Основы современных сетей на примере управляемых коммутаторов D-Link

Владимир Музыка
D-Link Россия, Краснодар
Региональный представитель
vmuzyka@dlink.ru

Содержание

- **Типы сетей**
- **Модель OSI**
- **Типы коммутаторов**
- **Уровни организации сети**
- **VLAN**
- **Приоритеты и качество обслуживания**
- **Протоколы покрывающего дерева STP, RSTP, MSTP**
- **Агрегирование каналов**
- **Контроль полосы пропускания**

Организация сети

Организацией сети - называется обеспечение взаимосвязи между рабочими станциями, периферийным оборудованием (принтерами, накопителями на жестких дисках, сканерами, приводами CD-ROM) и другими устройствами.

Задача: согласование различных типов компьютеров независимо от того, какие устройства используются в сети — Macintosh, IBM-совместимые компьютеры или мэйнфреймы, — все они должны использовать для общения один и тот же язык.

Таким языком служит *ПРОТОКОЛ,* который является формальным описанием набора правил и соглашений, регламентирующих обмен информацией между устройствами в сети.

Организация сети

Первые компьютеры были ***Автономными устройствами***. Очень скоро стала очевидной низкая эффективность такого подхода.

Необходимо было найти решение, которое бы удовлетворяло трем перечисленным ниже требованиям, а именно:

- устраняло дублирование оборудования и ресурсов;
- обеспечивало эффективный обмен данными между устройствами;
- снимало проблему управления сетью.

Было найдено два решения, выполняющих поставленные условия.

Это были ***локальные*** и ***глобальные*** сети.

Организация сети

Локальные сети (Local Area Networks, LAN), позволяющие предприятиям, применяющим в своей производственной деятельности компьютерные технологии, повысить эффективность коллективного использования одних и тех же ресурсов, например , файлов и принтеров

Глобальные сети (Wide Area Networks, WAN), делающие возможным обмен данными между предприятиями, которые удалены на значительные расстояния друг от друга.

Локальная сеть

Локальные сети служат для объединения рабочих станций, периферии, терминалов и других устройств. Локальная сеть позволяет повысить эффективность работы компьютеров за счет совместного использования ими ресурсов, например файлов и принтеров.

Характерными особенностями локальной сети являются:

· ограниченные географические пределы;

· обеспечение многим пользователям доступа к среде с высокой пропускной способностью;

· постоянное подключение к локальным сервисам;

· физическое соединение рядом стоящих устройств.

Глобальная сеть

Глобальные сети. Быстрое распространение компьютеров привело к увеличению числа локальных сетей. Они появились в каждом отделе и учреждении. В то же время каждая локальная сеть — это отдельный электронный остров, не имеющий связи с другими себе подобными.

Требовалось найти способ передачи информации от одной локальной сети к другой. Решить эту задачу помогло создание ***глобальных сетей***.

Глобальные сети служат для объединения локальных сетей и обеспечивают связь между компьютерами, находящимися в локальных сетях. Они охватывают значительные географические пространства и дают возможность связать устройства, расположенные на большом удалении друг от друга.

Стандартизация. ISO

Международная организация по стандартизации (International Organization for Standardization, ISO) исследовала существующие схемы сетей.

В результате исследования была признана необходимость в создании эталонной модели сети, которая смогла бы помочь поставщикам создавать совместимые сети.

И в 1984 году ISO выпустила в свет эталонную модель взаимодействия открытых систем (OSI).

Эталонная модель OSI быстро стала основной архитектурной моделью взаимодействия между компьютерами. Несмотря на то, что были разработаны и другие архитектурные модели, большинство поставщиков сетей, желая сказать пользователям, что их продукты совместимы и способны работать с разными производимыми в мире сетевыми технологиями, ссылаются на их соответствие эталонной модели OSI.

Модель ISO

Эталонная модель OSI — ***это описательная схема сети***, ее стандарты гарантируют:

- высокую совместимость
- способность к взаимодействию различных типов сетевых технологий.

Кроме того, она иллюстрирует процесс перемещения информации по сетям.

Это концептуальная структура, определяющая сетевые функции, реализуемые на каждом ее уровне.

Модель OSI описывает, каким образом информация проделывает путь через сетевую среду (например, провода) от одной прикладной программы например, программы обработки таблиц) к другой прикладной программе, находящейся в другом подключенном к сети компьютере.

