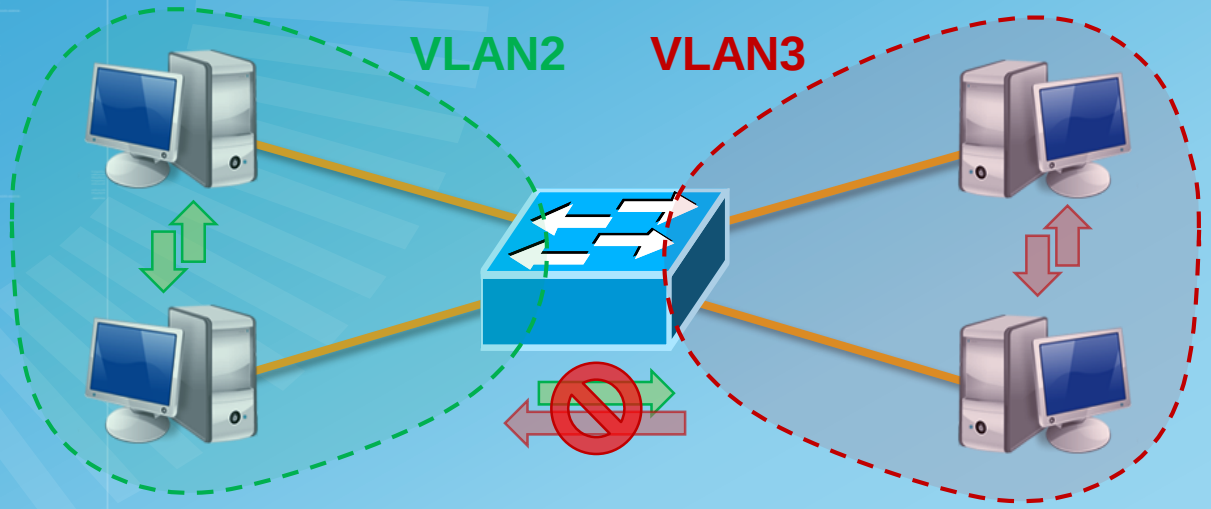
- **Виртуальная локальная сеть** (Virtual LAN, VLAN) – группа узлов сети, трафик которой (в т. ч. широковещательный) на канальном уровне полностью изолирован от других узлов сети.



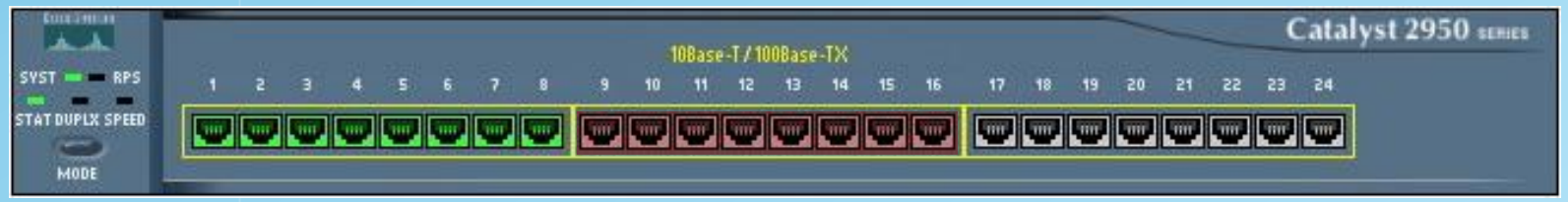
# IEEE 802.1q – тегирование кадров


- **TPID (Tag Protocol Identifier)** – идентификатор протокола тегирования (16 бит). Для 802.1q **0x8100**
- **Priority** – приоритет кадра (3 бита) по QoS
- **CFI (Canonical Format Indicator)** – индикатор канонического формата MAC-адреса (1 бит), используется для обеспечения совместимости между сетями Ethernet и Token ring
- **VLAN identifier (VID)** – идентификатор виртуальной сети (12 бит: от **0** до **4095**)

