

# Технология VLAN

 [moxa.ru/tehnologii/ethernet\\_network/tech-vlan](https://moxa.ru/tehnologii/ethernet_network/tech-vlan)

**Зачем нужна  
технология  
VLAN?**

**Как работает  
технология  
VLAN?**

**Режимы работы  
портов  
коммутаторов**

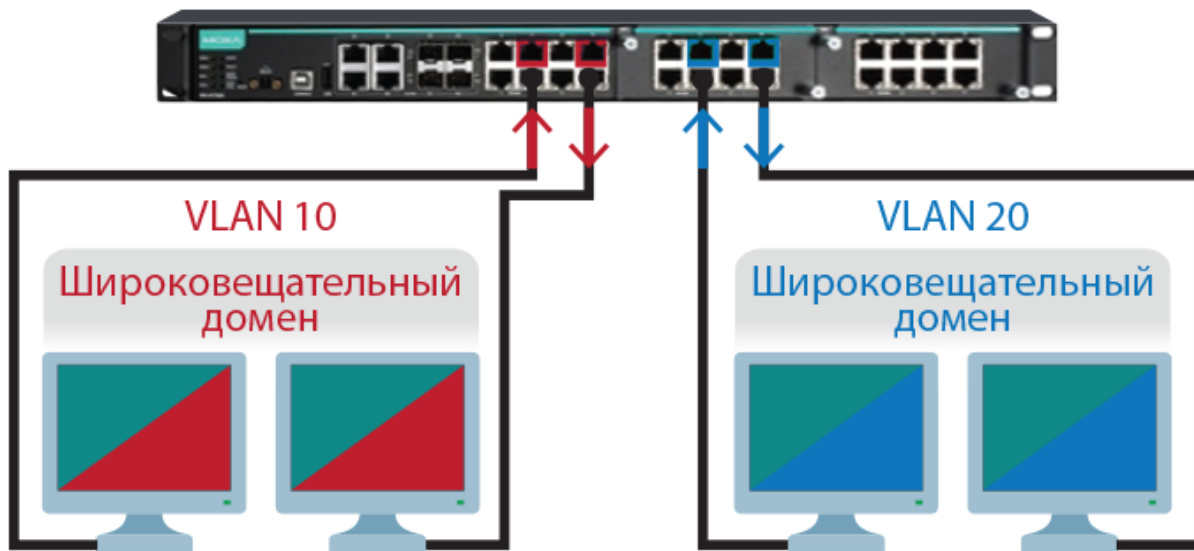
**VLAN на  
коммутаторах  
MOXA**

Локальные сети давно перестали состоять из нескольких абонентских устройств, расположенных внутри одного помещения. Современные сети предприятий представляют собой распределенные системы, состоящие из большого количества устройств разного назначения. Ситуация вынуждает разделять такие большие сети на автономные подсети, в итоге логические структуры сети отличаются от физических топологий. Подобные системы создаются с помощью технологии VLAN (Virtual Local Area Network – виртуальная локальная сеть), которая позволяет разделить одну локальную сеть на отдельные сегменты.

## Зачем нужна технология VLAN?

Технология VLAN обеспечивает:

- **Гибкое построение сети** — VLAN позволяет произвести сегментацию локальной сети на подсети по функциональному признаку независимо от территориального расположения устройств. То есть устройства одной подсети VLAN могут быть подключены к разным коммутаторам, удаленным друг от друга. И наоборот, к одному коммутатору могут быть подключены устройства, относящиеся к разным подсетям VLAN
- **Увеличение производительности** – VLAN разделяет подсеть на отдельные широковещательные домены. Это означает, что широковещательные сообщения будут получать только устройства, находящиеся в одной VLAN-подсети. Построение системы с использованием технологии VLAN позволяет уменьшить широковещательный трафик внутри сети, тем самым снижается нагрузка на сетевые устройства и улучшается производительность системы в целом.
- **Улучшение безопасности** – Устройства из разных подсетей VLAN не могут общаться друг с другом, что уменьшает шансы произвести несанкционированный доступ к устройствам системы. Связь между разными подсетями возможна только через маршрутизатор. Кроме того, использование маршрутизатора позволяет настроить политики безопасности, которые могут быть применены сразу ко всей группе устройств, принадлежащей одной подсети.



