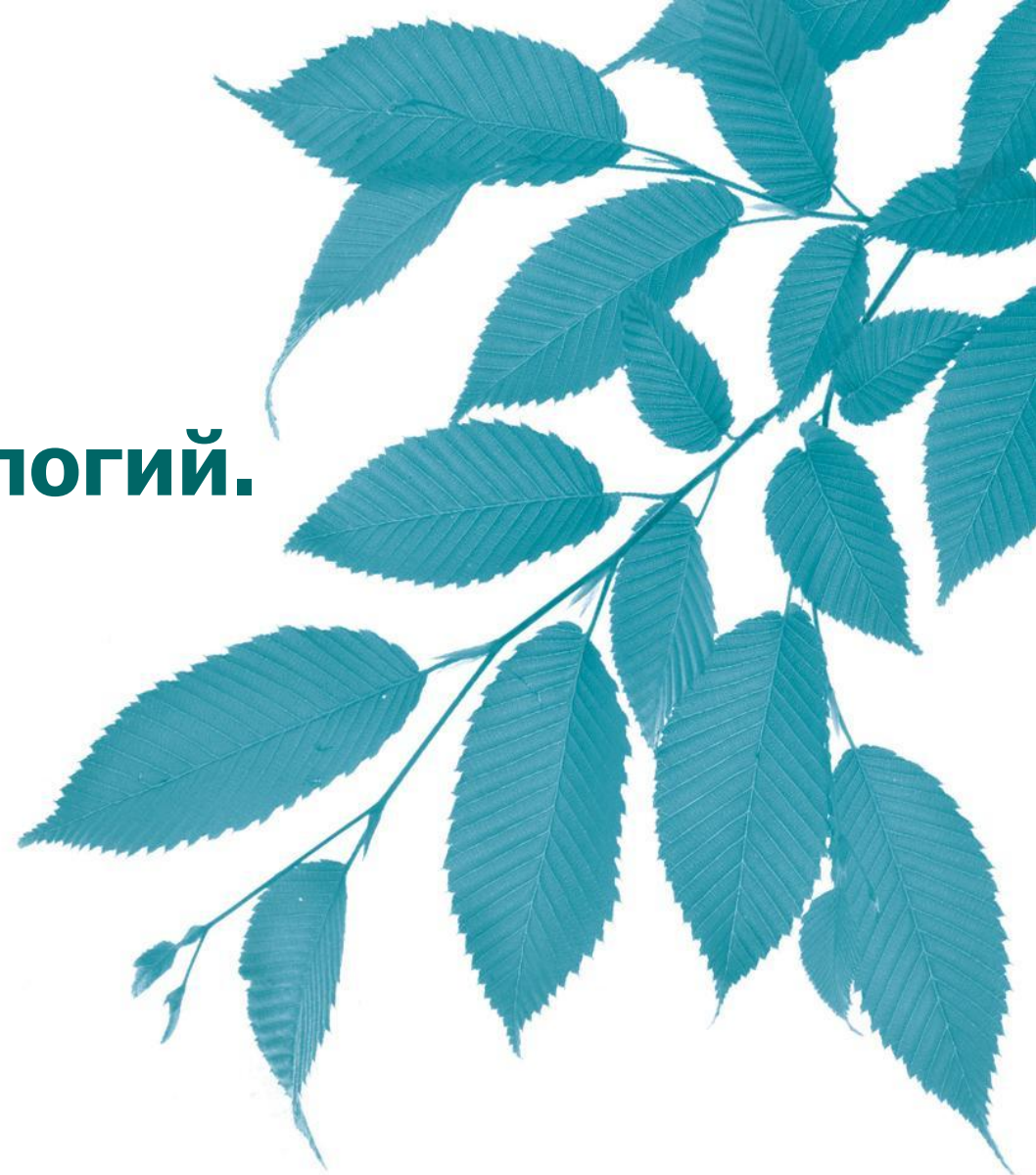




Основы сетевых технологий. Часть 1: Передача и коммутация данных в компьютерных сетях

Сертификационный курс

Лекция 6



Лекция 6

Технологии коммутации

Лекция 6. Технологии коммутации

- ☐ Алгоритм прозрачного моста;
- ☐ Методы коммутации;
- ☐ Конструктивное исполнение коммутаторов;
- ☐ Физическое стекирование коммутаторов;
- ☐ Технологии коммутации и модель OSI;
- ☐ Программное обеспечение коммутаторов;
- ☐ Общие принципы сетевого дизайна;
- ☐ Трехуровневая иерархическая модель сети;
- ☐ Протокол Spanning Tree Protocol (STP);
- ☐ Виртуальные локальные сети (VLAN);
- ☐ Технология Power over Ethernet.

- ❑ В настоящее время основным строительным блоком для создания локальных сетей являются **коммутаторы** (коммутаторы Ethernet, т.к. Ethernet является основной технологией локальных сетей).
- ❑ **Коммутатор:**
 - ❑ представляет собой многопортовый мост;
 - ❑ функционирует на канальном уровне модели OSI;
 - ❑ устанавливает одновременно несколько соединений между разными парами портов.
- ❑ **Наиболее распространенными и широко используемыми в настоящее время функциями коммутаторов являются:**
 - ❑ виртуальные локальные сети (VLAN);
 - ❑ семейство протоколов Spanning Tree – IEEE 802.1D, 802.1w, 802.1s;
 - ❑ статическое и динамическое по протоколу IEEE 802.1ad агрегирование каналов Ethernet;
 - ❑ обеспечение качества обслуживания QoS;
 - ❑ функции обеспечения безопасности, включая аутентификацию 802.1X, функции Port Security, IP-MAC-Port Binding и т.д.;
 - ❑ SNMP-управление и др.

Алгоритм прозрачного моста

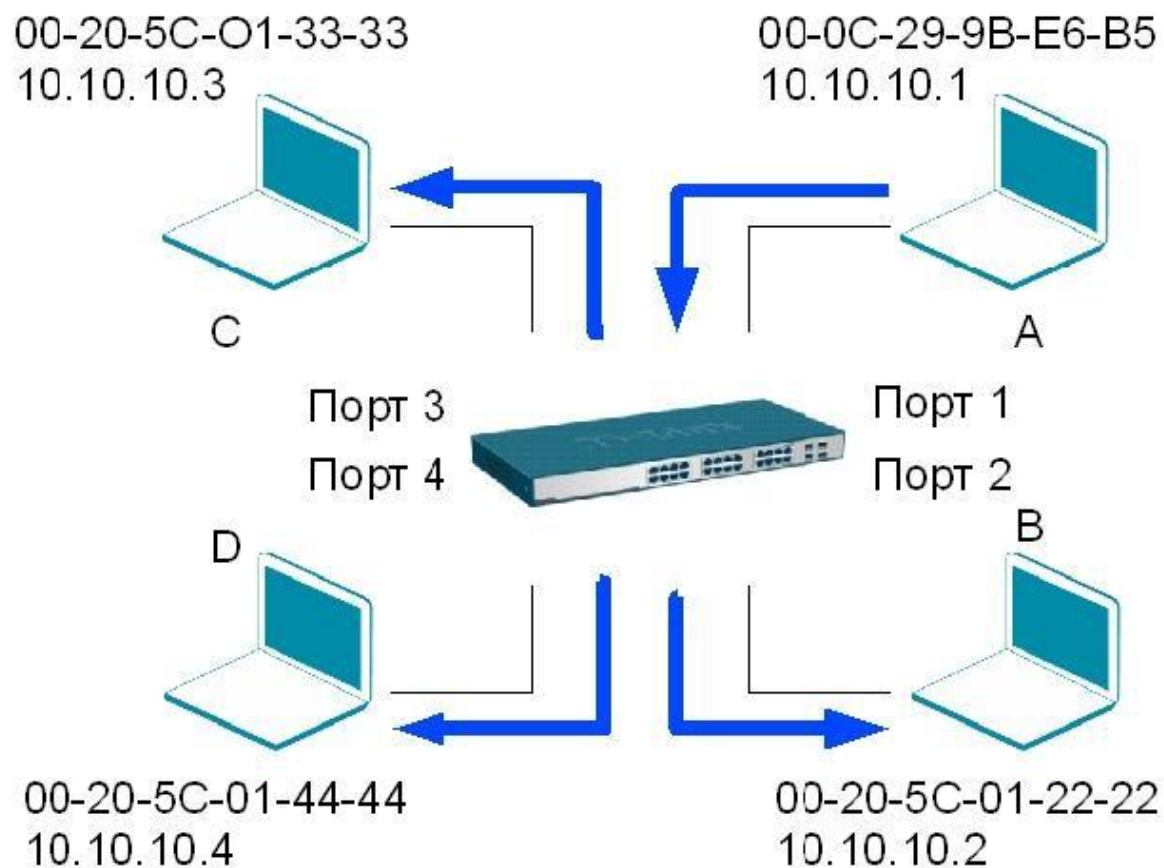
- ❑ Коммутаторы локальных сетей обрабатывают кадры на основе **алгоритма прозрачного моста** (transparent bridge), который определен стандартом IEEE 802.1D.
- ❑ **Модель работы прозрачного моста, описанная в IEEE 802.1D, определяет следующие процессы:**
 - ❑ продвижение кадров (Forwarding);
 - ❑ изучение адресов (Learning);
 - ❑ фильтрация кадров (Filtering).
- ❑ Процесс работы алгоритма прозрачного моста начинается с построения **таблицы коммутации** (Forwarding DataBase, FDB).

Алгоритм прозрачного моста

Построение таблицы коммутации

6 байт	6 байт	2 байта	4 байта	
Адрес назначения	Адрес источника	Тип Ethernet	ARP	FCS
FF-FF-FF-FF-FF-FF	00-0C-29-9B-E6-B5	Ethernet		

Таблица коммутации
Порт 1 00-0C-29-9B-E6-B5

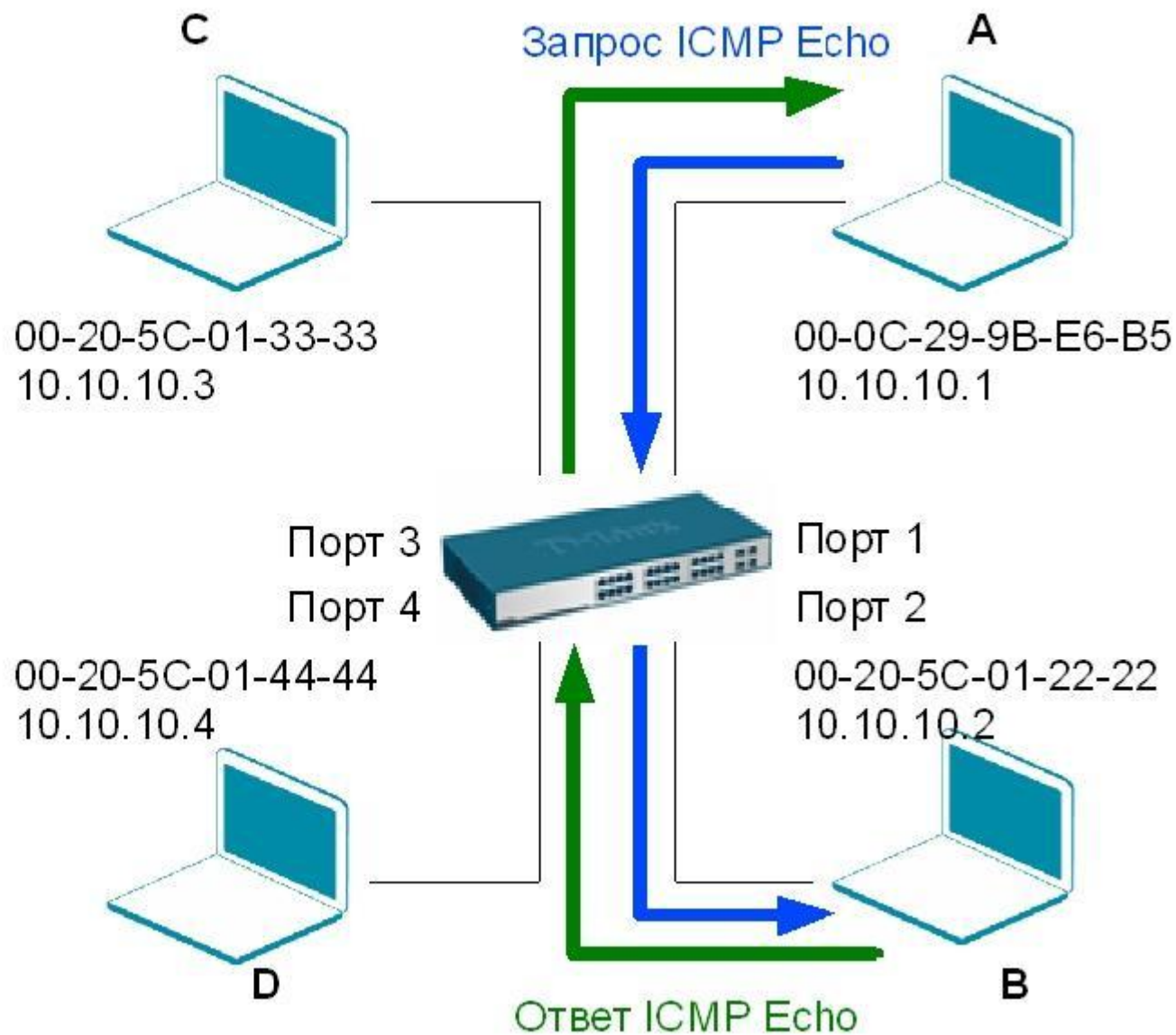


Алгоритм прозрачного моста

Передача кадра с порта на порт коммутатора

Таблица коммутации

Порт 1	00-0C-29-9B-E6-B5
Порт 2	00-20-5C-01-22-22



- ❑ Прежде чем принять решение о передаче кадра, коммутатор получает и анализирует его содержимое. В современных коммутаторах используются следующие методы коммутации пакетов, определяющие поведение устройства при получении кадра:
 - ❑ **коммутация с промежуточным хранением** (store-and-forward);
 - ❑ **коммутация без буферизации** (cut-through).

Метод коммутации store-and-forward



Метод коммутации cut-through



Конструктивное исполнение коммутаторов

- В зависимости от конструктивного исполнения (габаритных размеров), можно выделить три группы коммутаторов:
 - **настольные коммутаторы** (Desktop switch);
 - **автономные коммутаторы, монтируемые в телекоммуникационную стойку** (Rack mounted switch);
 - **коммутаторы на основе шасси** (Chassis switch).

Конструктивное исполнение коммутаторов

Настольные коммутаторы

- Обычно такие коммутаторы обладают корпусом обтекаемой формы с относительно небольшим количеством фиксированных портов, внешним или внутренним блоком питания, ножками (обычно резиновыми) для обеспечения вентиляции нижней поверхности устройства.
- Чаще всего коммутаторы настольного форм-фактора используются в сетях класса *SOHO* (Small Office, Home Office), где не требуется высокая производительность и расширенные сетевые функции.



Конструктивное исполнение коммутаторов

Автономные коммутаторы в стойечном исполнении

- ❑ Высотой 1U обладают корпусом для монтажа в 19" стойку, встроенным блоком питания и фиксированным количеством портов. По сравнению с настольными коммутаторами, коммутаторы, монтируемые в стойку, обеспечивают более высокую производительность и надежность, а также предлагают широкий набор сетевых функций и интерфейсов.
- ❑ Используются на уровнях доступа и распределения сетей малых и средних предприятий (*Small to Medium Business, SMB*), корпоративных сетей и сетей провайдеров услуг (*Internet Service Provider, ISP*).



Конструктивное исполнение коммутаторов

Стековые коммутаторы

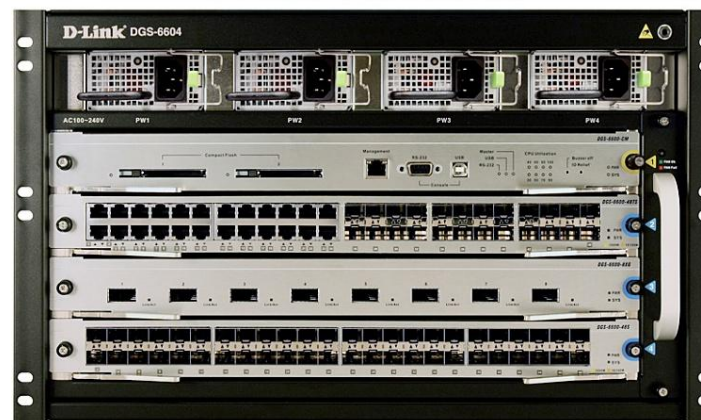
- ❑ Устройства представляют собой коммутаторы, которые могут работать как автономно, потому что выполнены в отдельном корпусе, так и совместно благодаря наличию специальных интерфейсов, позволяющих объединять коммутаторы в одно логическое устройство для увеличения количества портов, удобства управления и мониторинга.
- ❑ В этом случае отдельные коммутаторы образуют стек.



Конструктивное исполнение коммутаторов

Коммутаторы на основе шасси

- ❑ Содержат слоты, которые могут быть использованы для установки интерфейсных модулей расширения, резервных источников питания и процессорных модулей. Модульное решение обеспечивает гибкость применения, высокую плотность портов и возможность резервирования критичных для функционирования коммутатора компонентов.
- ❑ Коммутаторы на основе шасси предназначены для работы в крупных корпоративных магистральных сетях, городских сетях или сетях операторов связи.



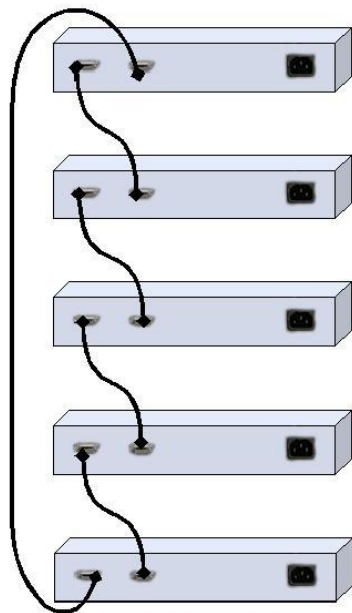
Физическое стекирование коммутаторов

❑ **Стек кольцевой топологии**

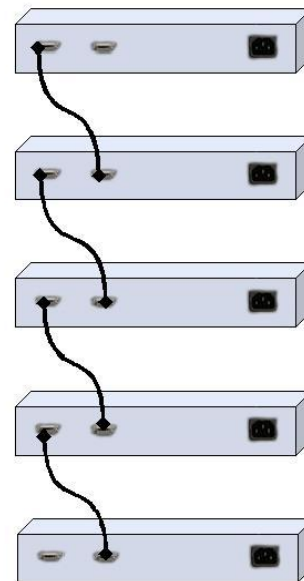
- ❑ каждое устройство в стеке подключается к вышележащему и нижележащему, при этом самый нижний и самый верхний коммутатор в стеке также соединяются;
- ❑ преимуществом кольцевой топологии является то, что при выходе одного устройства из строя или обрыве связи остальные устройства стека продолжают работу в обычном режиме.

❑ **Стек линейной топологии**

- ❑ каждое устройство также соединено с вышележащим и нижележащим, но самый верхний и самый нижний коммутаторы не соединяются.