# VLAN – один коммутатор

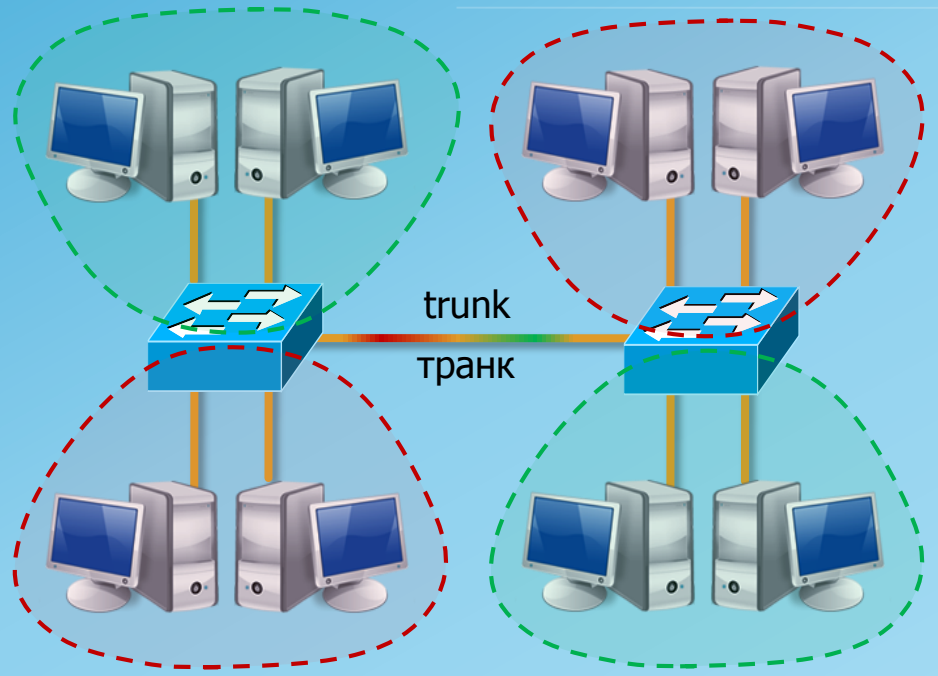


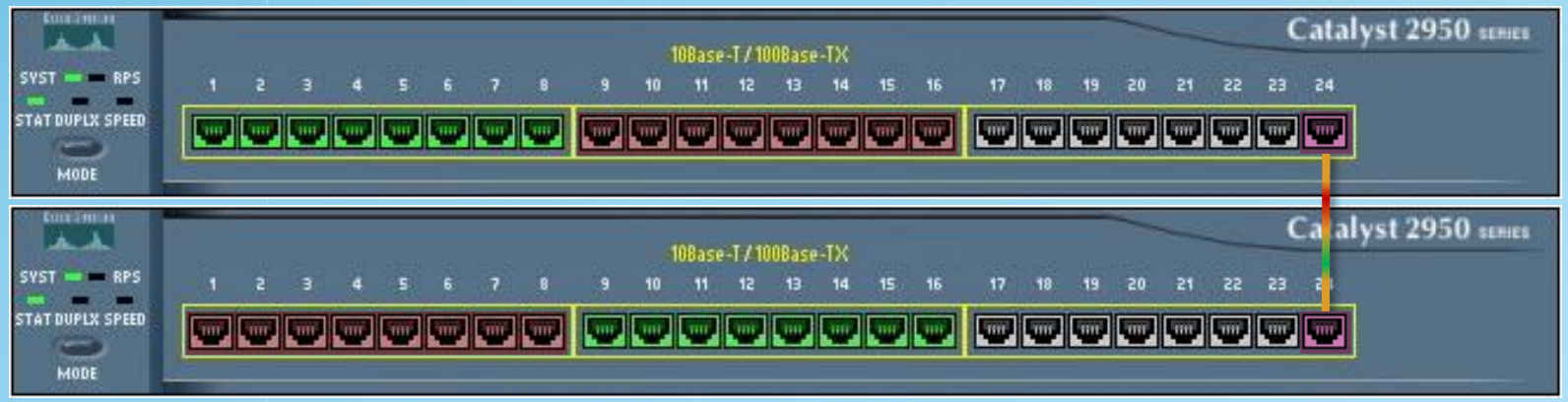

- Каждый VLAN ведет себя как отдельный изолированный коммутатор
- Передача кадров между VLAN-ами средствами канального уровня **невозможна**



# VLAN – несколько коммутаторов

- Несколько коммутаторов могут иметь общие VLAN-ы (должны быть настроены на всех коммутаторах)
- Для передачи тегированных кадров всех VLAN-ов используются специальные логические каналы – транки (trunk)