Модель ISO

Эталонная модель OSI делит задачу перемещения информации между компьютерами через сетевую среду на семь менее крупных и, следовательно, более легко разрешимых подзадач.

Такое разделение на уровни называется ***иерархическим представлением***. Каждый уровень соответствует одной из семи подзадач

Модель ВОС (ISO), Уровень 4

Предоставляя надежные услуги, ***Транспортный уровень*** *обеспечивает механизмы для установки, поддержания и упорядоченного завершения действия виртуальных каналов, обнаружения и устранения неисправностей транспортировки, а также управления информационным потоком* (с целью предотвращения переполнения одной системы данными от другой системы).

Модель BOC (ISO), Уровень 3 и 2

Данные	**При** Доступ к с
Данные	**Пред** Представление
Данные	**Се** Управлен
Блоки	**Тран** Безопасное со
Пакеты	**Сетевой** Определение пути и IP-адреса
Кадры	**Канальный** Физическая адресация (MAC и LLC)
Биты	**Физический** Кабель, сигналы, разъемы

Уровень 3 (сетевой)

Сетевой уровень — это комплексный уровень, который обеспечивает соединение и выбор маршрута между двумя конечными системами, которые могут находиться в географически разных сетях.

Уровень 2 (канальный)

Канальный уровень обеспечивает надежный транзит данных через физический канал. Выполняя эту задачу, уровень решает вопросы физической адресации, топологии сети, дисциплины в канале связи (т.е. каким образом конечная система использует сетевой канал), уведомления об ошибках, упорядоченной доставки кадров, а также вопросы управления потоком данных.

Модель BOC (ISO), Уровень 1

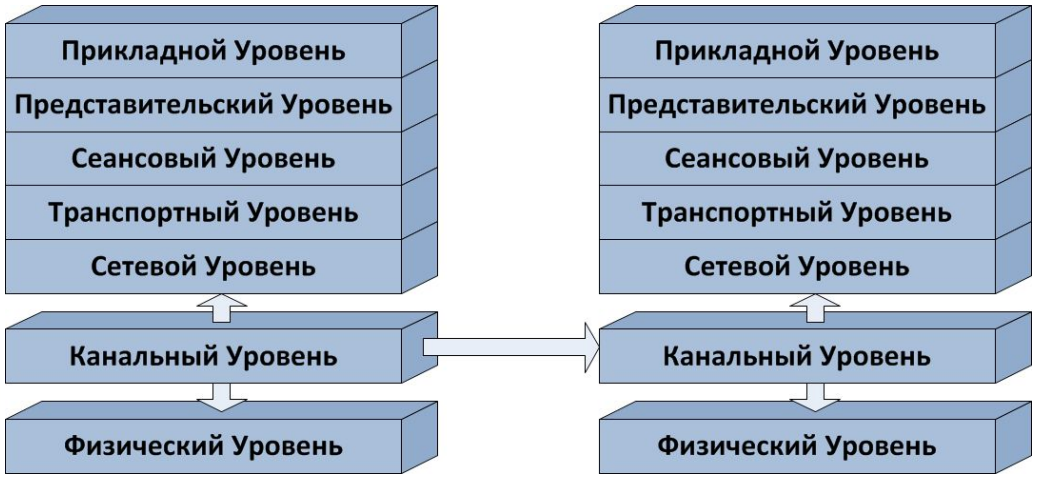
Данные	**При** Доступ к с
Данные	**Пред** Представление
Данные	**Се** Управлен
Блоки	**Тран** Безопасное со
Пакеты	**Сетевой** Определение пути и IP-адреса
Кадры	**Канальный** Физическая адресация (MAC и LLC)
Биты	**Физический** Кабель, сигналы, разъемы

Уровень 1 (физический)

Физический уровень определяет электро-технические, механические, процедурные и Функциональные характеристики активизации, поддержания и деактивизации физического канала между конечными системами.

Спецификации физического уровня определяют такие характеристики, как *уровни напряжений*, *временные параметры изменения напряжений*, *скорости физической передачи данных*, *максимальные расстояния передачи информации*, *физические разъемы*, и другие подобные характеристики.