## Как работает технология VLAN?

У каждой VLAN-подсети есть свой идентификатор, по которому определяется принадлежность той или иной подсети. Информация об идентификаторе содержится в теге, который добавляется в тело Ethernet-фрейма сети, в которой внедрено разделение на подсети VLAN.

Самый распространенный стандарт, описывающий процедуру тегирования трафика, – это открытый стандарт 802.1 Q. Кроме него есть проприетарные протоколы, но они менее популярны.

### Формат Ethernet – фрейма после тегирования:



### Тег размером 4 байта состоит из нескольких полей:

- **TPID (Tag Protocol Identifier)** — Идентификатор протокола тегирования. Для стандарта 802.1Q значение TPID - 0x8100
- **P-тег** – Определяет приоритет пакета. Используется при работе стандарта 802.1p для определения очередности обработки пакетов
- **CFI (Canonical Format Indicator)** – Идентификатор формата MAC-адреса, который использовался для совместимости между сетями Ethernet и Token Ring. В настоящее время поле CFI не используется в связи с отказом от сетей Token Ring
- **VLAN ID** – Идентификатор VLAN. Определяет, какой подсети VLAN принадлежит пакет

Именно по тегу сетевое оборудование определяет принадлежность пакета той или иной сети VLAN, осуществляет фильтрацию пакетов и определяет дальнейшие действия с ними: снять тег и передать на конечное оборудование, отбросить пакет, переслать следующему получателю с сохранением тега. Правила, определяющие действия с пакетом на основе тега, зависят от режима работы порта сетевого оборудования. В свою очередь, режим работы выбирается в соответствии с характеристиками подключаемого оборудования. В системе может присутствовать как оборудование с поддержкой технологии VLAN, так и без нее.

## Режимы работы портов коммутаторов

---

**Access-port** – порт доступа, передающий нетегированный трафик.

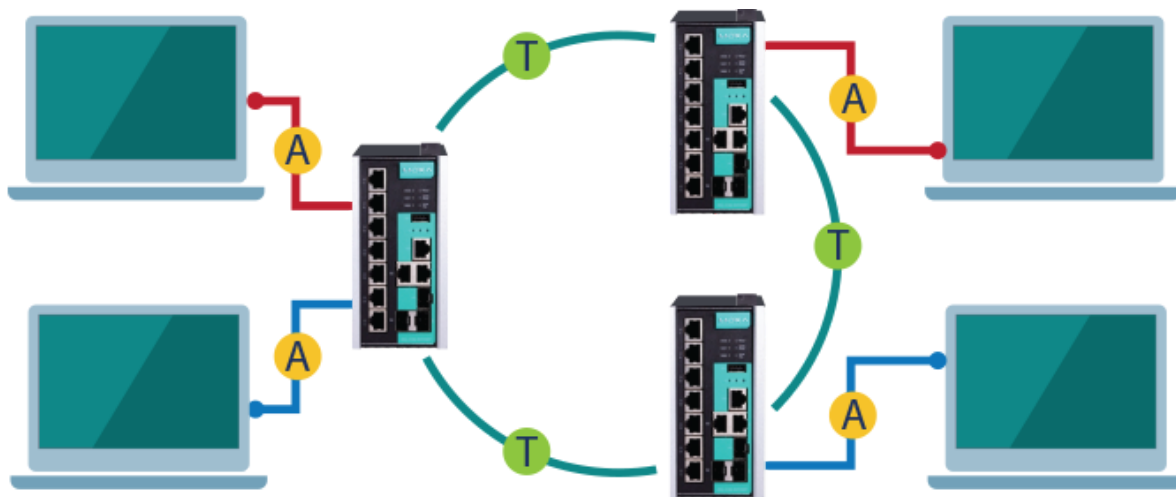
Используется для подключения конечных устройств, не поддерживающих технологию VLAN