Топология стекирования «кольцо»



Топология стекирования «цепочка»

- ❑ Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры.
- ❑ Различают:
 - ▣ **Коммутаторы уровня 2** (Layer 2 (L2) switch) анализируют входящие кадры, принимают решение об их дальнейшей передаче и передают их узлам назначения на основе MAC-адресов канального уровня модели OSI.
 - ▣ **Коммутатор уровня 3** (Layer 3 (L3) switch) осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI. Коммутаторы 3-го уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

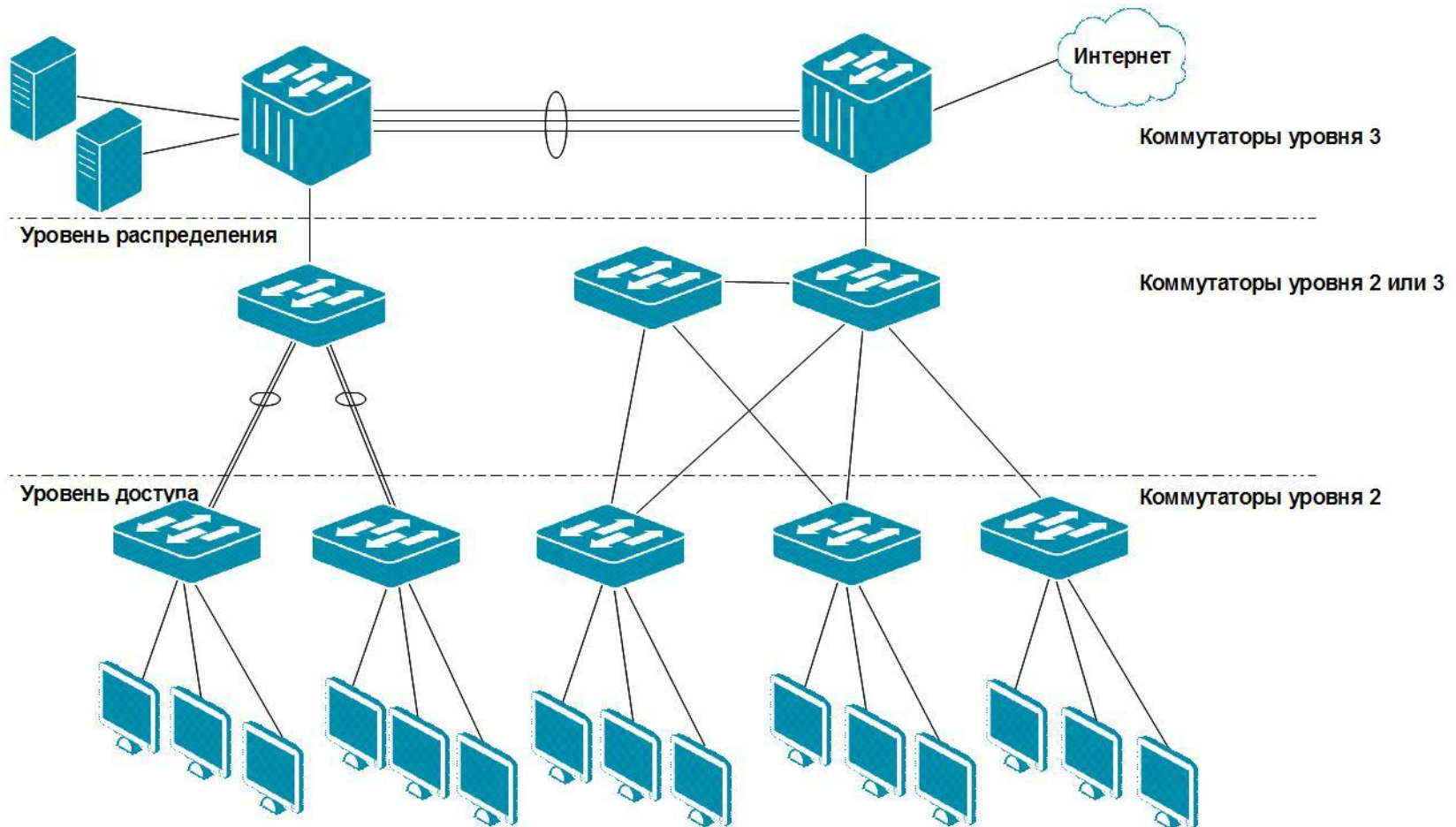
Программное обеспечение коммутаторов

- ❑ Программное обеспечение коммутаторов D-Link предоставляет набор сервисов, предназначенных для выполнения различных функций, обеспечивающих безопасность, отказоустойчивость сети, управление многоадресной рассылкой, качество обслуживания (QoS), а также развитые средства настройки и управления.
- ❑ Программное обеспечение коммутаторов взаимодействует с приложениями D-Link D-View v.6, представляющими собой прикладные программы сетевого управления. Эти управляющие программы поддерживаются всей линейкой управляемых коммутаторов D-Link.
- ❑ Компания D-Link предоставляет возможность бесплатного обновления программного обеспечения коммутаторов по мере появления новых версий с обновленным функционалом.

- ❑ Грамотный сетевой проект основывается на многих принципах, базовыми из которых являются:
 - ❑ изучение возможных точек отказа;
 - ❑ определение типа трафика сети;
 - ❑ анализ доступной полосы пропускания;
 - ❑ создание сети на базе иерархической или модульной модели.

Трехуровневая иерархическая модель сети

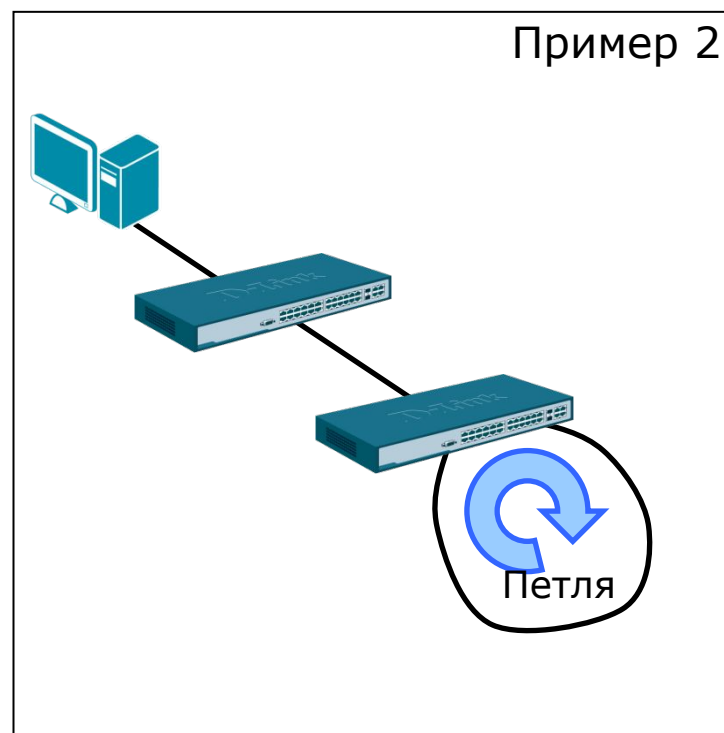
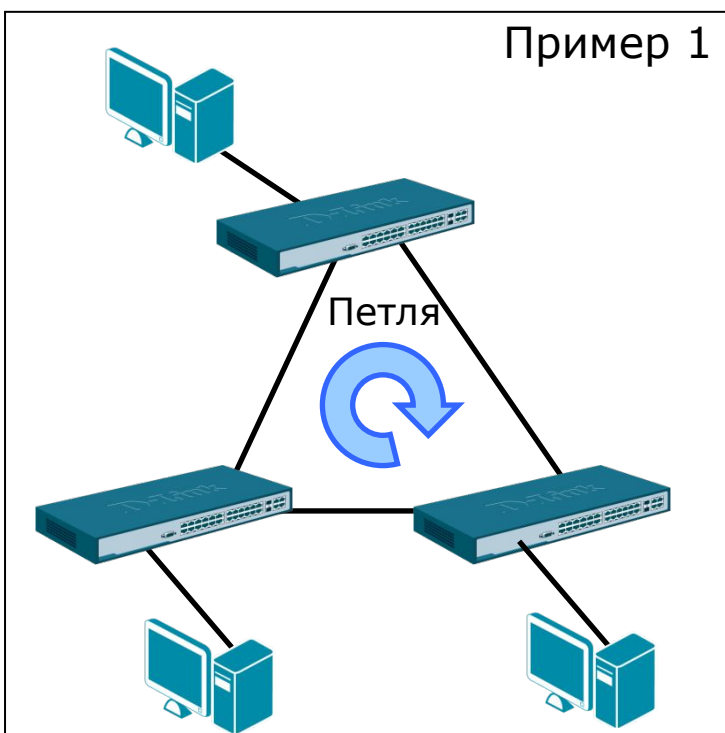
- ❑ Иерархическая модель определяет подход к проектированию сетей и включает в себя три логических уровня:
 - ❑ уровень доступа (access layer);
 - ❑ уровень распределения/агрегации (distribution layer);
 - ❑ уровень ядра (core layer).



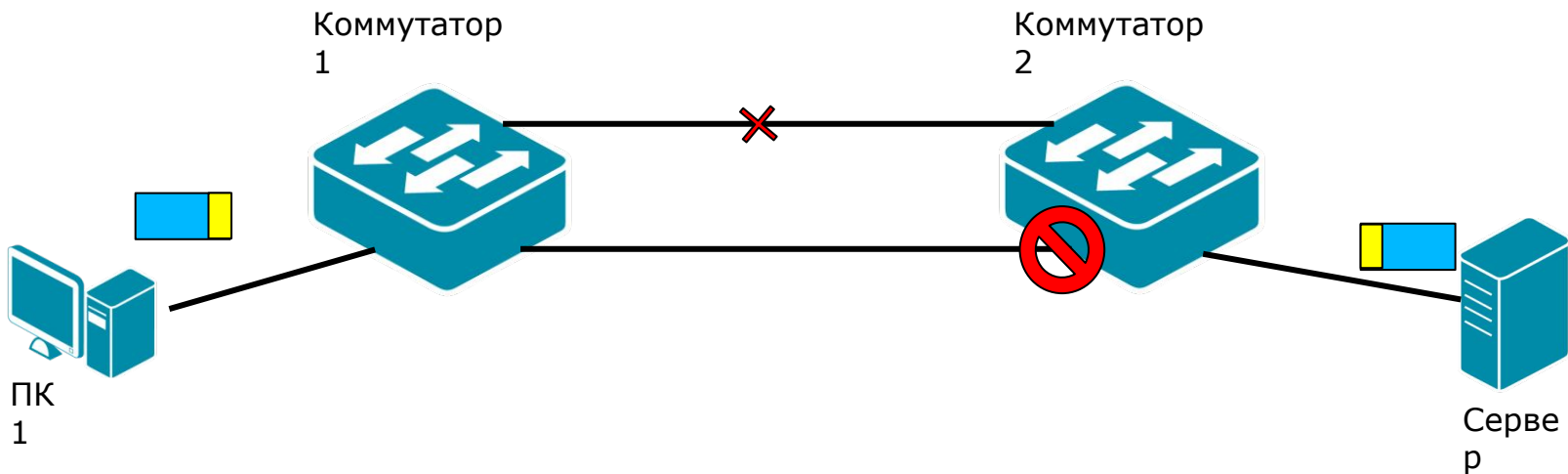
Протокол Spanning Tree (STP)

Понятие петель

- ❑ Коммутационные петли создают проблемы, самые актуальные из которых:
 - ❑ широковещательные штормы;
 - ❑ множественные копии кадров;
 - ❑ множественные петли.



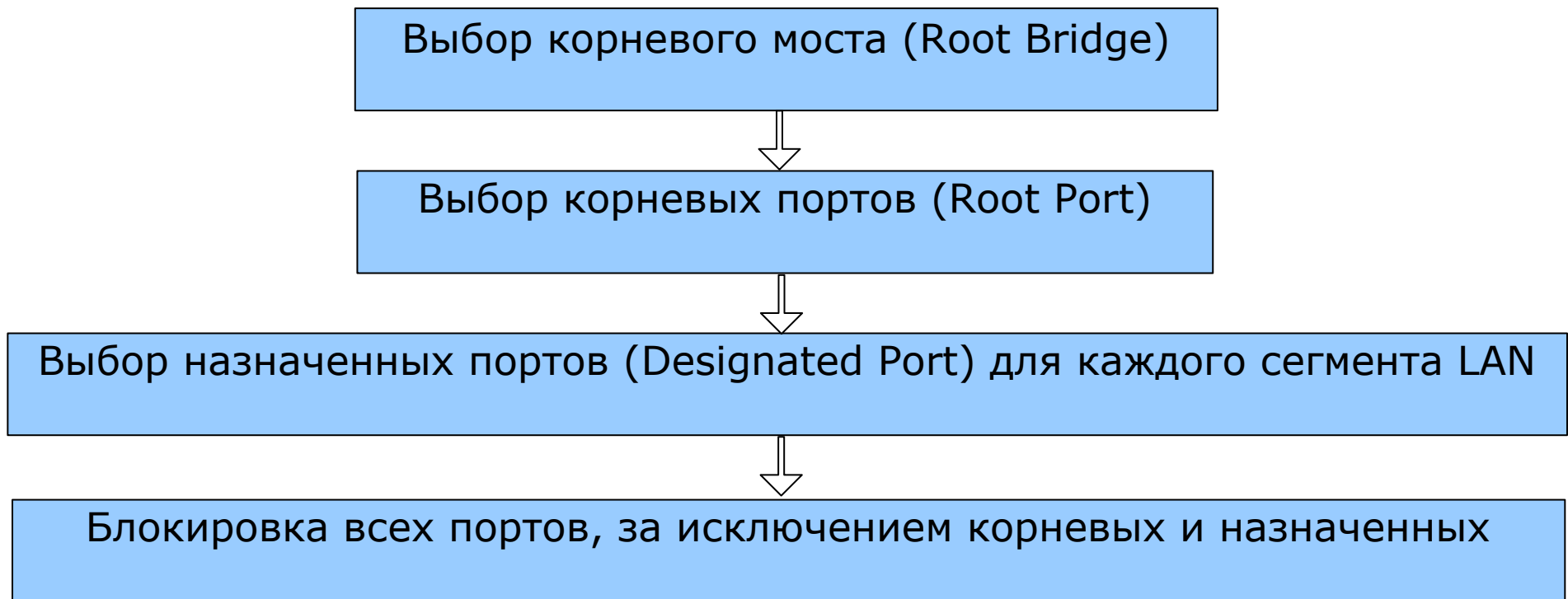
Протокол Spanning Tree (STP)



- ❑ **Протокол связующего дерева Spanning Tree Protocol (STP) является протоколом 2 уровня модели OSI, который:**
 - ❑ позволяет строить древовидные, свободные от петель, конфигурации связей между коммутаторами локальной сети;
 - ❑ обеспечивает возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода активных каналов из строя.
- ❑ **В настоящее время существуют следующие версии протоколов связующего дерева:**
 - ❑ IEEE 802.1D Spanning Tree Protocol (STP);
 - ❑ IEEE 802.1w Rapid Spanning Tree Protocol (RSTP);
 - ❑ IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

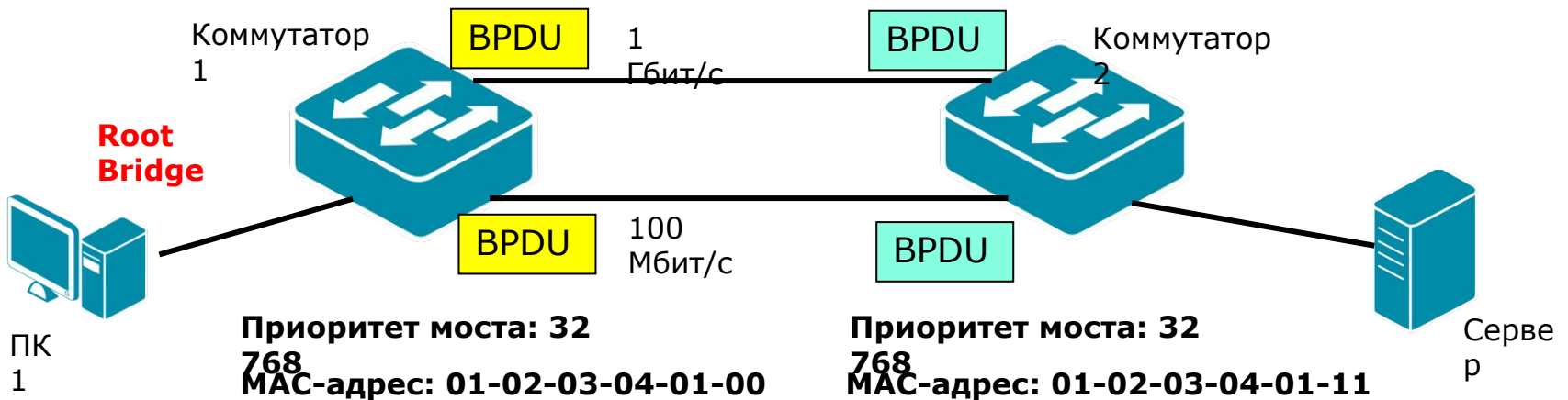
Протокол Spanning Tree (STP)

Построение активной топологии связующего дерева



- ❑ Конфигурация связующего дерева строится коммутаторами автоматически с использованием обмена служебными кадрами, называемыми **Bridge Protocol Data Units (BPDU)**.
- ❑ Для построения устойчивой активной топологии с помощью протокола STP необходимо с каждым коммутатором сети ассоциировать уникальный **идентификатор моста** (Bridge ID), а с каждым портом коммутатора ассоциировать **стоимость пути** (Path Cost) и **идентификатор порта** (Port ID).

Протокол Spanning Tree (STP)



Выбор корневого моста:

- ❑ Каждый коммутатор имеет уникальный *идентификатор моста*. Идентификатор моста – это 8-байтное поле, которое состоит из 2-х частей:
 - ❑ Приоритет моста (Bridge Priority) - 2 байта;
 - ❑ MAC-адрес - 6 байт.

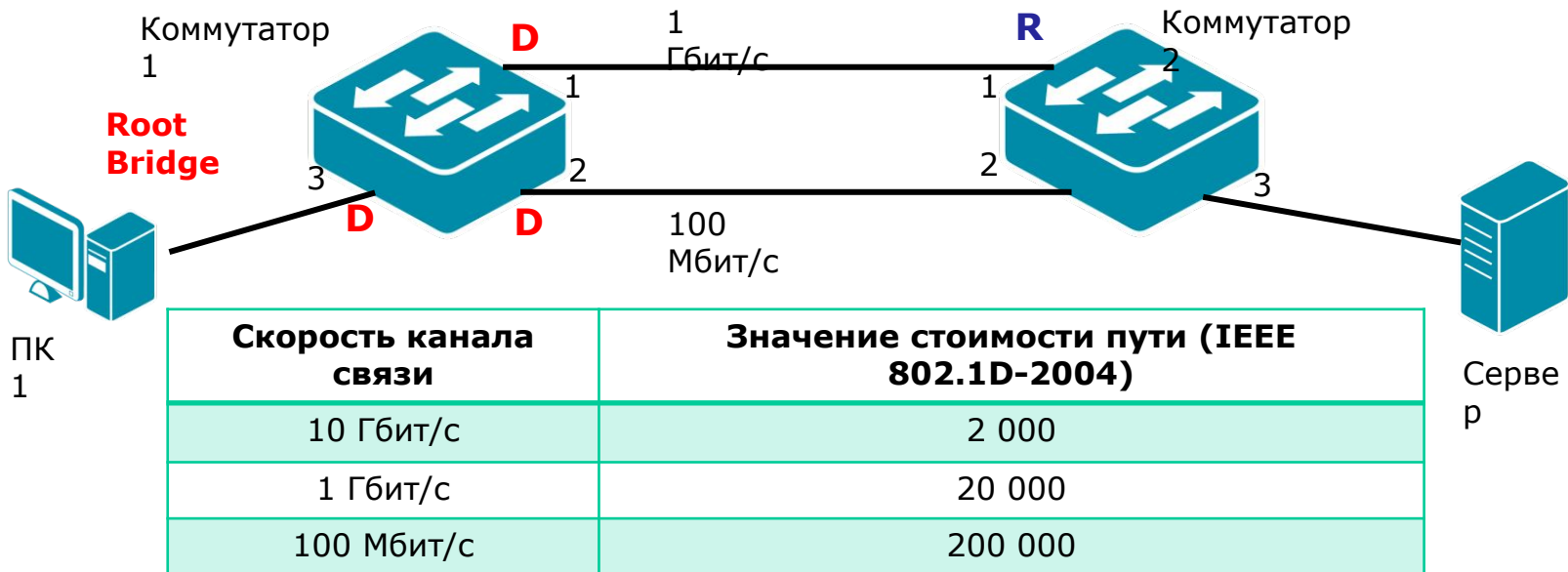
Идентификатор моста

Идентификатор моста	
Приоритет моста (по умолчанию: 32 768)	MAC-адрес
2 байта	6 байт

Правила выбора корневого моста

- ❑ Корневым мостом становится устройство с наименьшим значением идентификатора:
- ❑ Минимальное значение приоритета моста – 0, максимальное – 61 440, значение по умолчанию - 32 768.
 - ❑ сначала сравниваются приоритеты. Устройство с наименьшим значением приоритета становится корневым мостом;
 - ❑ если приоритеты равны, сравниваются MAC-адреса. Устройство с наименьшим MAC-адресом становится корневым мостом.