Одноранговая модель взаимодействия



Многоуровневая модель OSI исключает прямую связь между равными по положению уровнями, находящимися в разных системах. Каждый уровень системы имеет свои определенные задачи, которые он должен выполнять.

Для выполнения этих задачи, он должен общаться с соответствующим уровнем в другой системе.

Обмен сообщениями между одноранговыми уровнями или, как их еще называют, ***блоками данных протокола*** *(protocol data units, PDUs),* осуществляется с помощью протокола соответствующего уровня.

Каждый уровень может использовать свое специфическое название для PDU.

Физический и канальный уровни

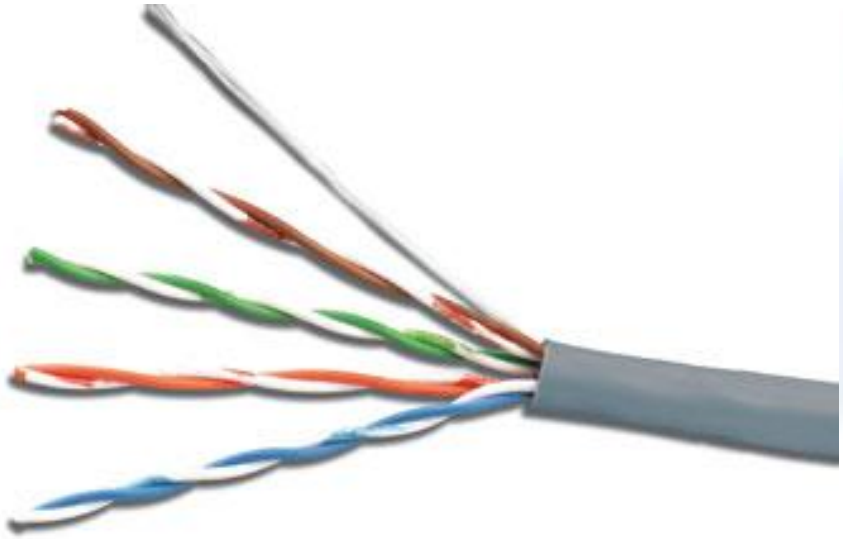
Средой передачи данных называется физическая среда, пригодная для прохождения сигнала.

Чтобы компьютеры могли обмениваться кодированной информацией, среда должна обеспечить их физическое соединение друг с другом. Существует несколько видов сред, применяемых для соединения компьютеров:

- коаксиальный кабель;
- неэкранированная витая пара;
- экранированная витая пара;
- оптоволоконный кабель.