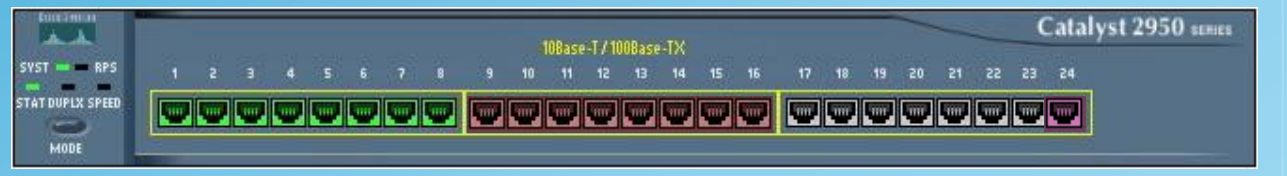



# VLAN – Cisco IOS


- `switch#show vlan`
  - выводит сведения о существующих VLAN-ах
- `switch(config)#vlan 152`
  - переход в режим конфигурирования параметров указанной виртуальной сети
  - создает VLAN с заданным номером, если она не существует
- `switch(config-if)#switchport mode { access | trunk }`
  - переводит текущий интерфейс коммутатора в выбранный режим работы
- `switch(config-if)#switchport access vlan 152`
  - назначает текущему интерфейсу (интерфейс должен работать в режиме доступа – switchport mode access) vlan с указанным номером
  - создает VLAN с заданным номером, если она не существует
- `switch(config-if)#switchport trunk allowed vlan 152 153 […]`
  - задает список виртуальных сетей, которым разрешён доступ в текущий транк

# Статические VLAN

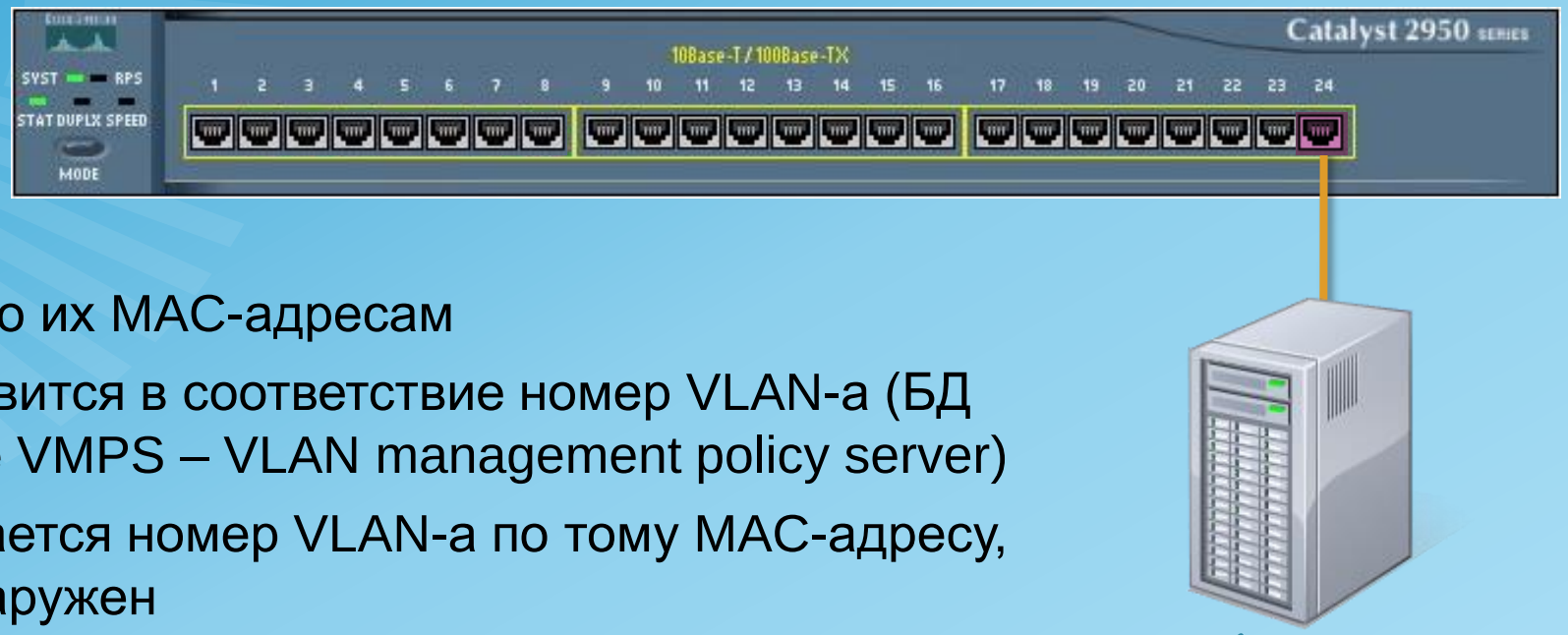
- Группировка узлов по интерфейсам коммутаторов
- Каждому интерфейсу ставится в соответствие номер виртуальной сети
- Все кадры, приходящие на данный интерфейс, тегируются соответствующим идентификатором VLAN
- При отправке кадра с интерфейса тег кадра сравнивается с номером VLAN интерфейса, при несовпадении кадр дропается