Протокол Spanning Tree (STP)

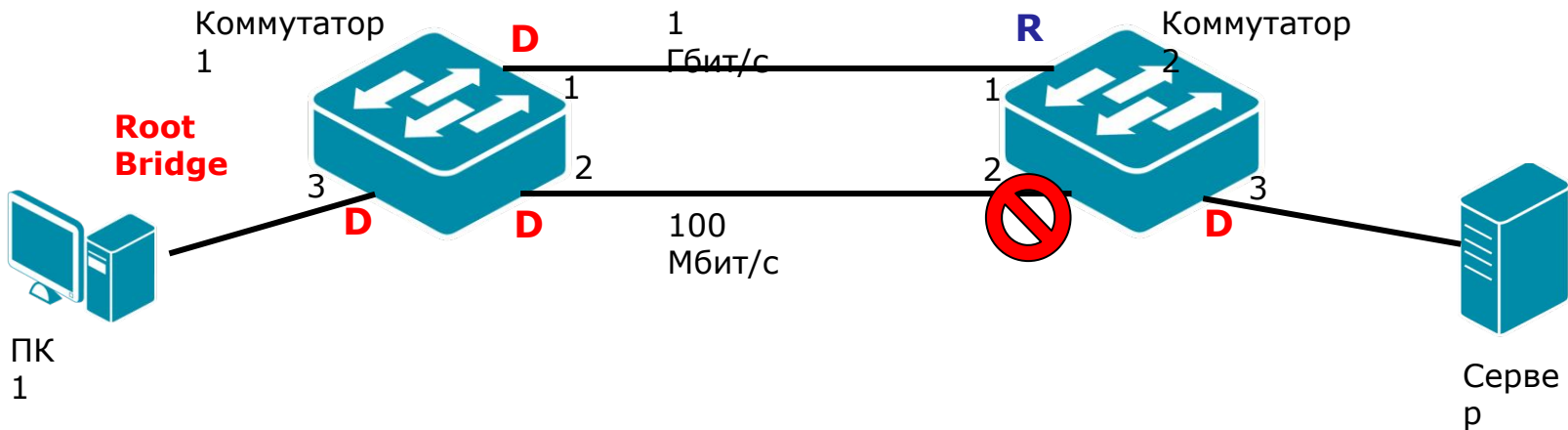


Все порты у корневого моста – **назначенные** (Designated)

Выбор корневых портов

- ☐ Когда процесс выбора корневого моста завершен, оставшиеся коммутаторы сети определяют единственный путь до корневого моста. Это выполняется путем выбора корневого порта на каждом некорневом мосте.
- ☐ Выборы корневого порта включают оценку расстояния до корневого моста (Root Path Cost). Оно рассчитывается как суммарное условное время на передачу данных по всем каналам связи, ведущим от порта данного коммутатора до порта корневого моста.
- ☐ Сравнив стоимости всех возможных маршрутов до корня, каждый коммутатор выбирает среди них один с наименьшим значением стоимости. В случае если минимальные стоимости пути нескольких маршрутов окажутся одинаковыми, корневым портом станет порт, имеющий наименьшее значение идентификатора порта.

Протокол Spanning Tree (STP)



После выбора корневых и назначенных портов все остальные порты коммутаторов сети блокируются.

Выбор назначенных портов

- ❑ Для каждого сегмента в коммутируемой сети выбирается один назначенный порт. Этот порт принимает кадры от сегмента и передает их в направлении корневого моста через корневой порт данного коммутатора.
- ❑ Назначенный порт сегмента определяется путем сравнения значений стоимости пути всех маршрутов от данного сегмента до корневого моста. Им становится порт, имеющий наименьшее значение стоимости, среди всех портов, подключенных к данному сегменту. Если минимальные значения стоимости пути окажутся одинаковыми у двух или нескольких портов, то для выбора назначенного порта сегмента STP принимает решение на основе последовательного сравнения идентификаторов мостов и идентификаторов портов.

Протокол Spanning Tree (STP)

Bridge Protocol Data Unit (BPDU)

- ❑ Вычисление структуры связующего дерева происходит при включении коммутатора и при изменении топологии. Эти вычисления требуют периодического обмена информацией между коммутаторами связующего дерева, что достигается при помощи специальных кадров, называемых блоками данных протокола моста – **BPDU** (Bridge Protocol Data Unit).
- ❑ Коммутатор отправляет BPDU, используя уникальный MAC-адрес порта в качестве адреса-отправителя и групповой MAC-адрес протокола STP 01-80-C2-00-00-00 в качестве адреса-получателя.
- ❑ **Существует три типа кадров BPDU:**
 - ❑ **Configuration BPDU** (CBPDU) – конфигурационный кадр BPDU, который используется для вычисления связующего дерева (тип сообщения: 0x00);
 - ❑ **Topology Change Notification** (TCN) **BPDU** – уведомление об изменении топологии сети (тип сообщения: 0x80);
 - ❑ **Topology Change Notification Acknowledgement** (TCA) – подтверждение о получении уведомления об изменении топологии сети.

Протокол Spanning Tree (STP)

Bridge Protocol Data Unit (BPDU)

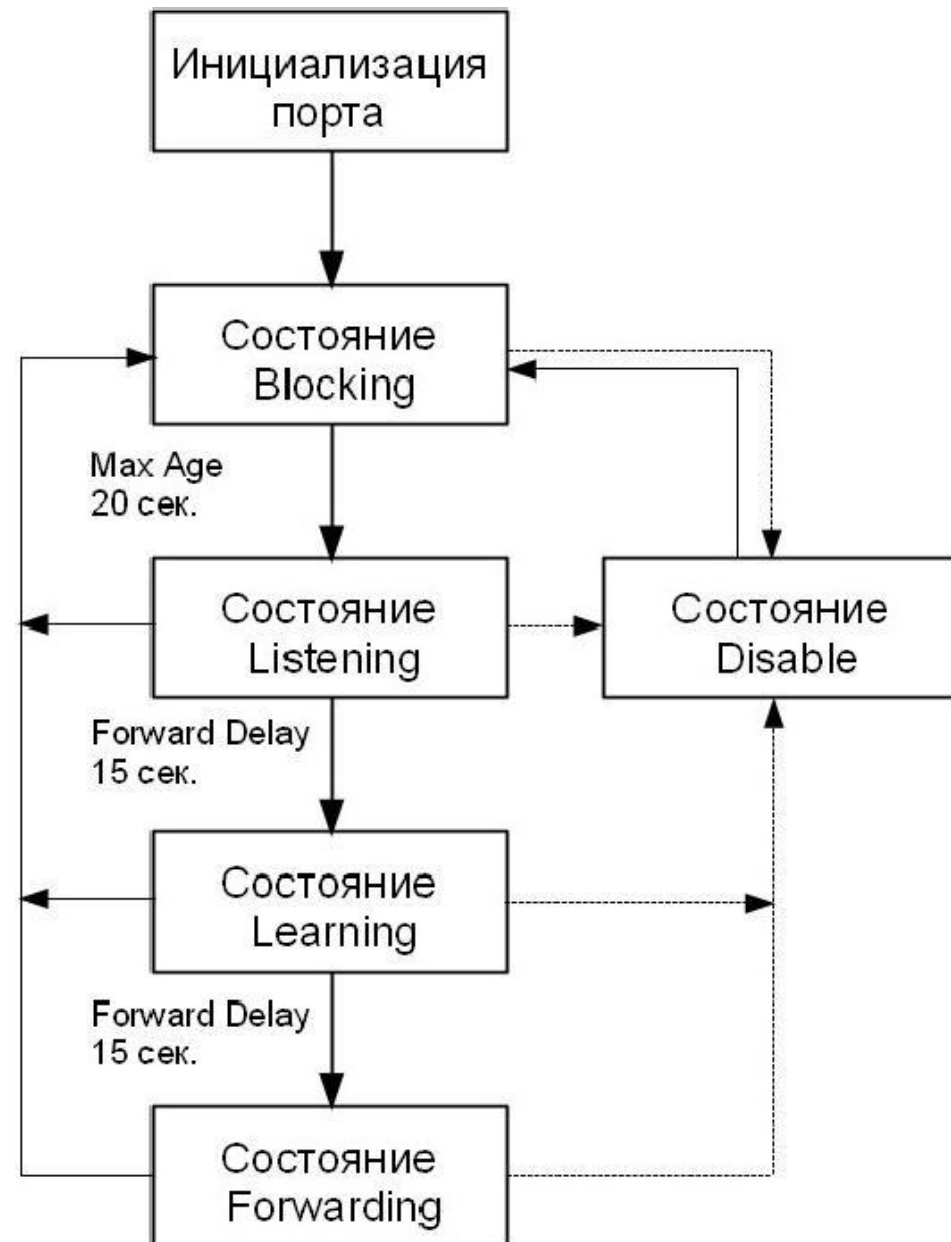
- ❑ Коммутаторы обмениваются BPDU через равные интервалы времени (по умолчанию 2 с), что позволяет им отслеживать состояние топологии сети.

	Байты
Идентификатор протокола (Protocol Identifier)	2
Версия протокола (Protocol Version Identifier)	1
Тип BPDU (BPDU Type)	1
Флаги (Flags)	1
Идентификатор корневого моста (Root Identifier)	8
Расстояние до корневого моста (Root Path Cost)	2
Идентификатор моста (Bridge Identifier)	8
Идентификатор порта (Port Identifier)	2
Время жизни сообщения (Message Age)	2
Максимальное время жизни сообщения (Max Age)	2
Время приветствия (Hello Time)	2
Задержка смены состояний (Forward Delay)	2

Протокол Spanning Tree (STP)

Состояния портов

- ❑ **Blocking** («Блокировка») – порт принимает и обрабатывает только кадры BPDU. Все остальные кадры отбрасываются.
- ❑ **Listening** («Прослушивание») – порт продолжает принимать, обрабатывать и ретранслировать только кадры BPDU.
- ❑ **Learning** («Обучение») – порт начинает принимать все кадры и на основе MAC-адресов источника строить таблицу коммутации. В этом состоянии порт все еще не передает кадры.
- ❑ **Forwarding** («Продвижение») – порт может обрабатывать кадры данных в соответствии с построенной таблицей коммутации, а также принимать, передавать и обрабатывать кадры BPDU.
- ❑ **Disable** («Отключен») – порт не участвует ни в работе протокола STP, ни в продвижении кадров данных.



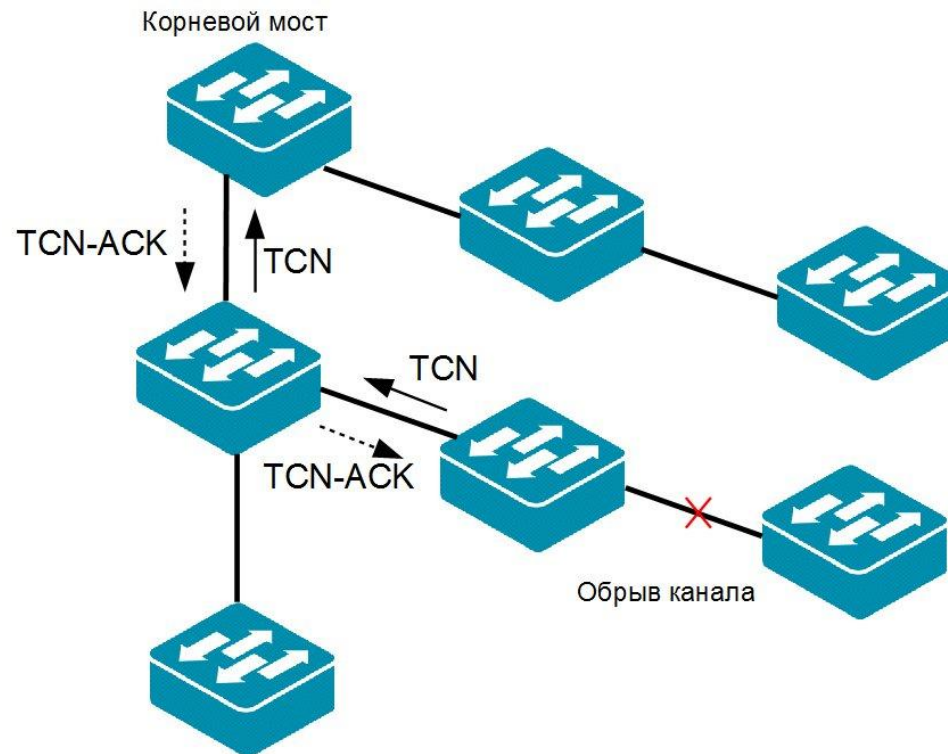
Таймеры STP

- ❑ **Hello Time** – интервал времени, через который корневой мост отправляет конфигурационные BPDU. Значение таймера Hello Time *по умолчанию 2 секунды*, диапазон возможных значений от 1 до 10 секунд.
- ❑ **Forward Delay** – интервал времени, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение». Значение таймера Forward Delay *по умолчанию 15 секунд*, диапазон возможных значений от 4 до 30 секунд.
- ❑ **Max Age** – это интервал времени, в течение которого коммутатор хранит параметры текущей конфигурации связующего дерева. Значение таймера Max Age устанавливается корневым мостом и позволяет гарантировать, что все коммутаторы сети обладают одинаковой информацией о времени хранения конфигурации STP. Значение таймера Max Age *по умолчанию 20 секунд*, диапазон возможных значений от 6 до 40 секунд.

Протокол Spanning Tree (STP)

Изменение топологии

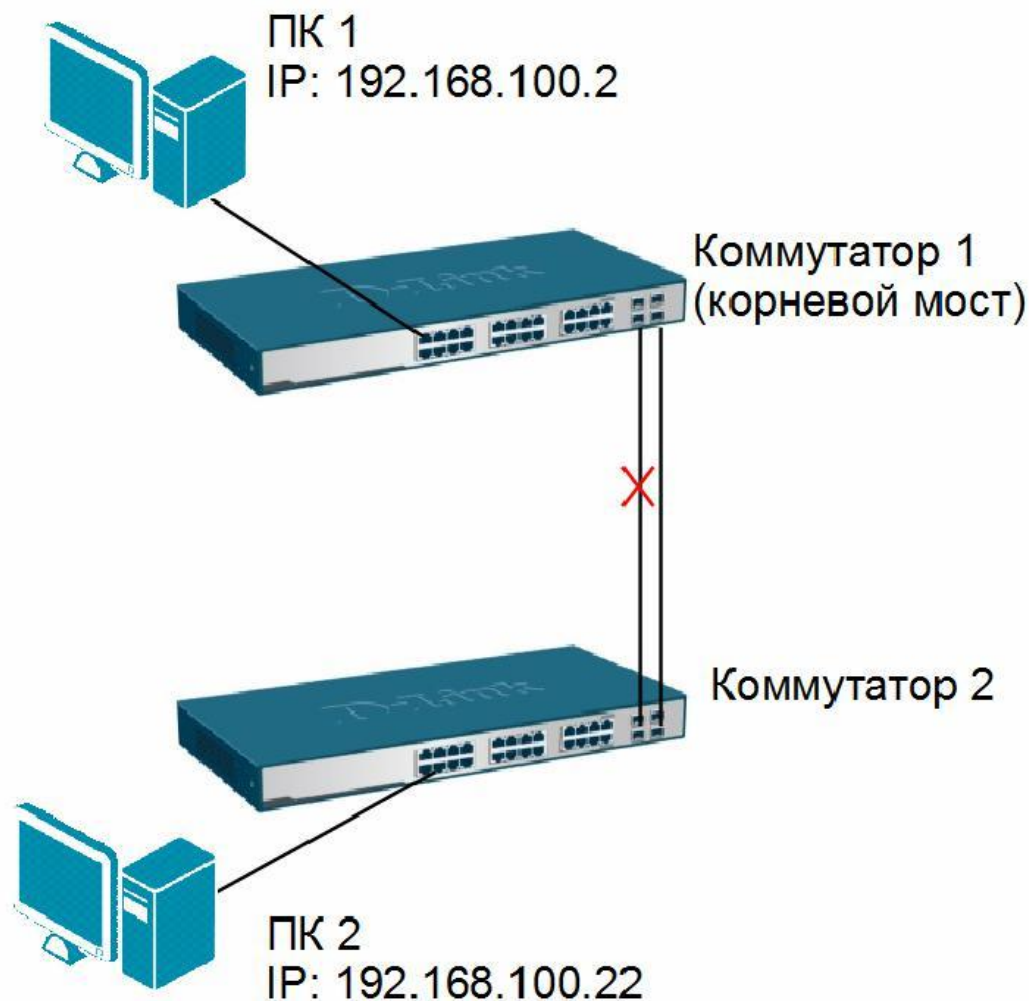
- ❑ Коммутатор отправляет BPDUs с уведомлением об изменении топологии (Topology Change Notification BPDUs, TCN BPDU) в случае возникновения одного из следующих событий:
 - ❑ некорневой мост получает сообщение TCN BPDU на свой назначенный порт;
 - ❑ после истечения времени, определенного таймером Forward Delay, порт переходит в состояние Forwarding, но коммутатор уже имеет назначенный порт для данного сегмента;
 - ❑ порт, находившийся в состоянии Forwarding или Listening, переходит в состояние Blocking (в случае проблем с каналом связи);
 - ❑ коммутатор становится корневым мостом.