Неэкранированная витая пара

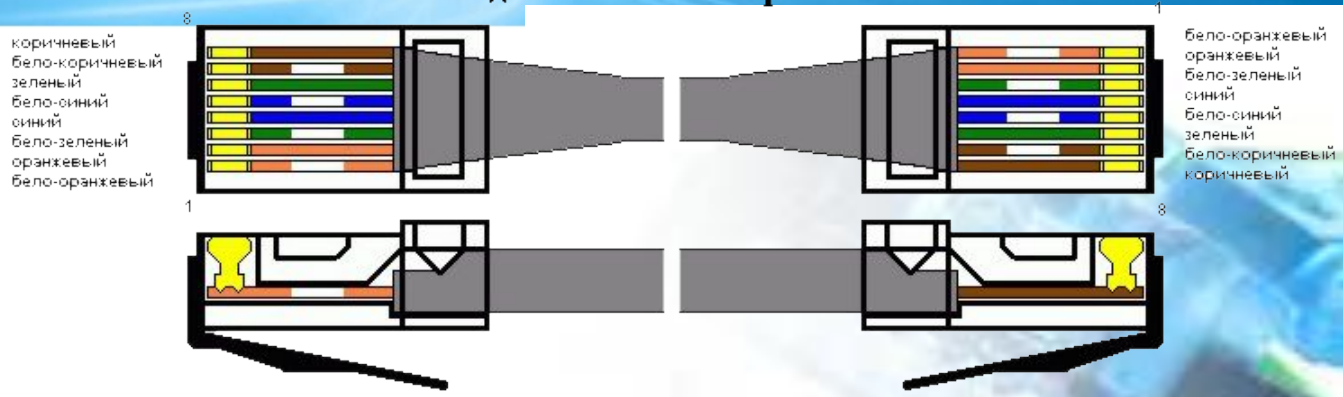
D-Link
Building Networks for People



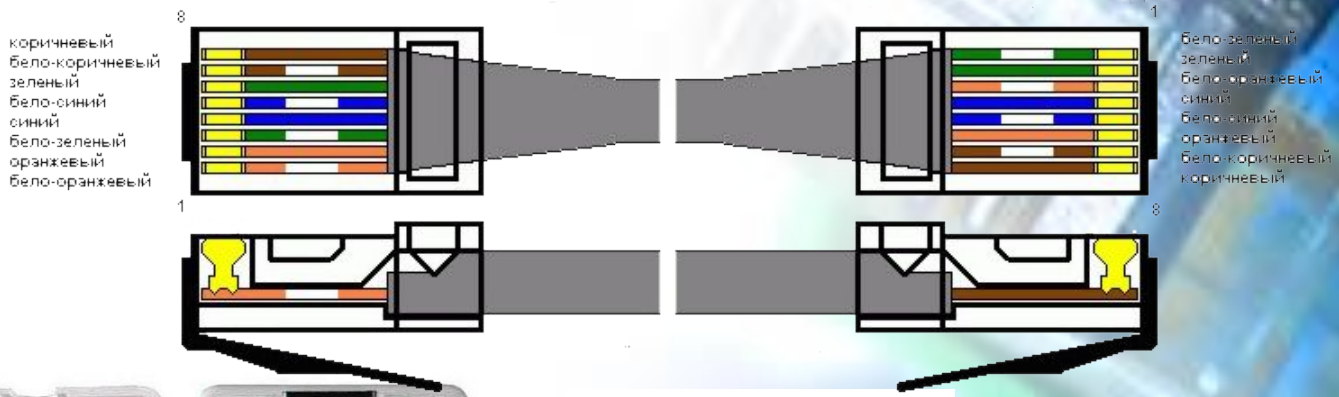
Неэкранированная витая пара

D-Link
Building Networks for People

Соединение компьютер-хаб

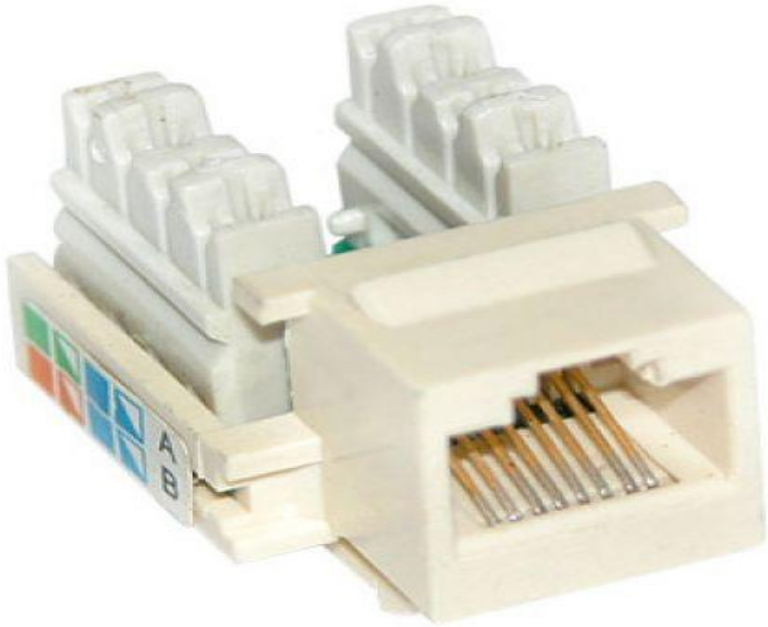


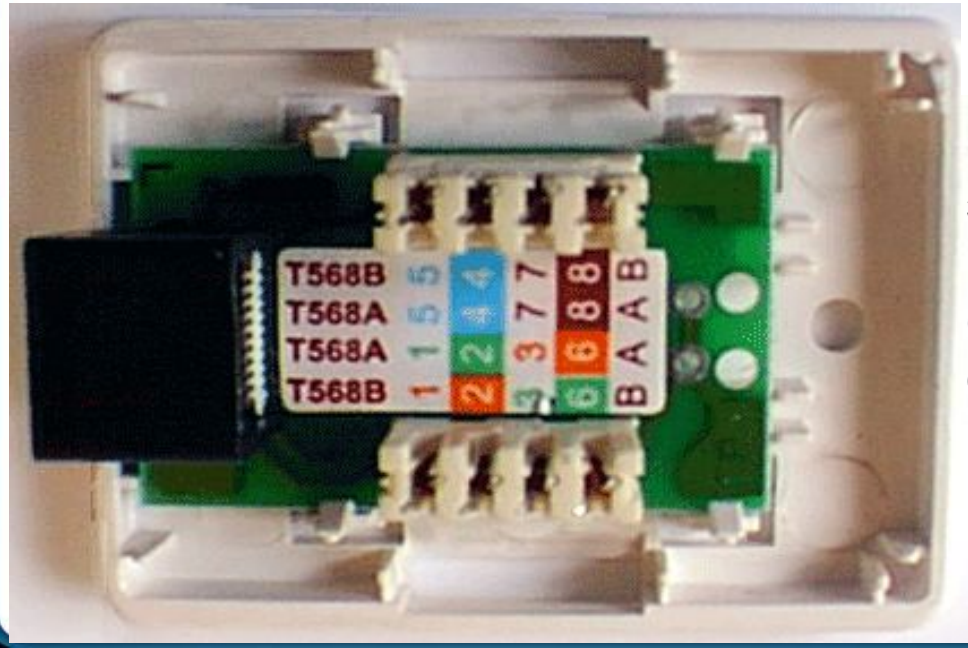
Соединение компьютер-компьютер , хаб-хаб



Неэкранированная витая пара

RJ45 — разъем стандарта **Registered Jack**. По внешнему сходству часто путают с разъемом формата 8P8C, который используется в локальных вычислительных сетях Ethernet (ЛВЧ).





В свою очередь Registered jack (RJ), это стандартизированный физический интерфейс, который используется для соединения телекоммуникационного оборудования. Стандартные варианты разъема Registered Jack: RJ11, RJ14, RJ25, RJ45.


D-Link
Building Networks for People

Оптоволоконный кабель