| Switch port | VLAN | Switch port | VLAN | Switch port | VLAN |
|---|---|---|---|---|---|
| Fe01 | 2 | Fe09 | 3 | Fe17 | 1 |
| Fe02 | 2 | Fe10 | 3 | Fe18 | 1 |
| Fe03 | 2 | Fe11 | 3 | Fe19 | 1 |
| Fe04 | 2 | Fe12 | 3 | Fe20 | 1 |
| Fe05 | 2 | Fe13 | 3 | Fe21 | 1 |
| Fe06 | 2 | Fe14 | 3 | Fe22 | 1 |
| Fe07 | 2 | Fe15 | 3 | Fe23 | 1 |
| Fe08 | 2 | Fe16 | 3 | Fe24 | trunk |

```
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

# Динамические VLAN



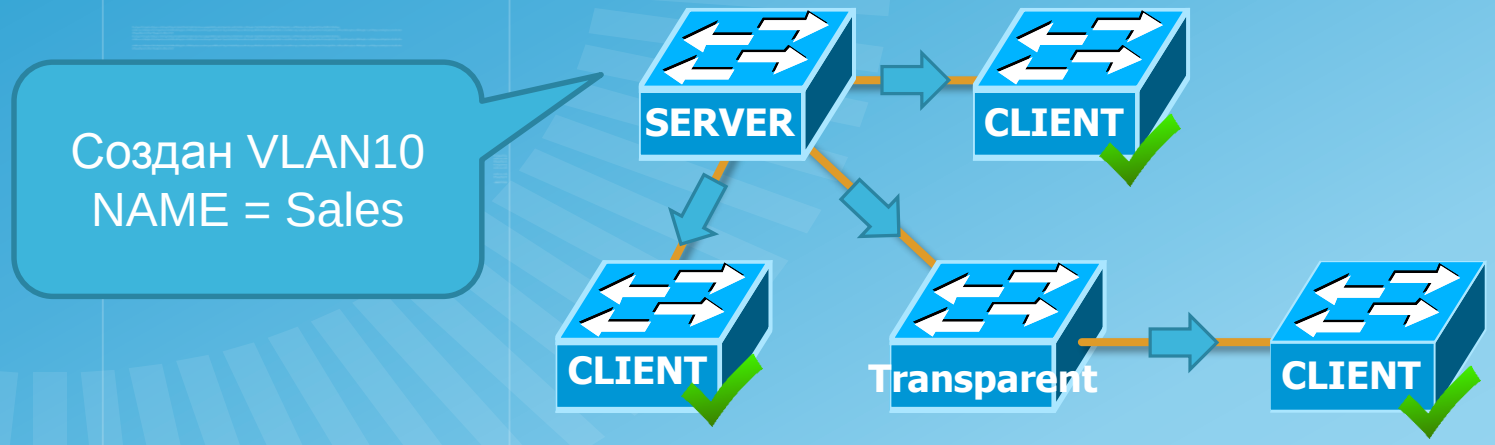

- Группировка узлов по их MAC-адресам
- Каждому адресу ставится в соответствие номер VLAN-а (БД хранится на сервере VMPS – VLAN management policy server)
- Интерфейсу назначается номер VLAN-а по тому MAC-адресу, который на нём обнаружен