Протокол Spanning Tree (STP)

Настройка STP

- ❑ Рассмотрим пример настройки протокола STP на коммутаторах D-Link серии DGS-1210-28/ME



Настройка STP

D-Link®
Building Networks for People

Smart
Anonymous - 10.90.90.92

Save Tools Wizard Help Logout

DGS-1210-28/ME

- System
- VLAN
- L2 Functions
 - Jumbo Frame
 - Port Mirroring
 - Loopback Detection
 - MAC Address Table
 - Spanning Tree
 - STP Bridge Global Settings**
 - STP Port Settings
 - MST Configuration Identification
 - STP Instance Settings
 - MSTP Port Information
 - Link Aggregation
 - Multicast
 - SNTP
 - LLDP
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

STP Bridge Global Settings Safeguard

STP State ☒ Enabled ☐ Disabled

STP Version	STP	Root Bridge	00:00:00:00:00:00:00:00
Bridge Priority	4096	Root Cost	0
Tx Hold Count (1-10)	3	Root Maximum Age	20
Maximum Age (6-40 secs)	20	Root Forward Delay	15
Hello Time (1-10 secs)	2	Root Port	0
Forward Delay (4-30 secs)	15		
Forwarding BPDU	Enabled		

Apply Refresh

Протокол Spanning Tree (STP)

Настройка STP

D-Link®
Building Networks for People

Anonymous - 10.90.90.92

Save Tools Wizard Help Logout

DGS-1210-28/ME

- System
- VLAN
- L2 Functions
 - Jumbo Frame
 - Port Mirroring
 - Loopback Detection
 - MAC Address Table
 - Spanning Tree
 - STP Bridge Global Settings**
 - STP Port Settings
 - MST Configuration Identification
 - STP Instance Settings
 - MSTP Port Information
 - Link Aggregation
 - Multicast
 - SNTP
 - LLDP
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

STP Bridge Global Settings Safeguard

STP State ☒ Enabled ☐ Disabled

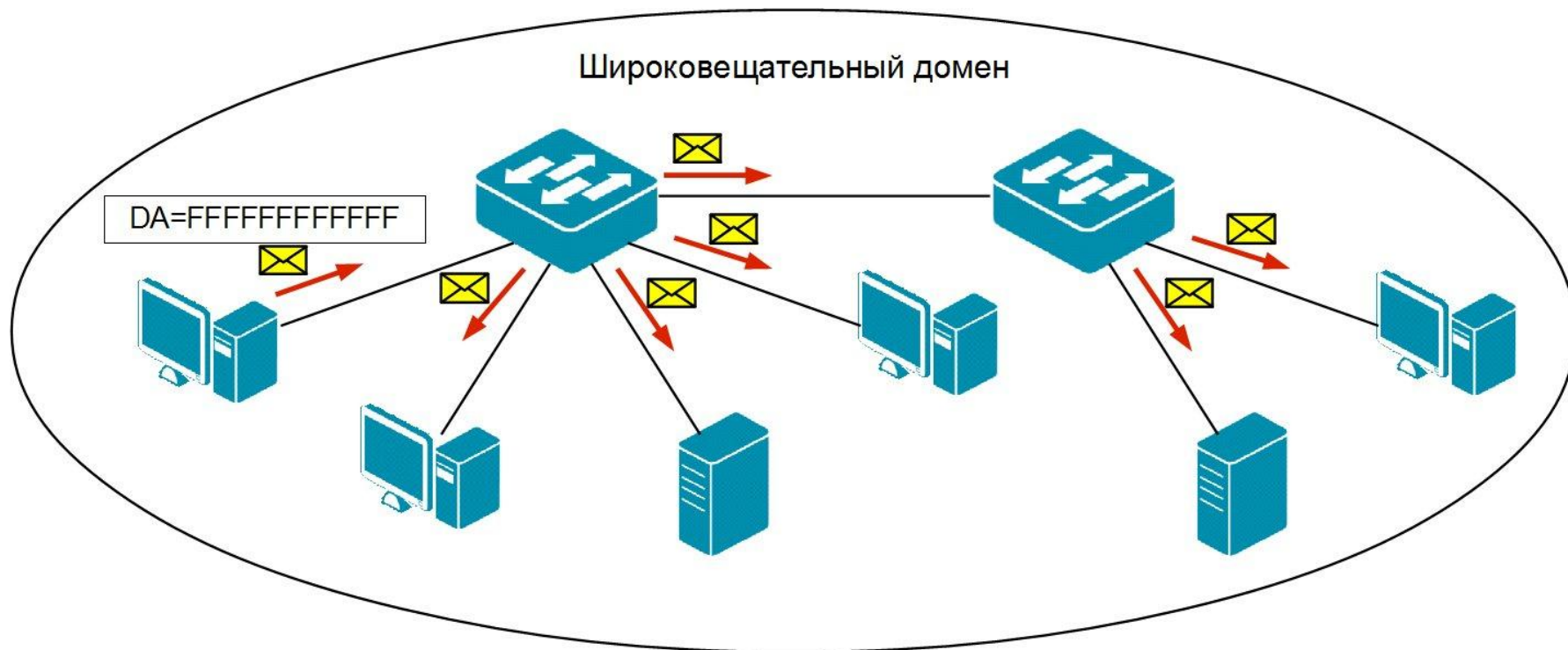
STP Version	STP	Root Bridge	00:00:00:00:00:00:00
Bridge Priority	32768	Root Cost	0
Tx Hold Count (1-10)	3	Root Maximum Age	20
Maximum Age (6-40 secs)	20	Root Forward Delay	15
Hello Time (1-10 secs)	2	Root Port	0
Forward Delay (4-30 secs)	15		
Forwarding BPDU	Enabled		

Apply Refresh

Виртуальные локальные сети (VLAN)

Понятие виртуальной локальной сети

- ❑ Широковещательный домен
 - ❑ Логический сегмент сети.
 - ❑ Любое устройство может передавать данные всем устройствам в сегменте.
 - ❑ Для отправки кадров всем устройствам, используются широковещательные адреса.



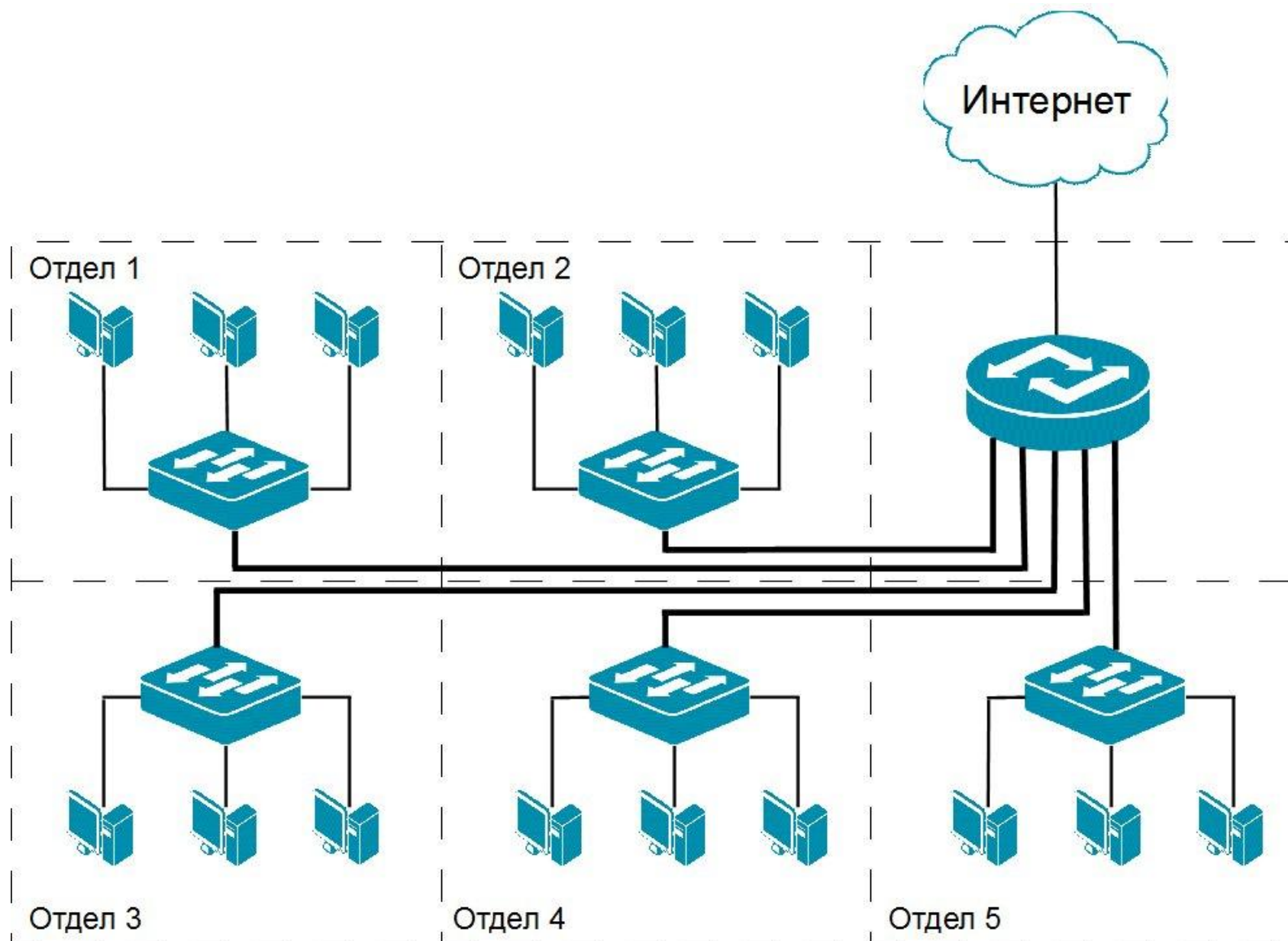
Виртуальная локальная сеть

- ❑ Логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне .

- ❑ **VLAN обладают следующими преимуществами:**
 - ❑ гибкость внедрения – VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы независимо от их физического размещения в сети;
 - ❑ ограничивают распространение широковещательного трафика, что увеличивает полосу пропускания, доступную для пользователя;
 - ❑ позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

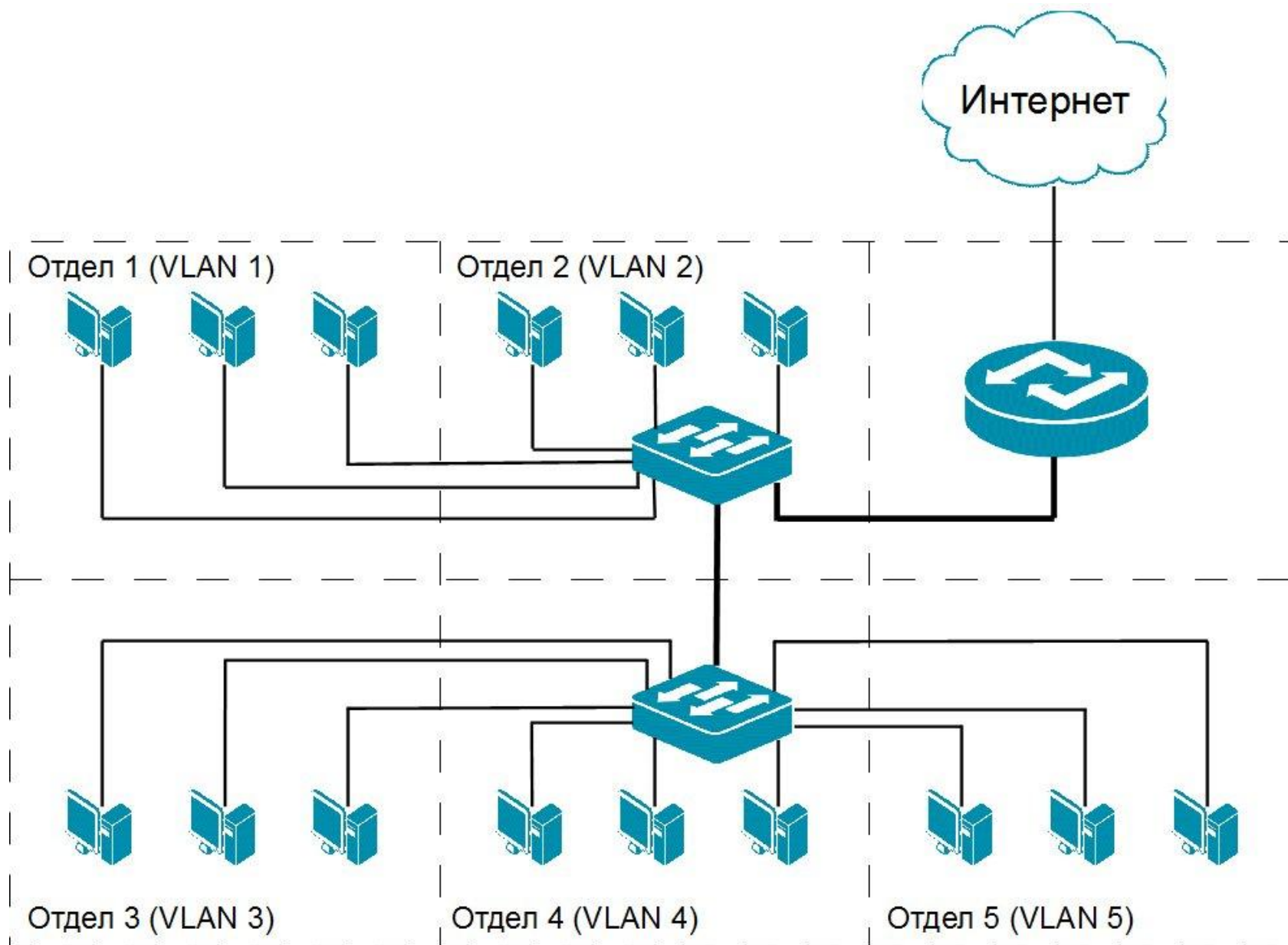
Виртуальные локальные сети (VLAN)

Физическая сегментация сети



Виртуальные локальные сети (VLAN)

Логическая сегментация сети



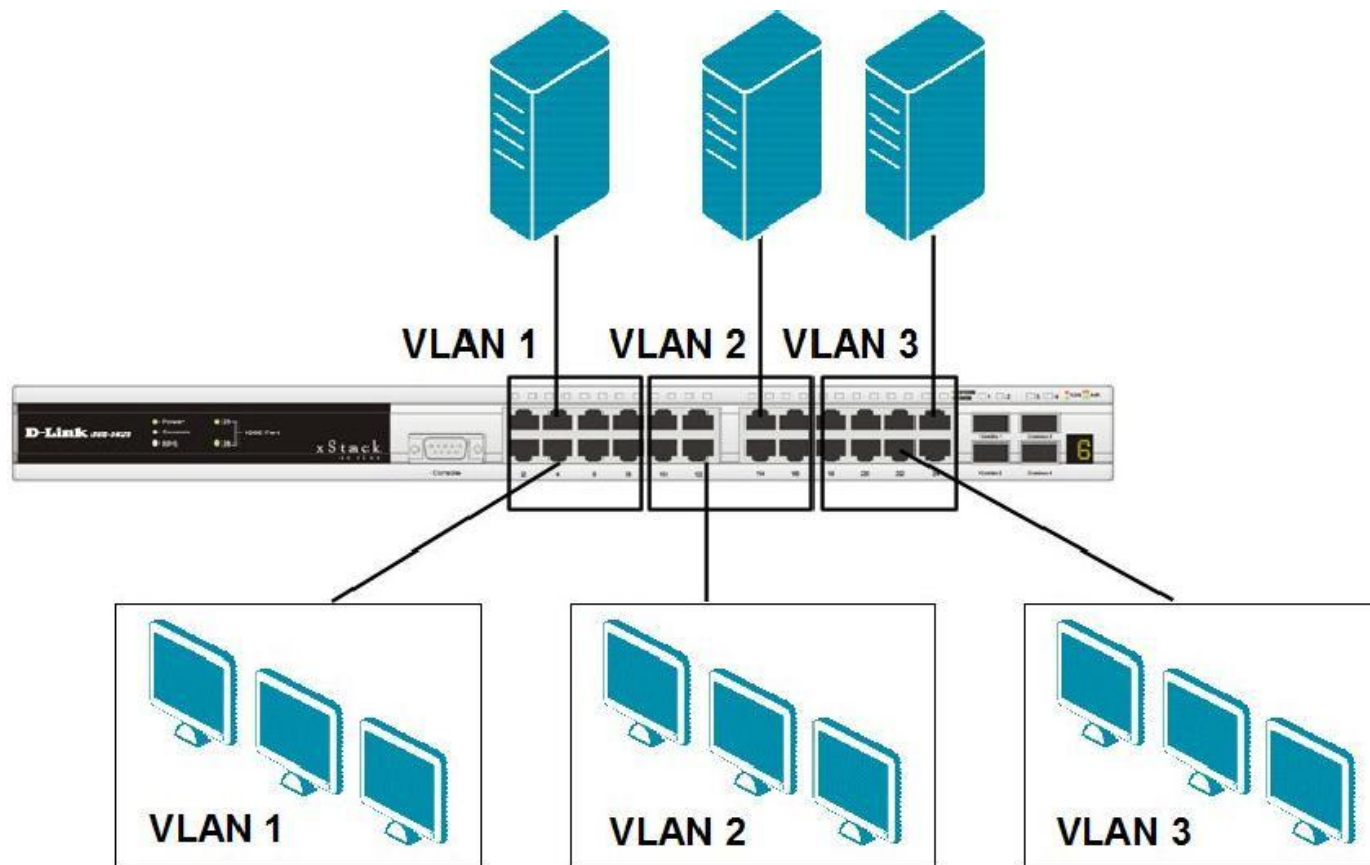
Типы VLAN

- ❑ В коммутаторах могут быть реализованы следующие типы VLAN:
 - ❑ на основе портов;
 - ❑ на основе стандарта IEEE 802.1Q;
 - ❑ на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
 - ❑ на основе портов и протоколов IEEE 802.1v;
 - ❑ на основе MAC-адресов;
 - ❑ асимметричные.

- ❑ Также для сегментации сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например *Traffic Segmentation*.

VLAN на основе портов (Port-based VLAN)

- ❑ При использовании VLAN на основе портов (Port-based VLAN), каждый порт назначается в определенную VLAN, независимо от того, какой компьютер подключен к этому порту.
- ❑ Конфигурация портов – статическая и может быть изменена только вручную.



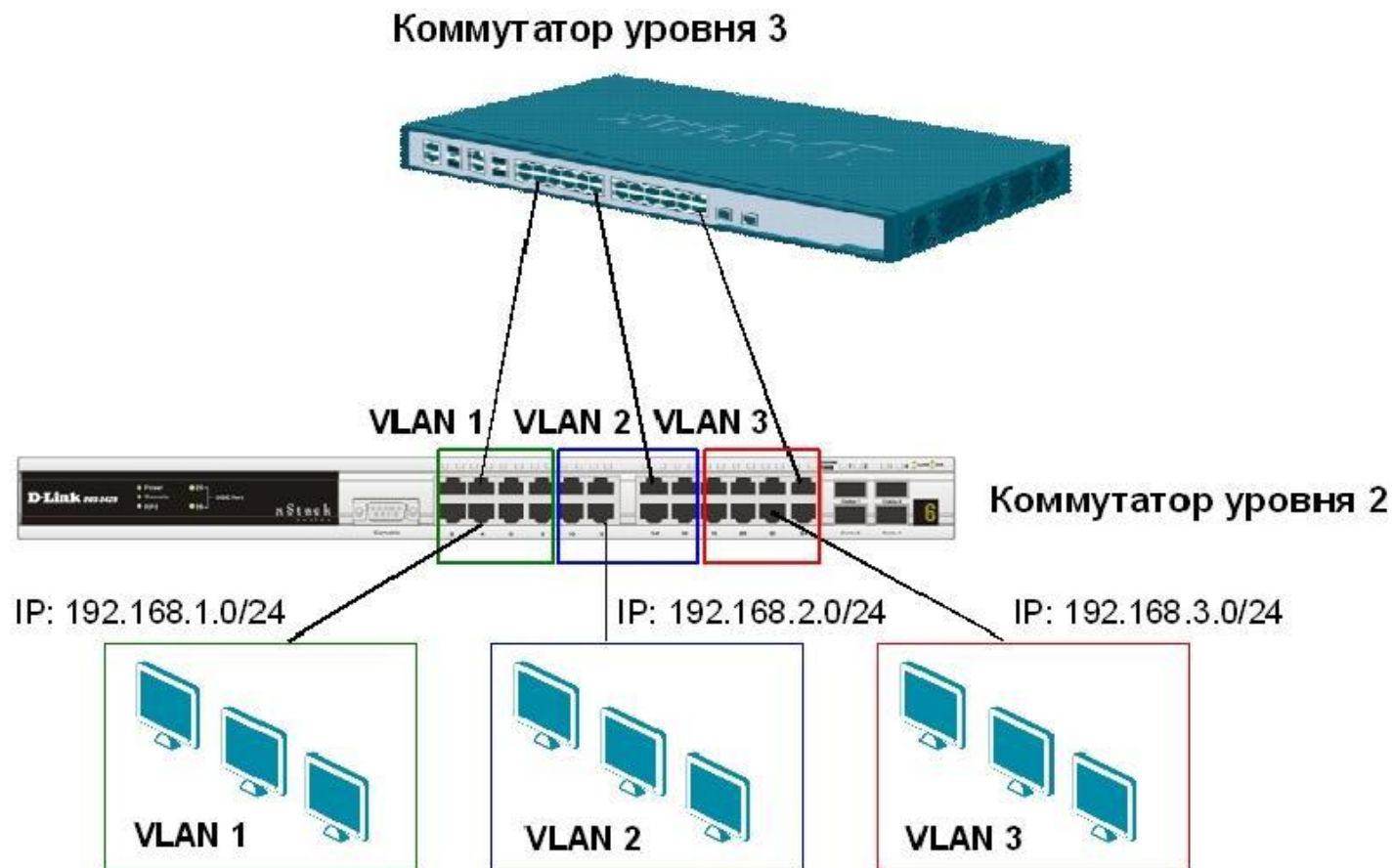
VLAN на основе портов (Port-based VLAN)

- ❑ Основные характеристики VLAN на основе портов.
 - ❑ применяются в пределах одного коммутатора;
 - ❑ простота настройки;
 - ❑ возможность изменения логической сегментации сети без физического перемещения станций;
 - ❑ каждый порт может входить только в одну VLAN.