Оптоволоконный кабель является средой передачи данных, которая способна проводить модулированный световой сигнал.

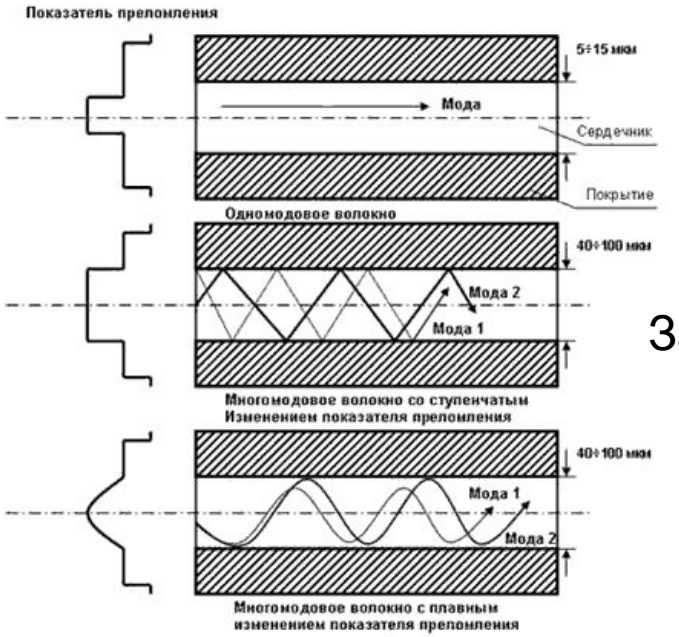
Оптоволоконный кабель невосприимчив к электро-магнитным помехам и способен обеспечивать более высокую скорость передачи данных, чем кабели UTP, STP и коаксиальный кабель.

В отличие от других сред передачи данных, имеющих в основе медные проводящие элементы, оптоволоконный кабель не проводит электрические сигналы. Вместо этого в оптоволоконном кабеле соответствующие битам сигналы заменяются световыми импульсами.

Оптоволоконный кабель

Оптоволоконный кабель, использующийся в сетях передачи данных, состоит из двух стекловолокон, заключенных в отдельные оболочки.

Если посмотреть на кабель в поперечном сечении, то можно увидеть, что каждое стекловолокно окружено слоем отражающего покрытия.