```
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan dynamic
```

| Switch port | VLAN |
|---|---|
| Fe01 | dynamic |
| Fe02 | dynamic |
| … | … |
| Fe22 | dynamic |
| Fe23 | dynamic |
| Fe24 | trunk |

| MAC-address | VLAN |
|---|---|
| aaaa.bbbb.0000 | 2 |
| aaaa.bbbb.1111 | 2 |
| aaaa.bbbb.2222 | 3 |

# VLAN Trunking Protocol (vtp)



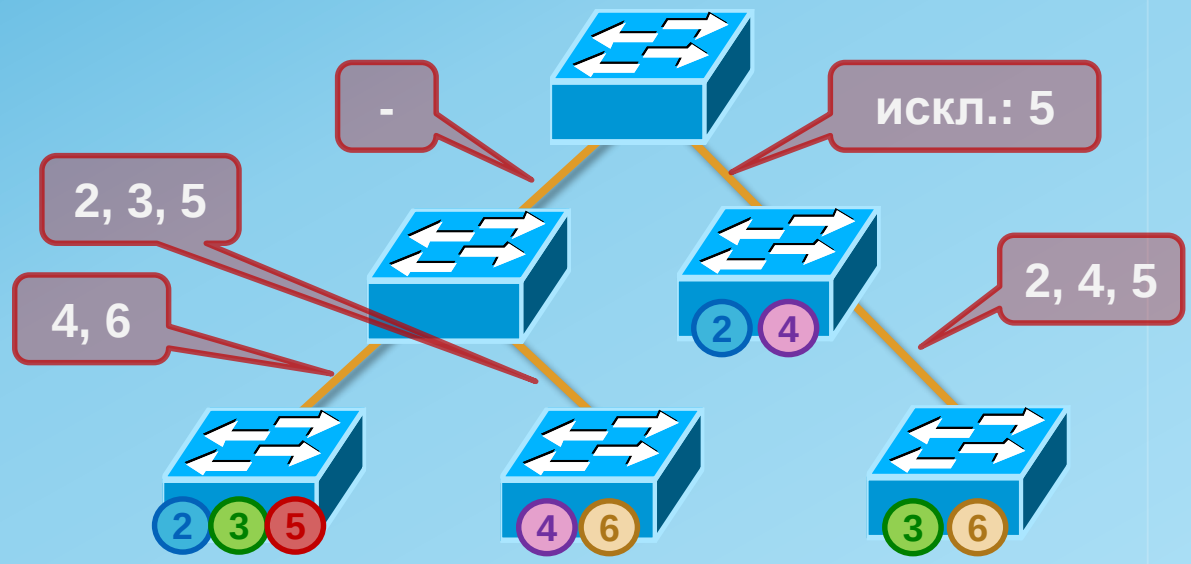

- Проприетарный протокол Cisco – не работает на других коммутаторах
- Обеспечивает автоматическую актуализацию информации о VLAN во на всех коммутаторах VTP-домена (т.е. отменяет необходимость создания / переименования / удаления VLAN на каждом коммутаторе)
- Версия базы VLAN-ов – configuration revision (сравнение при обновлении)
- VTP работает только по транковым портам
- Включает автоматический VTP Pruning

# vtp – Cisco IOS


- `switch#show vtp { status | … }`
  - выводит информацию о состоянии протокола vtp на коммутаторе
- `switch(config)#vtp mode { server | client | transparent }`
  - назначает коммутатору соответствующую роль в текущем домене vtp
- `switch(config)#vtp version { 1 | 2 | 3 }`
  - задает версию протокола vtp
- `switch(config)#vtp domain <имя домена>`
  - задает домен для изолированной работы vtp
- `switch(config)#vtp password <пароль>`
  - задает пароль для доступа к vtp-домену

# VLAN Pruning

- Позволяет исключать ненужные VLAN-ы из транков
- Автоматически работает на основе VTP:
  - Коммутаторы отслеживают, в каких VLAN-ах работает каждый из них
  - Трафик невостребованных VLAN-ов исключается из соответствующих транков
- Возможна ручная настройка




- `switch(config-if)#switchport trunk allowed vlan 152 153 […]`
  - задает список виртуальных сетей, которым разрешён доступ в текущий транк