Виртуальные локальные сети (VLAN)

VLAN на основе портов (Port-based VLAN)

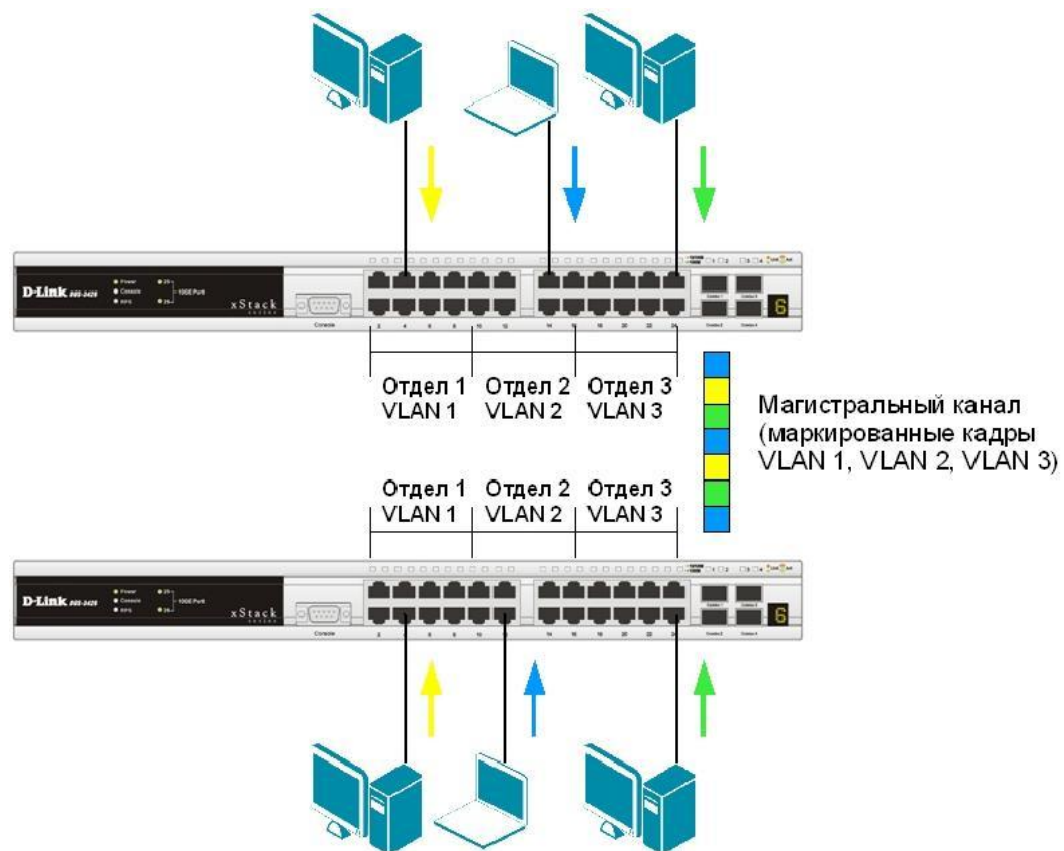
- Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень модели OSI.



Виртуальные локальные сети (VLAN)

VLAN на основе стандарта IEEE 802.1Q

- ❑ Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра для хранения информации о принадлежности к VLAN при его перемещении по сети.
- ❑ Можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и между несколькими коммутаторами с поддержкой стандарта IEEE 802.1Q.
- ❑ Кадры разных VLAN могут распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (магистральному каналу, Trunk Link).



Некоторые определения IEEE 802.1Q

- ❑ **Tagging (Маркировка кадра)** – процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра Ethernet.
- ❑ **Untagging (Извлечение тега из кадра)** – процесс извлечения информации о принадлежности к 802.1Q VLAN из заголовка кадра Ethernet.
- ❑ **VLAN ID (VID)** – идентификатор VLAN.
- ❑ **Port VLAN ID (PVID)** – идентификатор порта VLAN.
- ❑ **Ingress port (Входной порт)** – порт коммутатора, на который поступают кадры, и при этом принимается решение о принадлежности к VLAN.
- ❑ **Egress port (Выходной порт)** – порт коммутатора, с которого кадры передаются на другие сетевые устройства – коммутаторы или рабочие станции, и при этом принимается решение о маркировке.

Виртуальные локальные сети (VLAN)

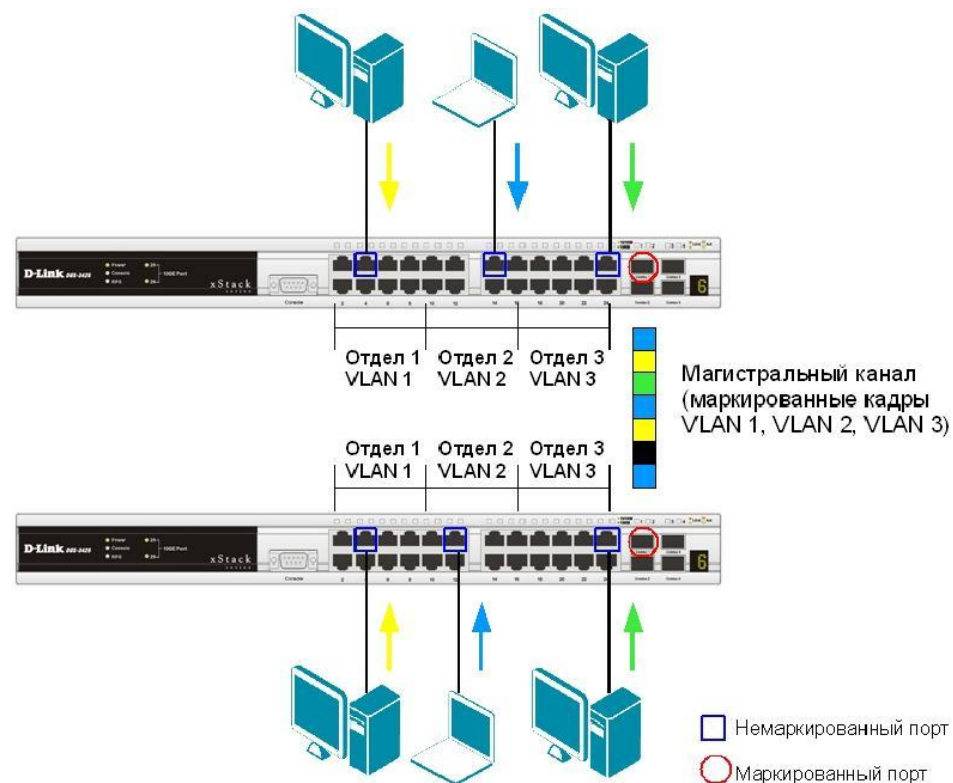
Маркированные и не маркированные порты

❑ Tagged (маркированный) порт:

- ❑ сохраняет тег 802.1Q в заголовках всех выходящих через него маркированных кадров и добавляет тег в заголовки всех выходящих через него не маркированных кадров.

❑ Untagged (не маркированный) порт:

- ❑ извлекает тег 802.1Q из заголовков всех выходящих через него маркированных кадров;
- ❑ обычно используется для подключения конечных устройств.



Тег VLAN IEEE 802.1Q

- ❑ К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт.

VID (VLAN ID) – 12-ти битный идентификатор VLAN определяет, какой VLAN принадлежит трафик.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Длина/тип (Length/Type)	Данные (Data)	Контрольная сумма кадра (CRC)
--------------------------	-------------------------	----------------------------	------------------	----------------------------------

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Длина/тип (Length/Type)	Данные (Data)	Контрольная сумма кадра (CRC)
Идентификатор протокола тега (TPID) 0x8100 Приоритет (Priority) Индикатор канонического формата (CFI) Идентификатор VLAN (VID)					
16 бит		3 бита	1 бит	12 бит	

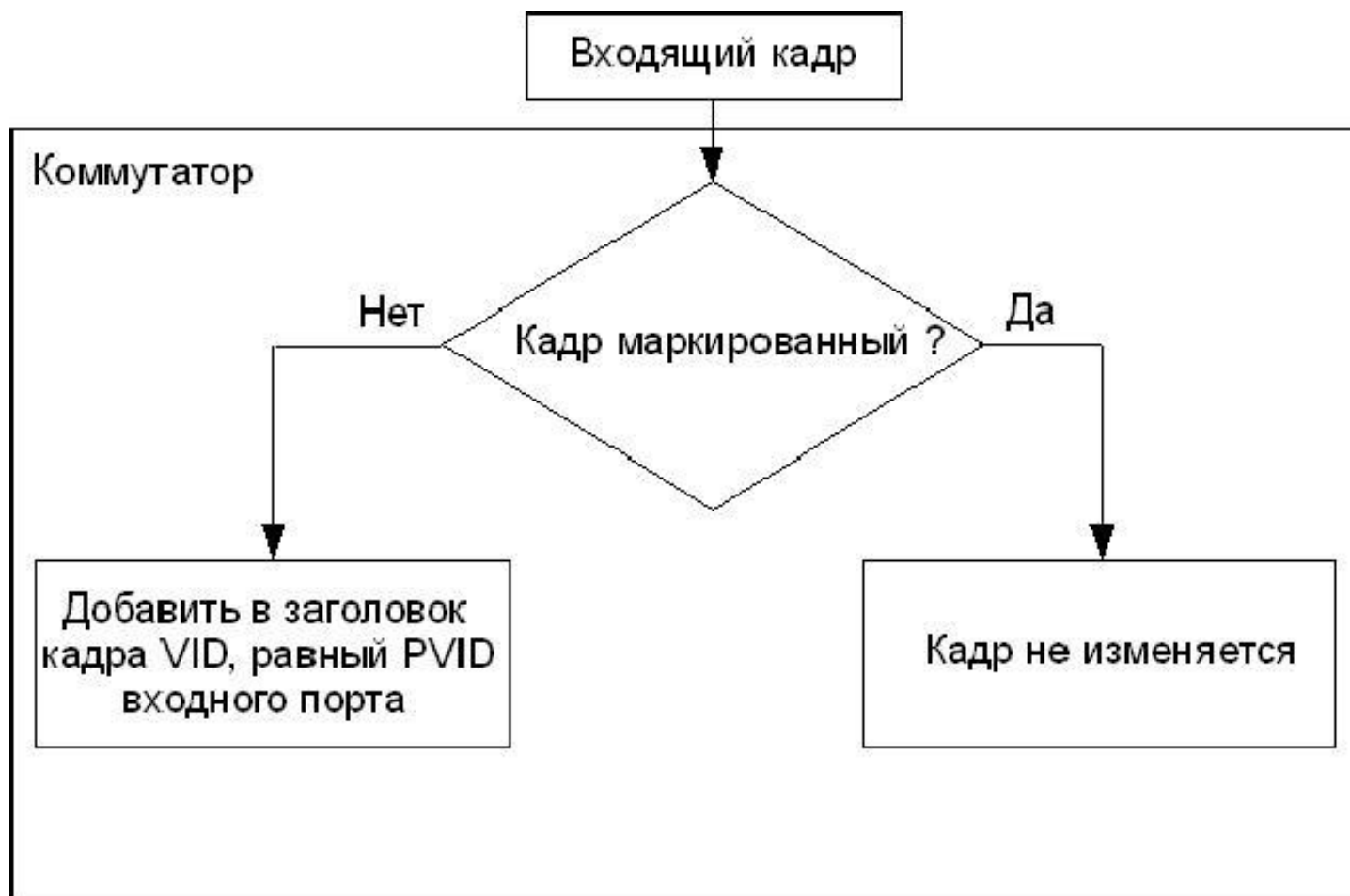
Port VLAN ID

- ❑ Каждый физический порт коммутатора имеет параметр, называемый **идентификатор порта VLAN (PVID)**.
- ❑ Идентификатор PVID определяет, в какую VLAN коммутатор направит немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт.
- ❑ Всем немаркированным кадрам присваивается идентификатор равный PVID порта, на который они были приняты.
- ❑ Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

Продвижение кадров VLAN IEEE 802.1Q

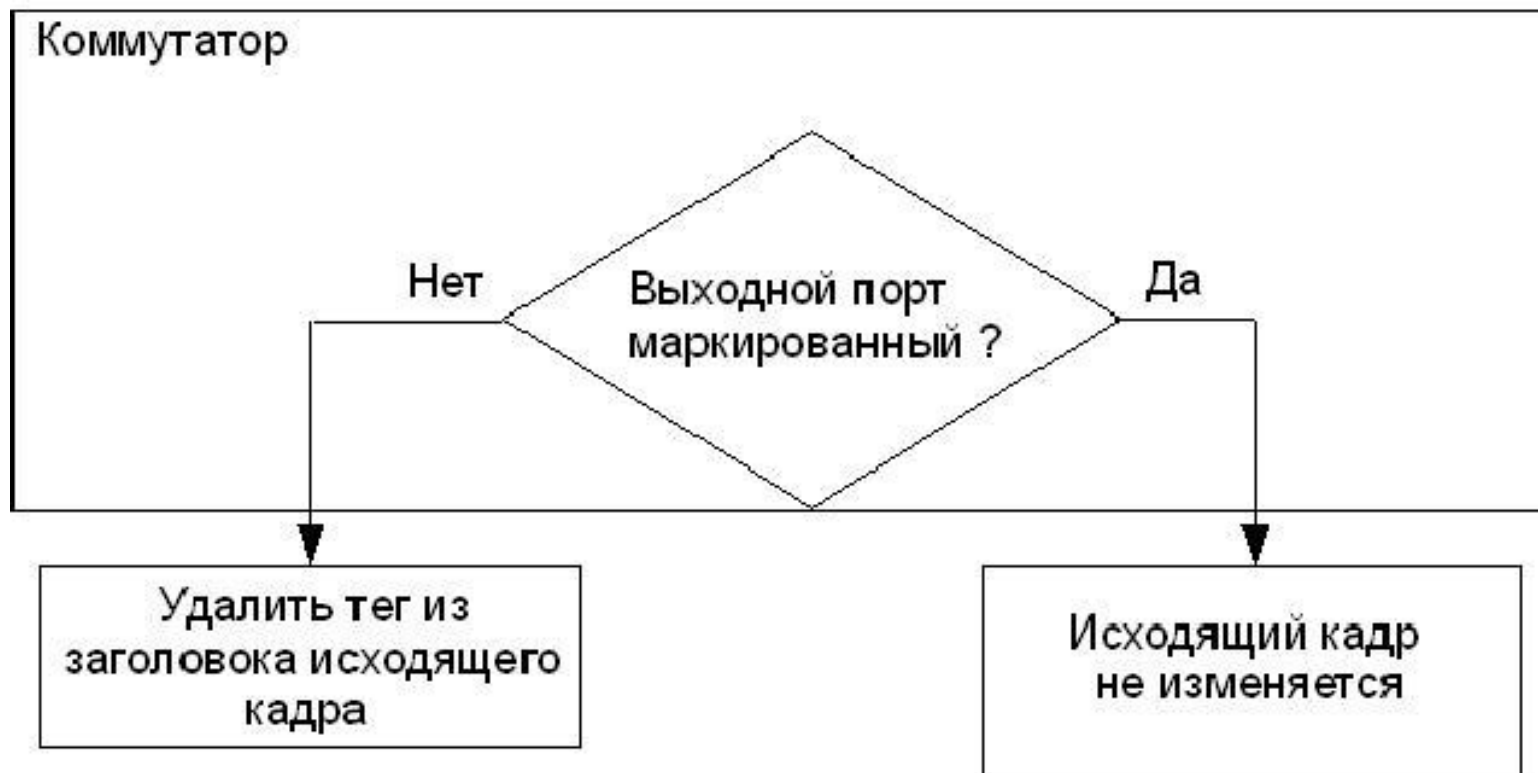
- Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих правил:
 - **правила входящего трафика** (ingress rules) – классификация получаемых кадров относительно принадлежности к VLAN;
 - **правила продвижения между портами** (forwarding rules) – принятие решения о продвижении или отбрасывании кадра;
 - **правила исходящего трафика** (egress rules) – принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

Правила входящего трафика



Виртуальные локальные сети (VLAN)

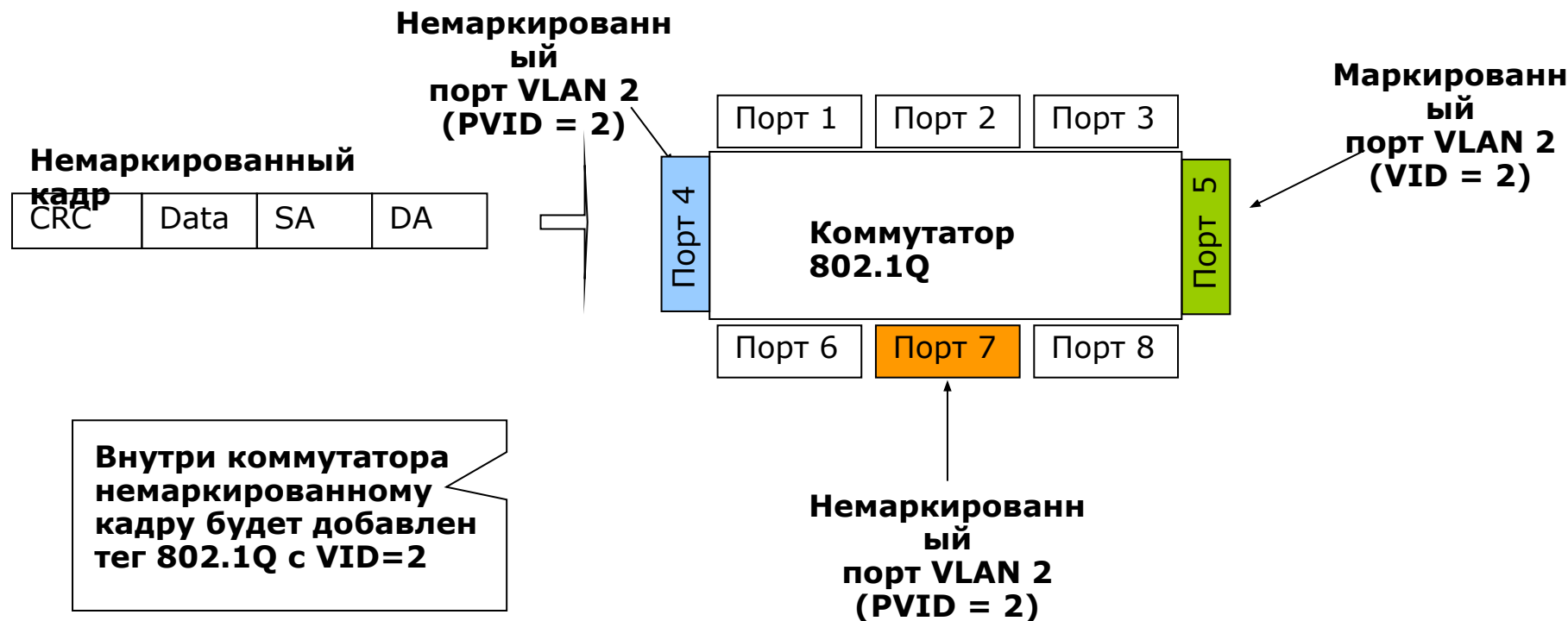
Правила исходящего трафика



Виртуальные локальные сети (VLAN)

Входящий немаркированный кадр

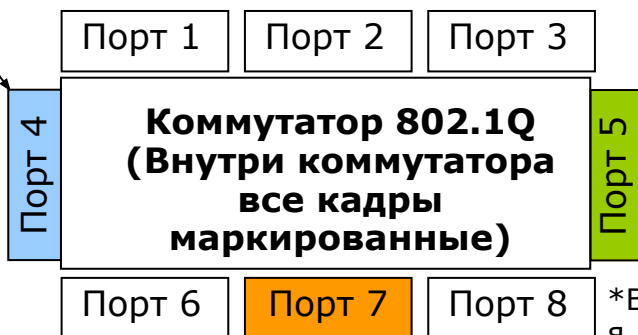
- ❑ Предположим, что PVID порта 4 равен 2.
- ❑ Входящему немаркированному кадру будет добавлен тег с VID равным PVID порта 4.
- ❑ Порт 5 – маркированный порт VLAN 2.
- ❑ Порт 7 – немаркированный порт VLAN 2.
- ❑ Полученный кадр передается через порты 5 и 7.