Тип Access назначается порту коммутатора, к которому подключено либо единичное абонентское устройство, либо группа устройств, находящихся в одной подсети. Кроме выбора режима работы порта Access необходимо указать идентификатор VLAN-подсети, к которой будет принадлежать оборудование, находящееся за этим портом.

Коммутатор, получив в порт Access данные от подключенных к нему абонентских устройств, добавит ко всем Ethernet-кадрам общий тег с заданным идентификатором подсети и далее будет оперировать уже тегированным пакетом. Напротив, принимая из основной сети данные, предназначенные Access-порту, коммутатор сверит идентификатор VLAN принимаемого пакета с номером VLAN-подсети этого порта. Если они совпадут, то данные будут успешно переданы в порт, а тег удалён, таким образом, подключенные к порту устройства продолжат работать без необходимости поддержки VLAN. Если же идентификатор не равен номеру подсети, кадр будет отброшен, не позволив передать пакет из «чужой» подсети VLAN.

**Trunk-port** – магистральный порт, передающий тегированные пакеты данных. Используется для подключения сетевых устройств с поддержкой VLAN, чаще всего для соединения коммутаторов между собой.



Помимо задания режима работы и идентификатора VLAN, при конфигурировании Trunk-портов создается список разрешенных для передачи подсетей VLAN, с которым коммутатор сверяется при получении пакетов. Благодаря этому через Trunk-порты могут передаваться пакеты нескольких VLAN-подсетей.

Коммутатор, получив в порт Trunk нетегированные данные, поступит аналогично Access-порту, т.е. промаркирует пакеты идентификатором VLAN-подсети, присвоенном этому порту, и передаст дальше в сеть. При получении пакета с таким же идентификатором VLAN, как и у самого порта, тег будет снят и данные отправлены на абонентское устройство без тега. В случае получения тегированного пакета с идентификатором VLAN, отличающимся от номера, присвоенного порту, коммутатор сравнит идентификатор со списком разрешенных VLAN-подсетей. Если номер будет указан в списке, то данные будут переданы по сети на следующее устройство без изменения тега. В случае, если идентификатор указывает на принадлежность незнакомой подсети VLAN, то пакет будет отброшен.

## VLAN на коммутаторах Moxa

### ЗАДАЧА:

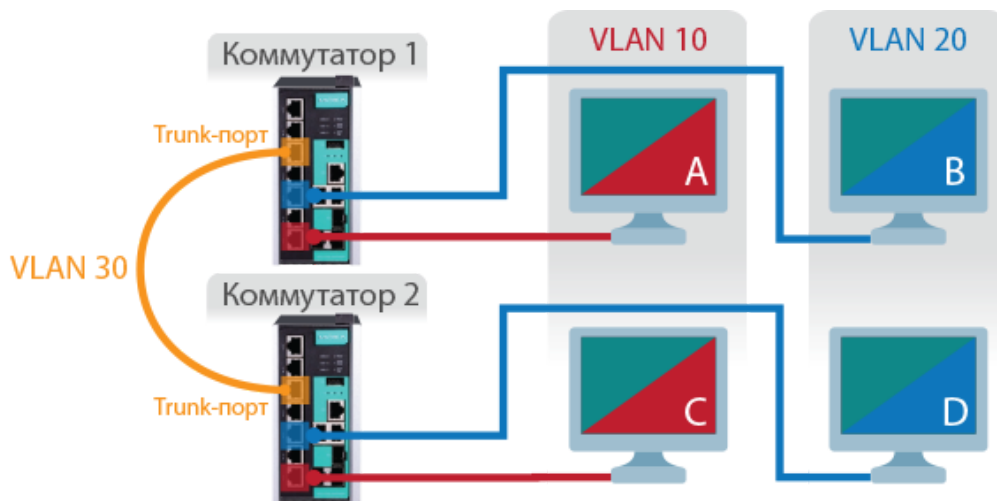
Необходимо построить общую сеть предприятия с разграничением доступа между технологической сетью, предназначенной для управления и мониторинга технологическими процессами и сетью общего назначения. Кроме того, оборудование одной подсети установлено на территориальном удалении друг от друга.