Затем следует слой из пластмассы, имеющей название ***кевлар*** *(Kevlar)* (защитный материал, обычно использующийся в пуле-непробиваемых жилетах), и дальше идет внешняя оболочка

Оптоволоконный кабель

D-Link
Building Networks for People

Канальный уровень

В эталонной модели OSI канальный и физический уровни являются смежными.

Канальный уровень обеспечивает надежный транзит данных через физический уровень. Этот уровень использует адрес ***управления доступом к среде передачи данных*** *(Media Access Control, MAC).*

Канальный уровень решает вопросы:

- физической адресации (в противоположность сетевой или логической адресации),
- топологии сети,
- дисциплины линий связи (каким образом конечной системе использовать сетевой канал);
- уведомления об ошибках;
- упорядоченной доставки кадров;
- управления потоком информации.

Канальный уровень

Канальный уровень использует MAC-адрес в качестве средства задания аппаратного или канального адреса, позволяющего нескольким станциям коллективно использовать одну и ту же среду передачи данных и одновременно уникальным образом идентифицировать друг друга.

Для того чтобы мог осуществляться обмен пакетами данных между физически соединенными устройствами, относящимися к одной локальной сети, каждое устройство-отправитель должно иметь MAC-адрес, который оно может использовать в качестве адреса пункта назначения.

Технология Ethernet

Ethernet был разработан Исследовательским центром корпорации Xerox в Пало Альто (PARC) в 1970 году и является на сегодняшний день наиболее популярным стандартом.

Первым локальным сетям требовалась очень небольшая пропускная способность для выполнения простых сетевых задач, существовавших в то время, — отправка и прием электронной почты, передача файлов данных и обработка заданий по выводу на печать.

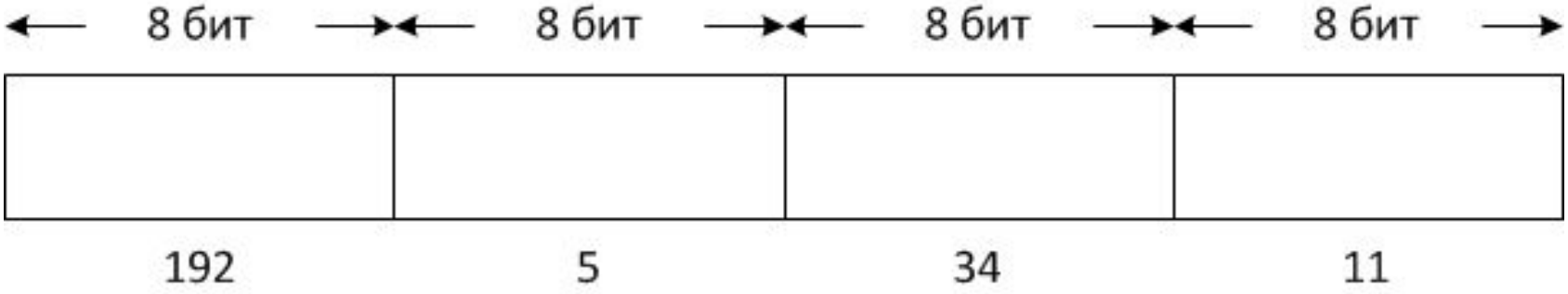
Ethernet стал основой для спецификации IEEE 802.3, которая была выпущена в 1980 году Институтом инженеров по электротехнике и электронике. Вскоре после этого компании Digital Equipment Corporation, Intel Corporation и Xerox Corporation совместно разработали и выпустили спецификацию Ethernet версии 2.0

IP-адресация

В сетях используются две схемы адресации. Одна из этих схем, MAC-адресация, была рассмотрена ранее. Второй схемой является IP-адресация.

Как следует из названия, IP-адресация базируется на протоколе IP (Internet Protocol). Каждая ЛВС должна иметь свой уникальный IP-адрес, который является определяющим элементом для осуществления межсетевого взаимо-действия в глобальных сетях.

IP-адресация



В IP-сетях конечная станция связывается с сервером или другой конечной станцией. Каждый узел имеет IP-адрес, который представляет собой уникальный 32-битовый логический адрес.

IP-адресация существует на уровне 3 (сетевом) эталонной модели OSI. В отличие от MAC-адреса, которые обычно существуют в плоском адресном пространстве, IP-адреса имеют иерархическую структуру.