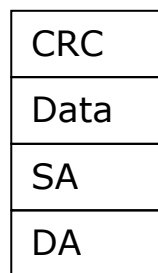
Виртуальные локальные сети (VLAN)

Передача немаркированного кадра через маркированный и немаркированный порты

Немаркированный порт VLAN 2 (PVID = 2)



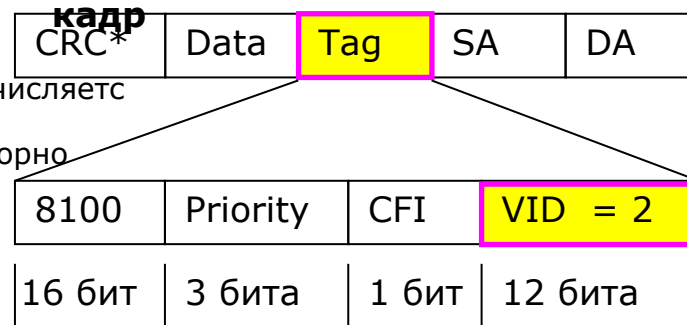
Немаркированный порт VLAN 2 (PVID = 2)



При выходе через немаркированный порт из кадра будет удален тег 802.1Q

Маркированный порт VLAN 2 (VID = 2)

Маркированный кадр



*Вычисляется повторно

VID связан с PVID входного порта

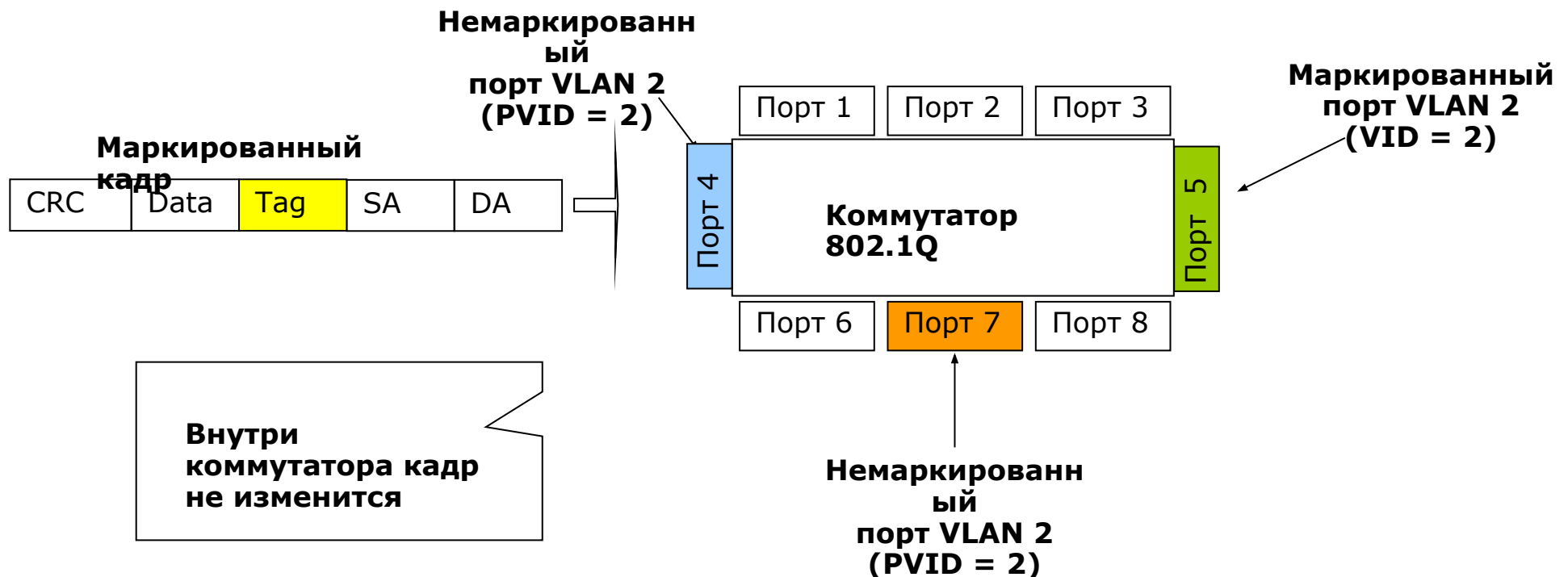
При выходе через маркированный порт в кадре будет сохранен тег 802.1Q

Поля
Priority – пользовательский приоритет (802.1p)
CFI – индикатор канонического формата
VID – идентификатор VLAN

Виртуальные локальные сети (VLAN)

Входящий маркированный кадр

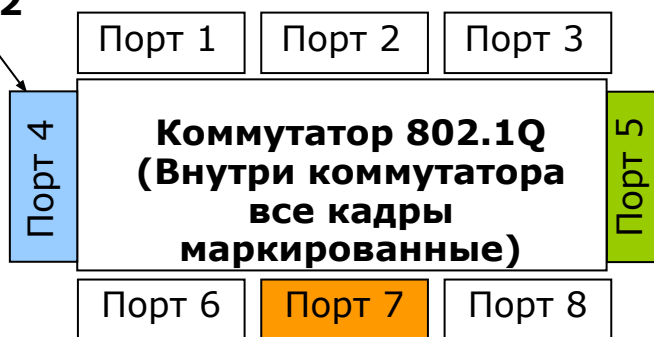
- ❑ Предположим, что входящий кадр маркированный с VID равным 2.
- ❑ Порт 5 – маркированный порт VLAN 2.
- ❑ Порт 7 – немаркированный порт VLAN 2.
- ❑ Полученный кадр передается через порты 5 и 7.



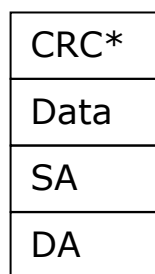
Виртуальные локальные сети (VLAN)

Передача маркированного кадра через маркированный и немаркированный порты

Немаркированный
порт VLAN 2
(PVID = 2)



Немаркированный
порт VLAN 2
(PVID = 2)

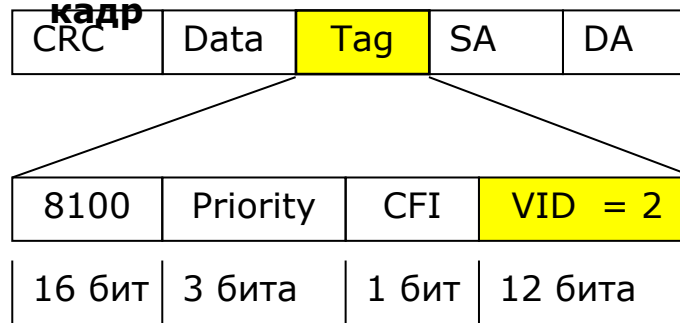


*Вычисляется повторно

При выходе через немаркированный порт из кадра будет удален тег 802.1Q

Маркированный
порт VLAN 2
(VID = 2)

Маркированный кадр



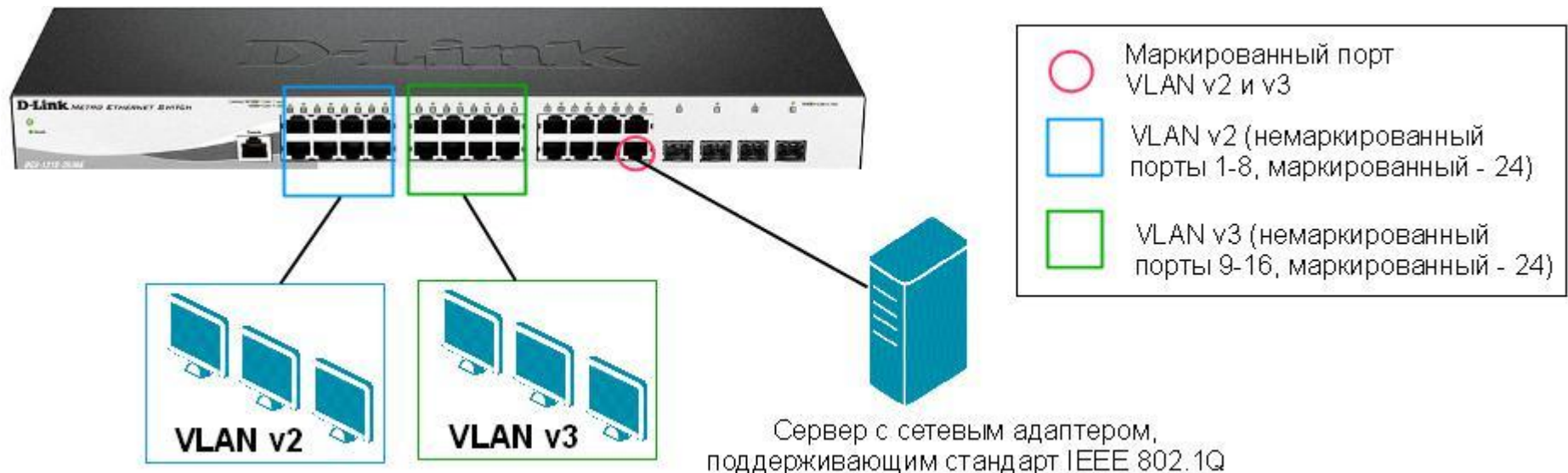
При выходе через маркированный порт в кадре будет сохранен тег 802.1Q

VID связан с PVID входного порта

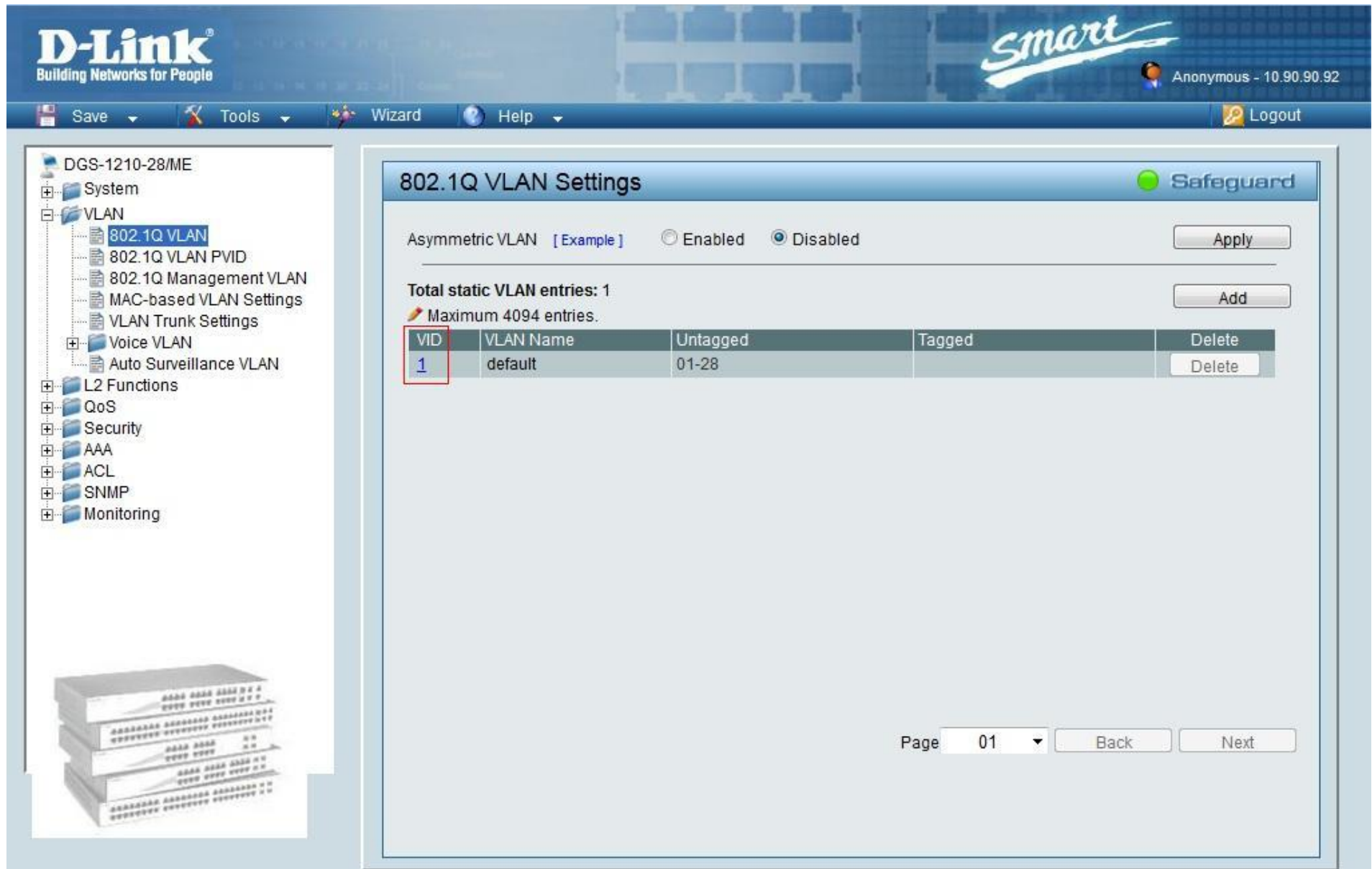
Поля
Priority – пользовательский приоритет (802.1p)
CFI – индикатор канонического формата
VID – идентификатор VLAN

Пример настройки VLAN IEEE 802.1Q

- Предположим, что в небольшом офисе, в котором имеется два отдела, необходимо изолировать трафик сотрудников разных отделов друг от друга, но в то же время обеспечить совместный доступ всех пользователей к серверу. Для этих целей можно использовать коммутатор с поддержкой стандарта IEEE 802.1Q и создать на нем две группы VLAN (VLAN v2 – для первого отдела, VLAN v3 – для второго отдела).



Пример настройки VLAN IEEE 802.1Q



D-Link® Building Networks for People

Anonymous - 10.90.90.92

Save Tools Wizard Help

DGS-1210-28/ME

- System
- VLAN
 - 802.1Q VLAN**
 - 802.1Q VLAN PVID
 - 802.1Q Management VLAN
 - MAC-based VLAN Settings
 - VLAN Trunk Settings
- Voice VLAN
- Auto Surveillance VLAN
- L2 Functions
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

802.1Q VLAN Settings Safeguard

Asymmetric VLAN [Example] ☐ Enabled ☒ Disabled Apply

Total static VLAN entries: 1 Add

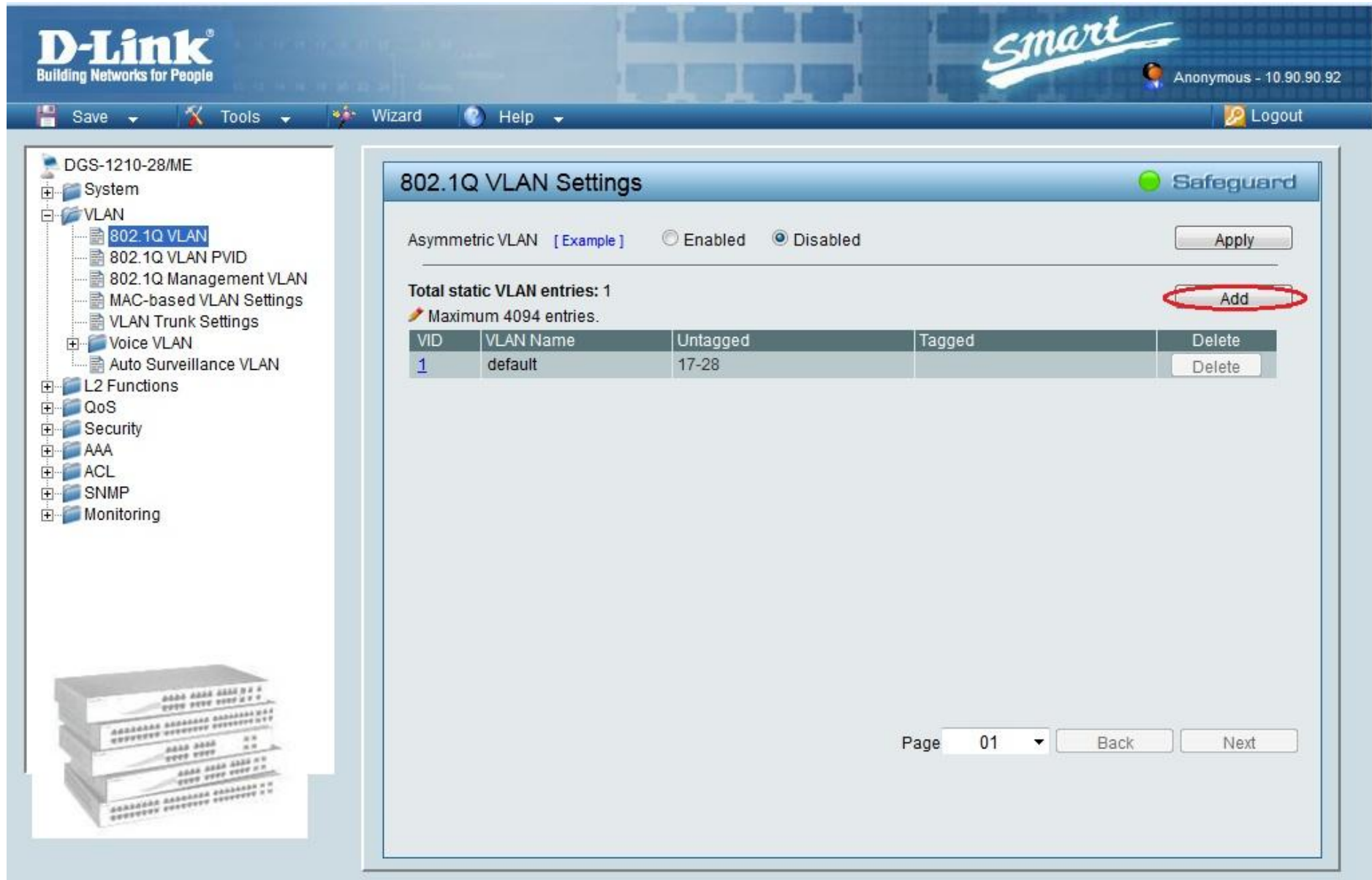
Maximum 4094 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-28		Delete

Page 01 Back Next

[illegible]

Пример настройки VLAN IEEE 802.1Q



D-Link®
Building Networks for People

Smart

Anonymous - 10.90.90.92

Save Tools Wizard Help Logout

DGS-1210-28/ME

- System
- VLAN
 - 802.1Q VLAN**
 - 802.1Q VLAN PVID
 - 802.1Q Management VLAN
 - MAC-based VLAN Settings
 - VLAN Trunk Settings
 - Voice VLAN
 - Auto Surveillance VLAN
- L2 Functions
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

802.1Q VLAN Settings ● Safeguard

Asymmetric VLAN [\[Example \]](#) ☐ Enabled ☒ Disabled Apply

Total static VLAN entries: 1 Add

Maximum 4094 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	17-28		Delete

Page 01 Back Next

Пример настройки VLAN IEEE 802.1Q


Building Networks for People


Anonymous - 10.90.90.92

Save
Tools
Wizard
Help
Logout

DGS-1210-28/ME

System

VLAN

802.1Q VLAN

802.1Q VLAN PVID

802.1Q Management VLAN

MAC-based VLAN Settings

VLAN Trunk Settings

Voice VLAN

Auto Surveillance VLAN

L2 Functions

QoS

Security

AAA

ACL

SNMP

Monitoring



VID Settings

Safeguard

VID

2

VLAN Name

v2

Back

Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	☒	☒	☒	☒	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒

Пример настройки VLAN IEEE 802.1Q

D-Link® Building Networks for People

Smart

Anonymous - 10.90.90.92

Save Tools Wizard Help Logout

DGS-1210-28/ME

- System
- VLAN
 - 802.1Q VLAN**
 - 802.1Q VLAN PVID
 - 802.1Q Management VLAN
 - MAC-based VLAN Settings
 - VLAN Trunk Settings
- Voice VLAN
- Auto Surveillance VLAN
- L2 Functions
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

VID Settings Safeguard

VID: 3

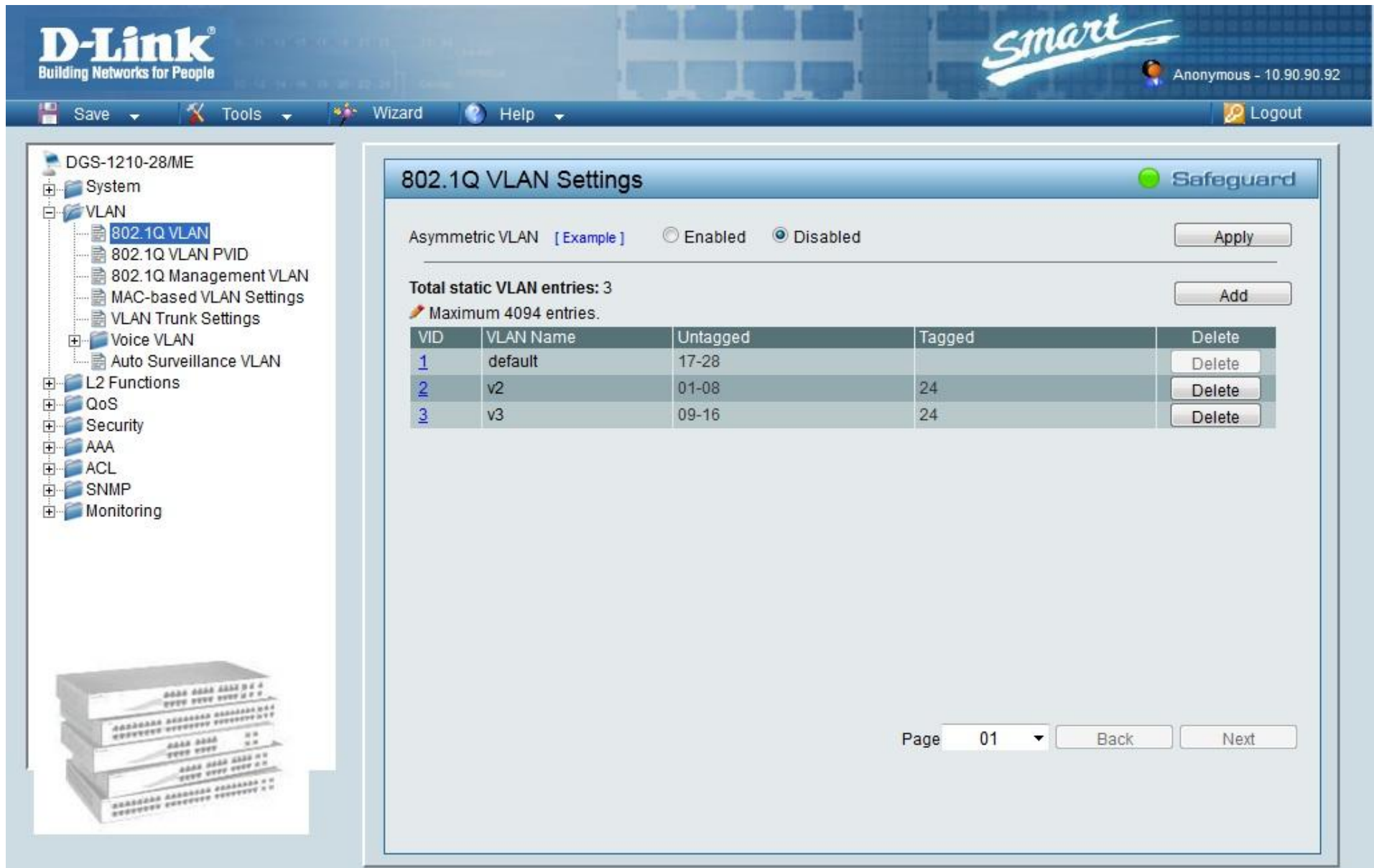
VLAN Name: v3

Back Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐
Not Member	All	☐	☐	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒

Пример настройки VLAN IEEE 802.1Q



D-Link® Building Networks for People

Anonymous - 10.90.90.92

Save Tools Wizard Help Logout

DGS-1210-28/ME

- System
- VLAN
 - 802.1Q VLAN**
 - 802.1Q VLAN PVID
 - 802.1Q Management VLAN
 - MAC-based VLAN Settings
 - VLAN Trunk Settings
 - Voice VLAN
 - Auto Surveillance VLAN
- L2 Functions
- QoS
- Security
- AAA
- ACL
- SNMP
- Monitoring

802.1Q VLAN Settings Safeguard

Asymmetric VLAN [Example] ☐ Enabled ☒ Disabled

Total static VLAN entries: 3
 Maximum 4094 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	17-28		Delete
2	v2	01-08	24	Delete
3	v3	09-16	24	Delete

Page 01

- ❑ **Power over Ethernet (PoE)** — эта технология позволяет передавать удаленному (оконечному) устройству вместе с данными электрическую энергию через кабель на основе стандартной витой пары в сети Ethernet.
- ❑ **Достоинства:**
 - ❑ электропитание удаленного сетевого устройства и обмен данными с ним осуществляется по одному сетевому кабелю;
 - ❑ низкие затраты на установку систем, их модернизацию и сервисное обслуживание;
 - ❑ повышенная эксплуатационная безопасность: обеспечивается защита от короткого замыкания, падения напряжения, превышения потребляемого тока и т.п.;
 - ❑ простота развертывания сети, особенно в сложных пространственных условиях (крыши, заборы, внутренние помещения в аэропортах и вокзалах, кафе, кинотеатры и т.п.) и простота перемещения PoE-совместимых оконечных устройств;
 - ❑ возможность управления параметрами питания удаленных устройств, т.к. оборудование с поддержкой PoE часто является управляемым, что упрощает администрирование сети.

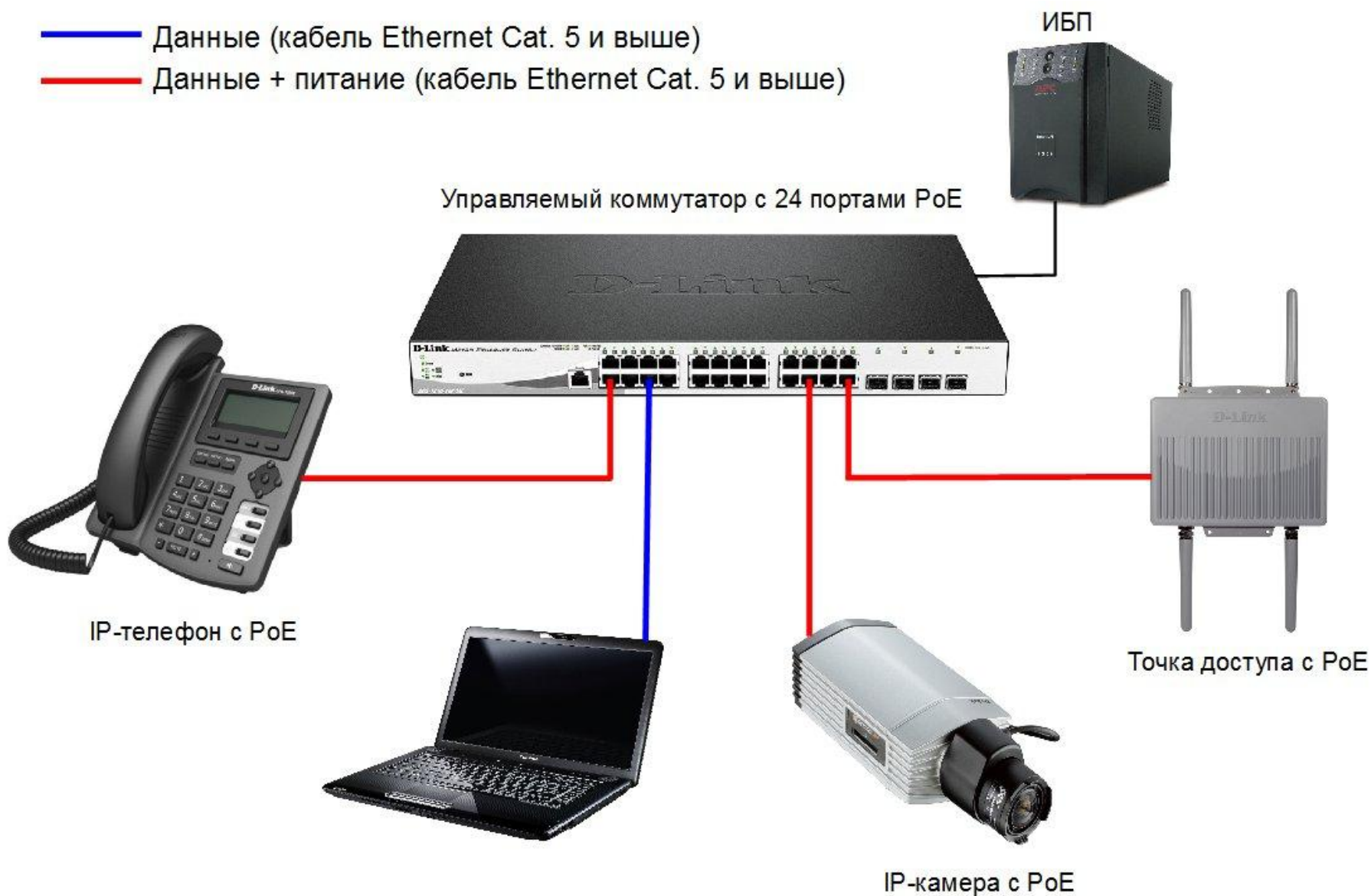
- ❑ Технология PoE является расширением стандарта IEEE 802.3.
- ❑ Первая версия технологии была описана в стандарте IEEE 802.3af-2003, которая в 2005 году вошла в 33 раздел стандарта IEEE 802.3-2005.
- ❑ В 2009 году появилась новая расширенная версия технологии PoE, описанная в стандарте IEEE 802.3at-2009, также известном как PoE+ или PoE plus.
- ❑ В настоящее время требования к PoE-системам определяются разделом 33 стандарта IEEE 802.3-2012 (в него полностью включен стандарт IEEE 802.3at-2009).
- ❑ Технология PoE предназначена для использования в устройствах с интерфейсами 10BASE-T, 100BASE-TX и 1000BASE-T.

- ❑ Спецификация PoE описывает работу двух типов устройств:
 - ❑ **питающие устройства** (Power Sourcing Equipment, PSE) выполняют функции источников питания и предназначены для подачи электропитания в сеть Ethernet, к которой подключены питаемые устройства (PD);
 - ❑ **питаемые устройства** (Powered Device, PD) получают электропитание через кабель от питающих устройств.

- ❑ В сети Ethernet могут использоваться два типа *питающего* оборудования PSE:
 - ❑ **«Endpoint»** - коммутатор с поддержкой PoE;
 - ❑ **«Midspan»** - инжектор PoE.

Технология Power over Ethernet

Схема построение сети PoE с использованием коммутатора PoE



Технология Power over Ethernet

Схема построение сети PoE с использованием инжектора PoE

Коммутатор с 8 портами без поддержки PoE



Инжектор PoE



- Данные (кабель Ethernet Cat. 5 и выше)
- Данные + питание (кабель Ethernet Cat. 5 и выше)

IP-камера с PoE

- ❑ Спецификация PoE определяет два типа систем питания: **Тип 1** (Type 1) и **Тип 2** (Type 2). Система питания состоит из одного PSE и одного PD, связанных каналом связи.

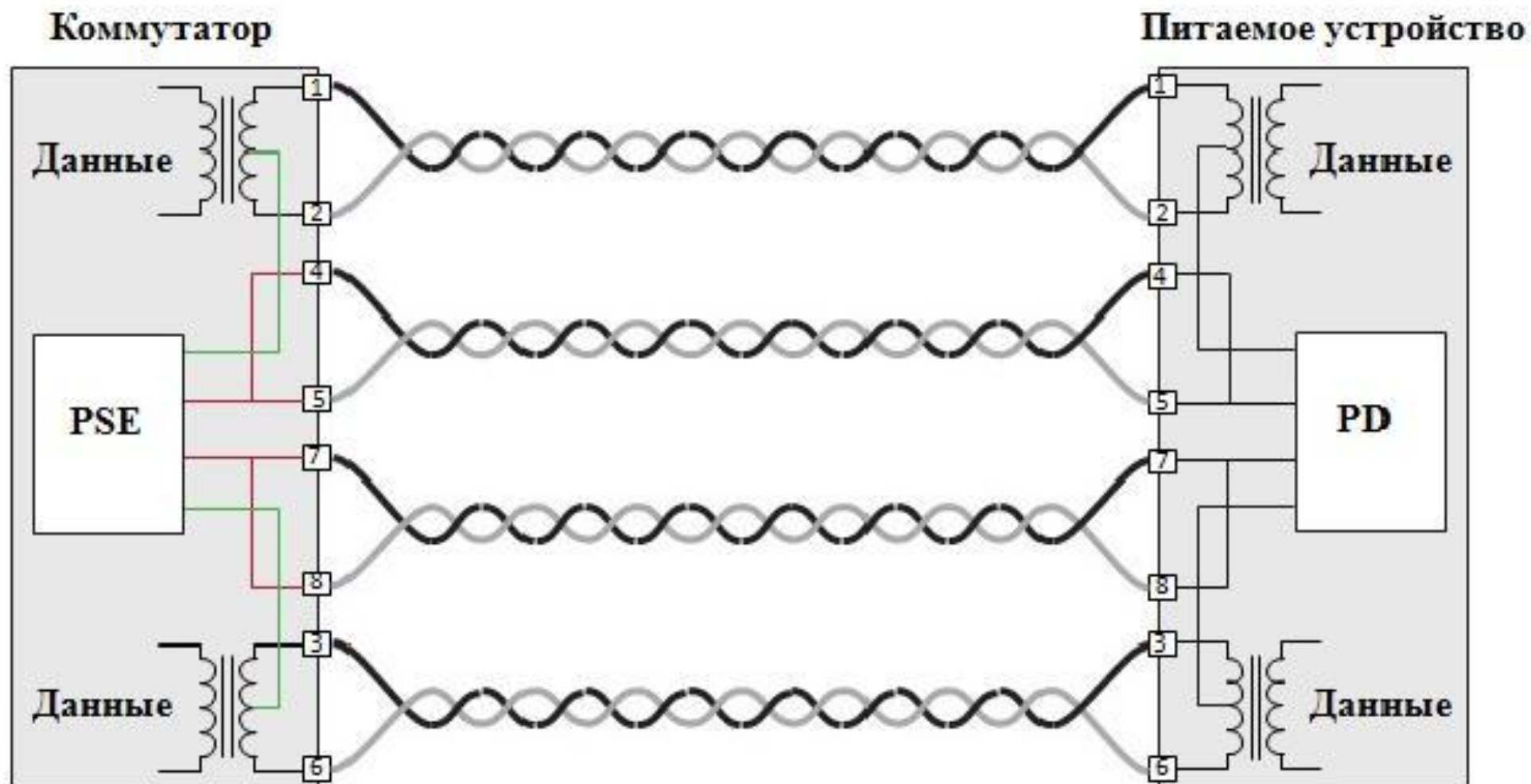
- ❑ **Устройства PSE и PD Типа 1:**
 - ❑ предназначены для работы только в сетях 10BASE-T и 100BASE-TX;
 - ❑ для передачи питания используются две пары кабеля на основе витой пары категории 3 и выше;
 - ❑ номинальный постоянный ток 350 мА для каждой витой пары;
 - ❑ сопротивление кабеля постоянному току 20 Ом;
 - ❑ выходное напряжение лежит в диапазоне от 44 до 57 В постоянного тока;
 - ❑ минимальный уровень выходной мощности равен 15,4 Вт;
 - ❑ входное напряжение лежит в диапазоне от 37 до 57 В постоянного тока;
 - ❑ максимальная входная мощность в среднем равна 13 Вт с учетом потерь в кабеле.

❑ **Устройства PSE и PD Типа 2:**

- ❑ предназначены для работы в сетях 10BASE-T, 100BASE-TX и 1000BASE-T;
- ❑ для передачи питания используются две пары кабеля на основе витой пары категории 5/5е и выше;
- ❑ номинальный постоянный ток 600 мА для каждой витой пары;
- ❑ сопротивление кабеля постоянному току 12,5 Ом;
- ❑ выходное напряжение лежит в диапазоне от 50 до 57 В постоянного тока;
- ❑ минимальный уровень выходной мощности равен 30 Вт;
- ❑ входное напряжение лежит в диапазоне от 42,5 до 57 В постоянного тока;
- ❑ максимальная входная мощность в среднем равна 25,5 Вт с учетом потерь в кабеле.