Организовать подобную систему можно с помощью технологии VLAN. Рассмотрим пример реализации данной задачи на коммутаторах Moxa EDS-510E-3GTXSFP.

Технологию VLAN поддерживают все управляемые коммутаторы Moxa.

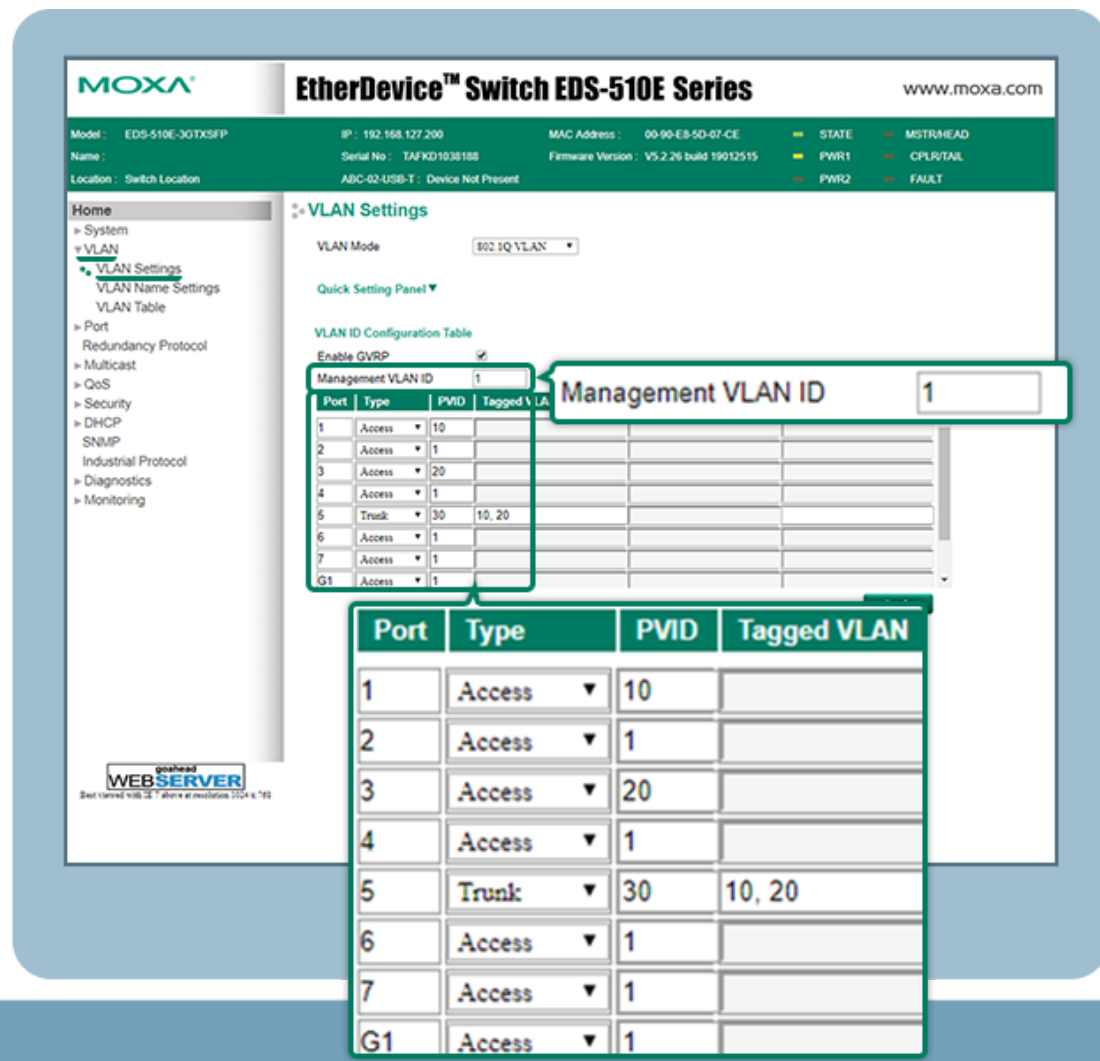
Оборудование, которое должно находиться в технологической сети (компьютеры А и С), отнесем в подсеть с идентификатором VLAN 10. Оборудование сети общего назначения отнесем в подсеть с идентификатором VLAN 20 (компьютеры В и D). Обмен между этими подсетями происходить не будет. В то же время из-за удаленного расположения устройств оборудование одной VLAN-подсети