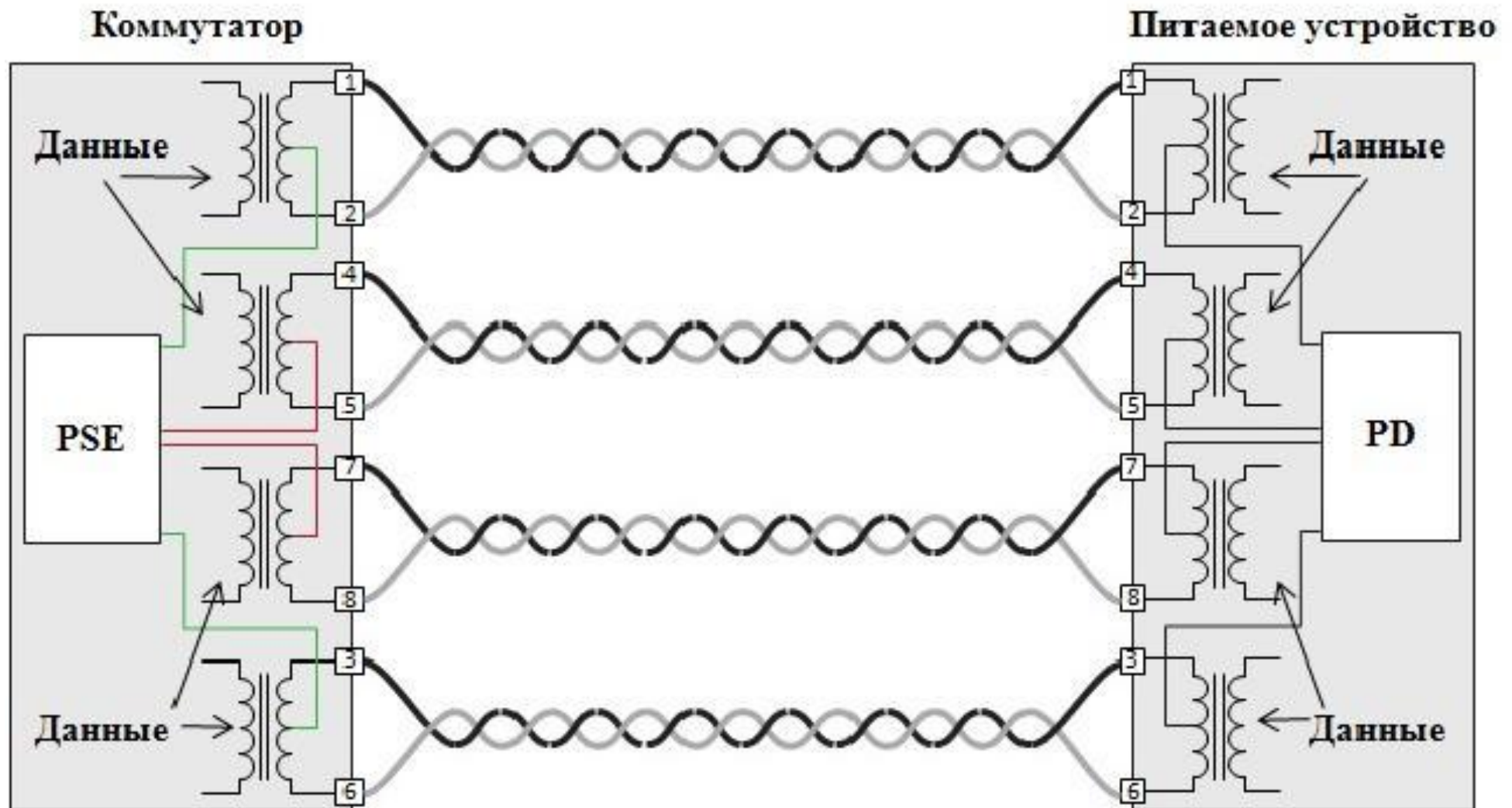
Технология Power over Ethernet

Схема питания Endpoint PSE в сети 10/100BASE-TX (вариант А – зеленый; вариант В – красный)



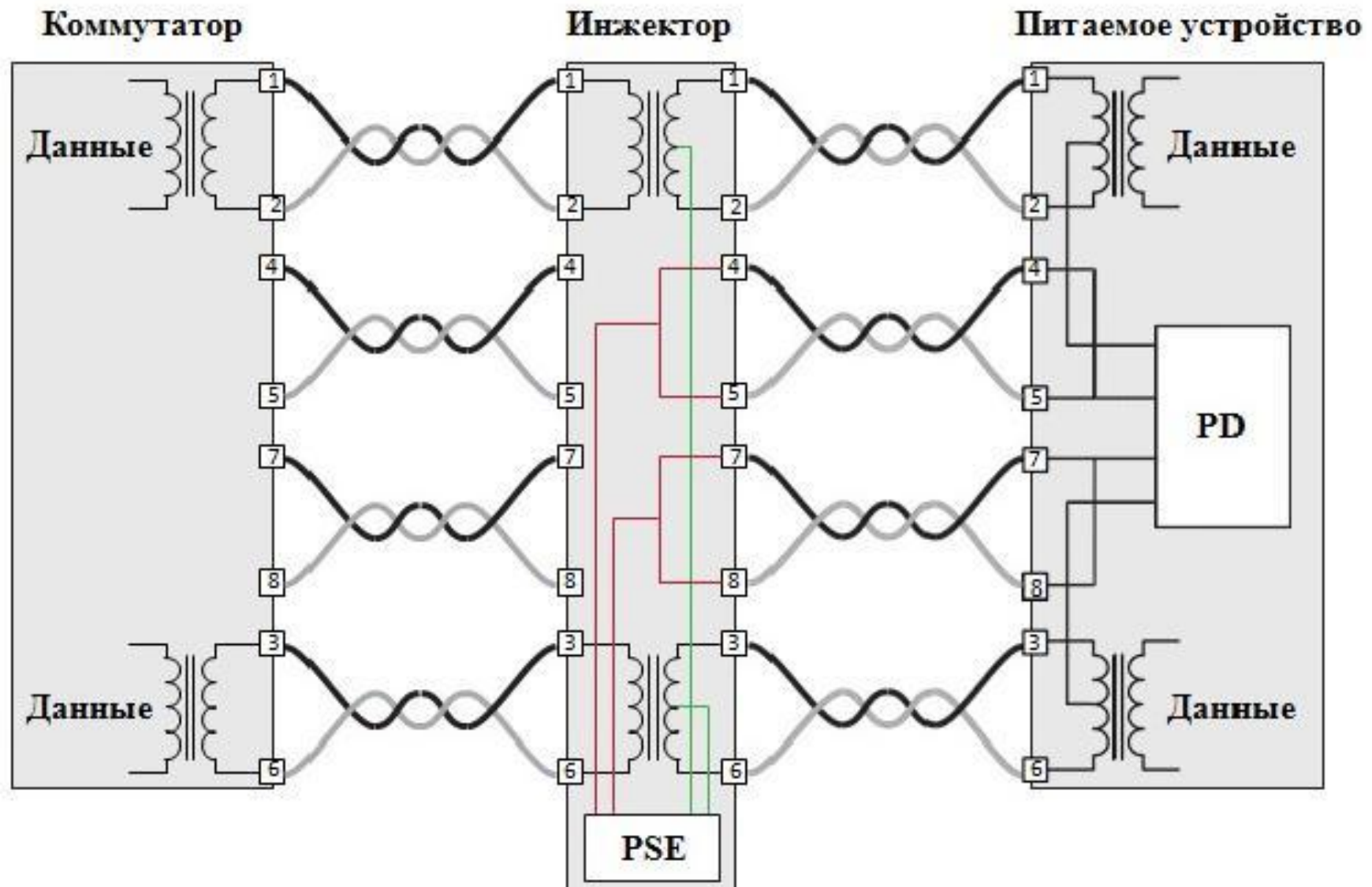
Технология Power over Ethernet

Схема питания Endpoint PSE в сети 1000BASE-T (вариант А – зеленый; вариант В – красный)



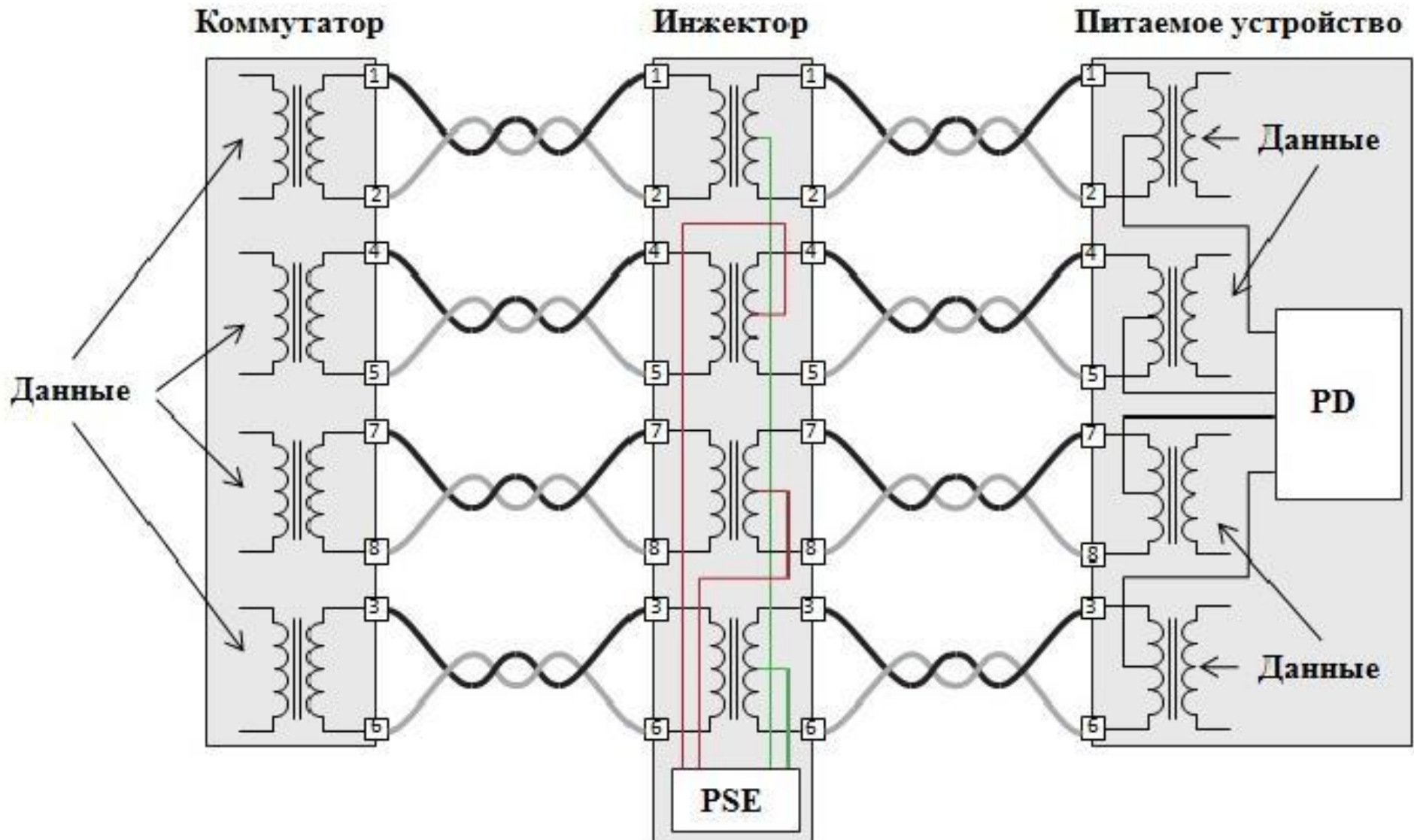
Технология Power over Ethernet

Схема питания Midspan PSE в сети 10/100BASE-TX (вариант А – зеленый; вариант В – красный)



Технология Power over Ethernet

Схема питания Midspan PSE в сети 1000BASE-T (вариант А – зеленый; вариант В - красный)



- ❑ После идентификации удаленного устройства как PoE-совместимого PSE выполняет его классификацию.
- ❑ Классификацией называется способность PSE отправлять запросы PD с целью определения мощности, потребляемой PD.
- ❑ Процедура классификации по мощности предназначена для взаимной идентификации PSE и PD. Механизм взаимной идентификации позволяет PD Типа 2 отличить PSE Типа 1 от PSE Типа 2, PSE Типа 2 отличить PD Типа 1 от PD Типа 2.
- ❑ Существует две формы классификации: классификация на физическом уровне и классификация на канальном уровне.

- ❑ **Классификация на физическом уровне** использует электрические характеристики PD, на основе которых PSE определяет какой класс присвоить PD на основе потребляемой им мощности и вычисляет свою минимальную мощность на выходе.

Класс	Минимальная мощность на выходе устройства PSE, Вт
0	15,4
1	4
2	7
3	15,4
4	30

- ❑ Спецификация PoE делит устройства PD в зависимости от потребляемой мощности на 5 классов: от 0 до 4

Класс	Средняя мощность на входе устройства PD, Вт
0	13
1	3,84
2	6,49
3	13
4	25,5

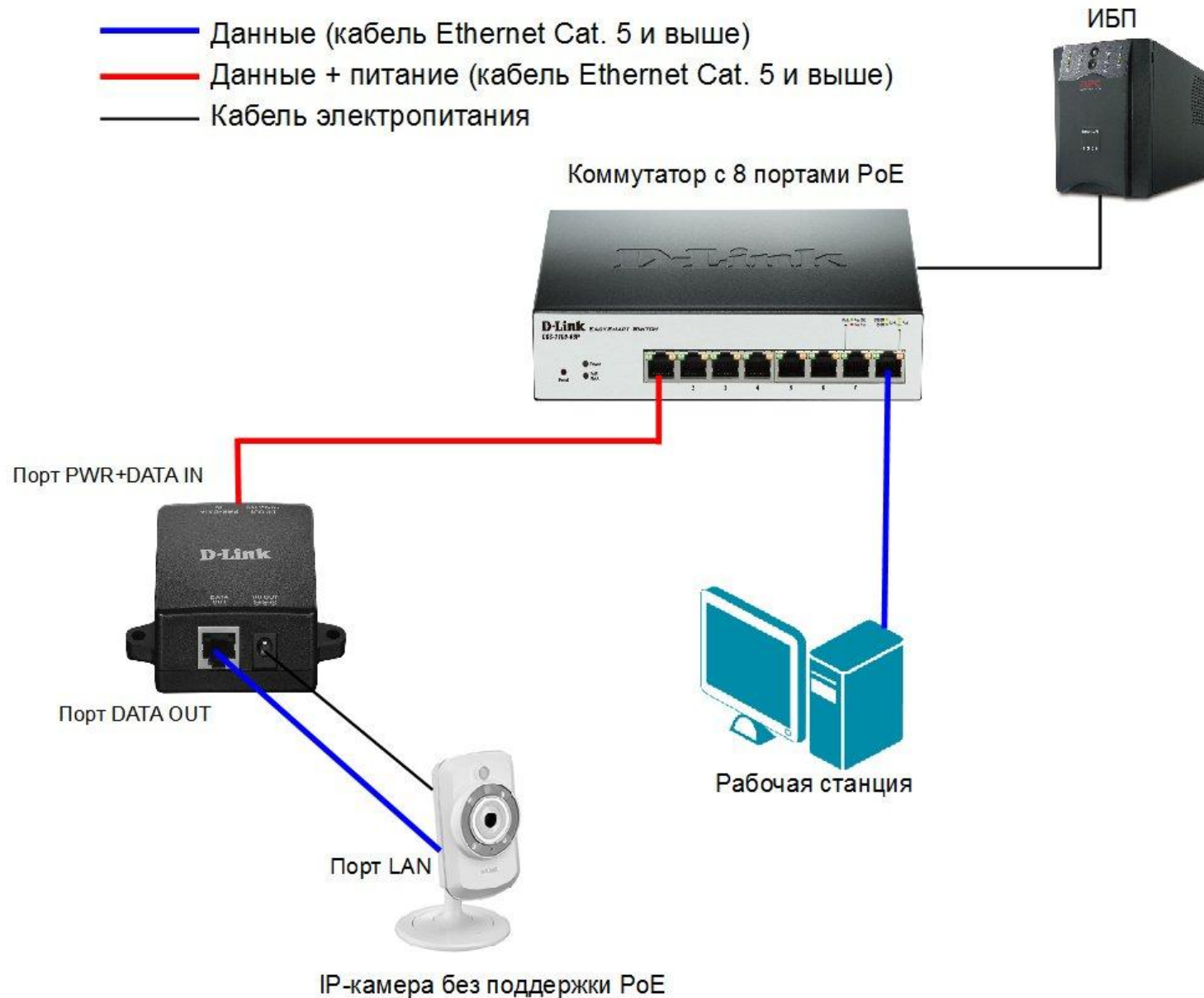
- ❑ **Классификация на канальном уровне** выполняется PSE и PD с помощью протокола Data Link Layer (DLL).
- ❑ Эта классификация обеспечивает более точное определение потребляемой мощности PD и позволяет PSE динамически изменять значение выходной мощности в зависимости от текущих потребностей PD.
- ❑ Устройства PSE могут выполнять классификацию PD на физическом уровне, на канальном уровне или использовать комбинацию обоих методов.
- ❑ После завершения процесса классификации устройство PSE подает в кабель напряжение 48 В. Спецификация PoE предусматривает автоматическое отключение напряжения питания, если сопротивление приемника или отдаваемый ток резко меняется.

PoE-сплиттер

- ☐ Сплиттер является пассивным устройством и используется для подключения к сети PoE устройств без поддержки функции PoE.
- ☐ Функция сплиттера противоположна функции инжектора.
- ☐ Сплиттер подключается к сети PoE, из которой получает данные и питание по кабелю на основе витой пары. На выходе он разделяет данные и питание, которые далее передаются соответственно через кабель на основе витой пары и стандартный кабель питания.

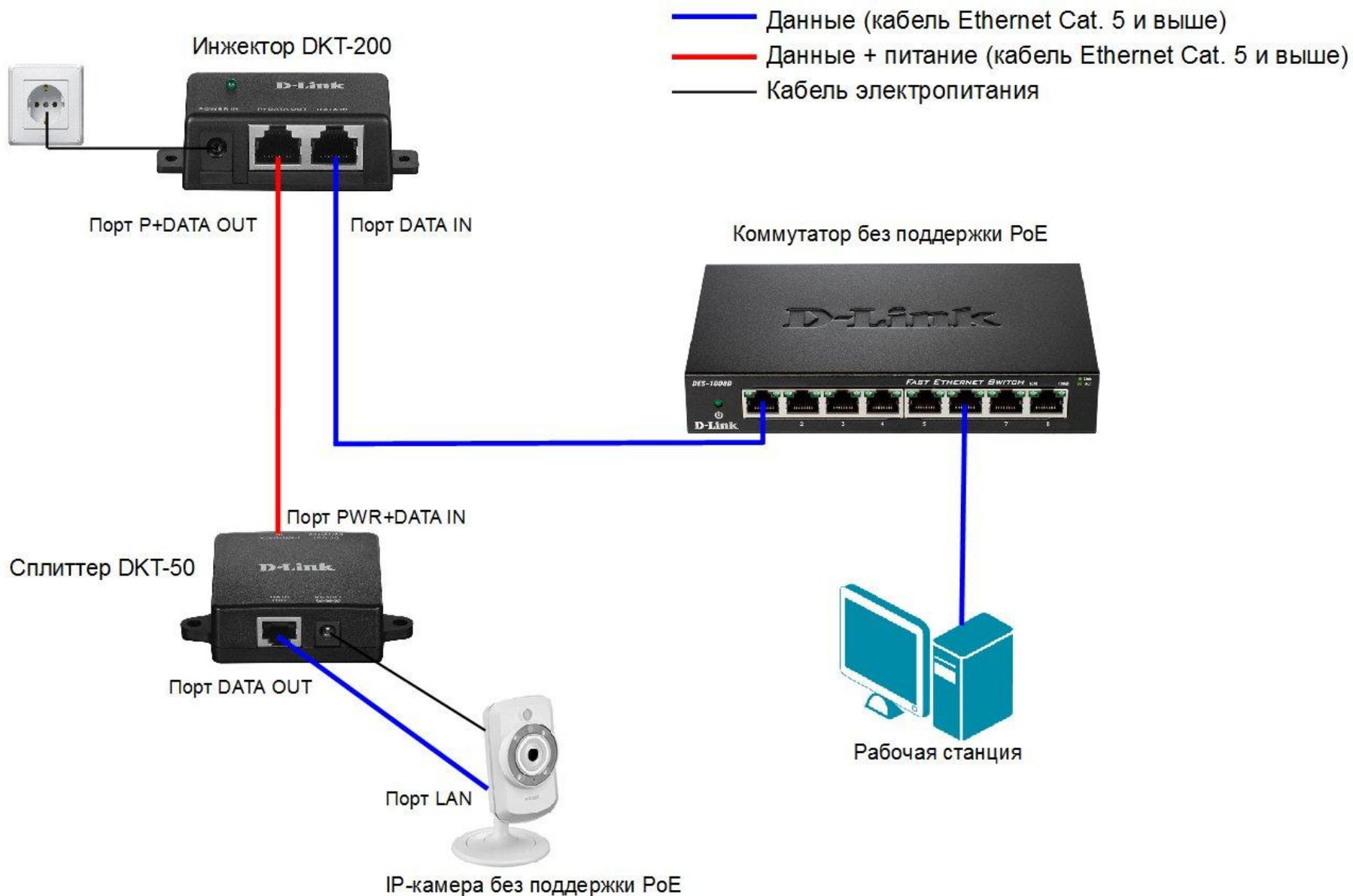
Технология Power over Ethernet

Подключение IP-камеры с помощью сплиттера к сети PoE



Технология Power over Ethernet

Организация подачи электропитания в сети без поддержки технологии PoE



Как выбрать коммутатор PoE для сети

- ❑ Подбирая коммутатор PoE, проектировщик или сетевой администратор должен ответить на ряд вопросов:
 - ❑ Поддерживается ли функция PoE на всех портах коммутатора?
 - ❑ Хватит ли мощности для обеспечения питания всех подключаемых устройств?
 - ❑ Поддерживается ли коммутатором функция защиты от превышения величины тока для каждого порта?

- ❑ **Энергетический потенциал PoE** (PoE Power Budget) – это общая мощность PoE, которую коммутатор может доставить ко всем портам.

Спасибо за внимание!