подключено к разным коммутаторам и необходимо обеспечить обмен данными между ними. Для этого объединим коммутаторы с помощью Trunk портов и поместим их в отдельную подсеть с идентификатором VLAN 30.



### Конфигурирование коммутаторов:

- Порты, к которым подключены устройства A и C, устанавливаем в режим access и назначаем PVID равный 10 (Порт 1 на скриншоте)
- Порты, к которым подключены устройства B и D, устанавливаем также в режим access и назначаем PVID равный 20 (Порт 3 на скриншоте)
- Коммутаторы между собой соединяются через trunk-порты. Назначаем этим портам PVID 30. Чтобы trunk-порты пропускали трафик от других VLAN-подсетей (в нашем случае 10 и 20), нужно указать VLAN 10 и 20 в качестве разрешенных. (Порт 5 на скриншоте)



- **PVID (Port VLAN Identifier)** – идентификатор VLAN-подсети, к которой относится оборудование, подключенное к порту
- **Tagged VLAN** – список разрешенных VLAN

Кроме того, следует обратить внимание на параметр Management VLAN ID – подсеть управления коммутатором. Компьютер, с которого необходимо управлять и следить за состоянием самих коммутаторов, должен находиться в подсети управления, указанной в Management VLAN ID. По умолчанию Management VLAN ID = 1, но для предотвращения несанкционированного доступа к коммутаторам рекомендуется идентификатор VLAN управления менять на любой свободный.

Обмен данными в сети предприятия будет осуществляться в соответствии с правилами обработки пакетов.

### Правила обработки пакетов для портов Access

- Входящие правила
  - Если фрейм без VID, то добавить тег с идентификатором равным PVID
  - Если фрейм с VID = PVID, то принять пакет. Иначе – пакет отбросить.
- Исходящие правила
  - Удалить тег

## Правила обработки пакетов для портов Trunk

- Входящие правила
  - Если фрейм без VID, то добавить тег с идентификатором равным PVID
  - Если фрейм с VID = PVID или VID есть в Tagged VLAN, то принять пакет.  
Иначе – пакет отбросить
- Исходящие правила
  - Если фрейм с VID = PVID, то снять тег
  - Если фрейм с VID есть в Tagged VLAN, то оставить тег

Таким образом, технология VLAN позволит создать гибкую систему предприятия с объединением удаленного оборудования и разграничением доступа между функциональными сегментами сети.

## Устройства, доступные для заказа в России:

---

### Рекомендуем почитать

---


Технология кольцевого резервирования Turbo Ring

 Сети Ethernet

QoS – Приоритизация трафика

 Сети Ethernet

Синхронизация точного времени. Стандарт IEEE 1588.

 Решения для электроэнергетики

Технология резервирования Turbo Chain

 Сети Ethernet