IP-адресация

Октет (8 бит) * Октет (8 бит) * Октет (8 бит) * Октет (8 бит)

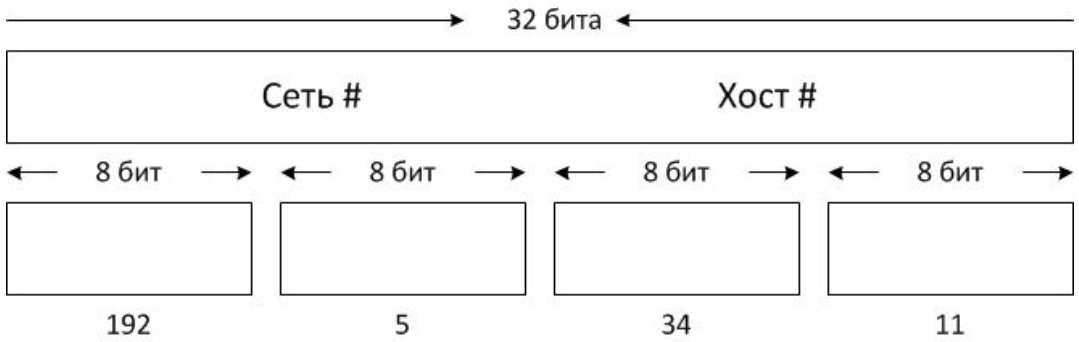
$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ * $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ * $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ * $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$

11000000 * 00000101 * 00100010 * 00001011

Так как двоичная система основана на возведении в степень числа 2, каждая позиция в октете представляет различные степени от 2. Величина показателя степени 2 назначается каждому разряду двоичного числа, начиная с крайнего правого.

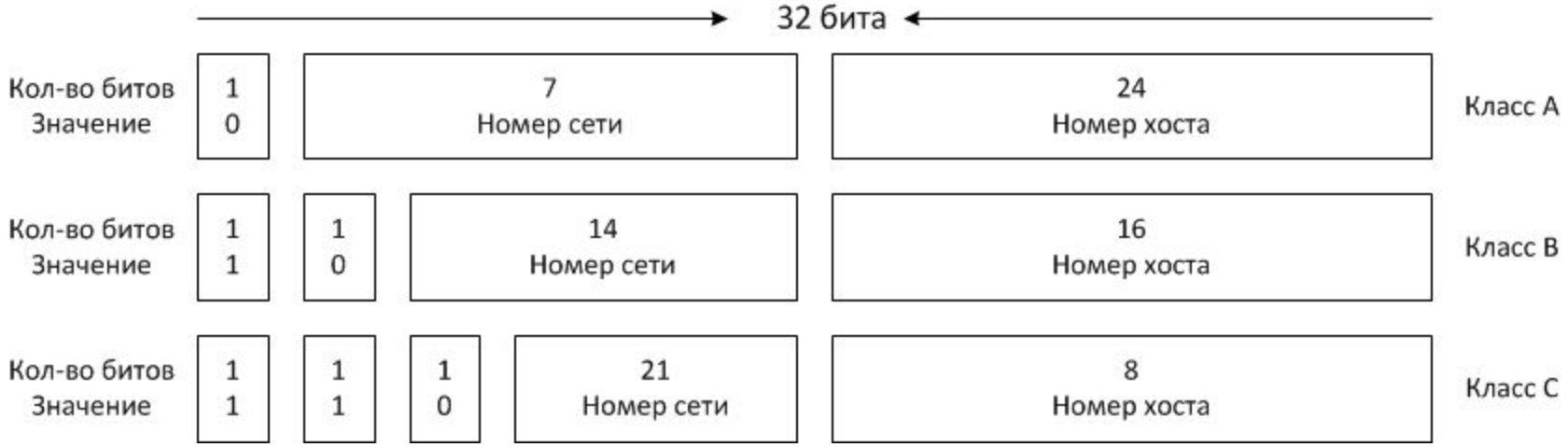
IP-адресация

Для того чтобы каждый сетевой адрес был уникальным и отличался от любого другого номера, организация под названием American Registry for Internet Numbers (Американский реестр Internet-номеров, ARIN) выделяет компаниям блоки IP-адресов в зависимости от размера их сетей. Адрес ARIN в Internet — www.arin.net.



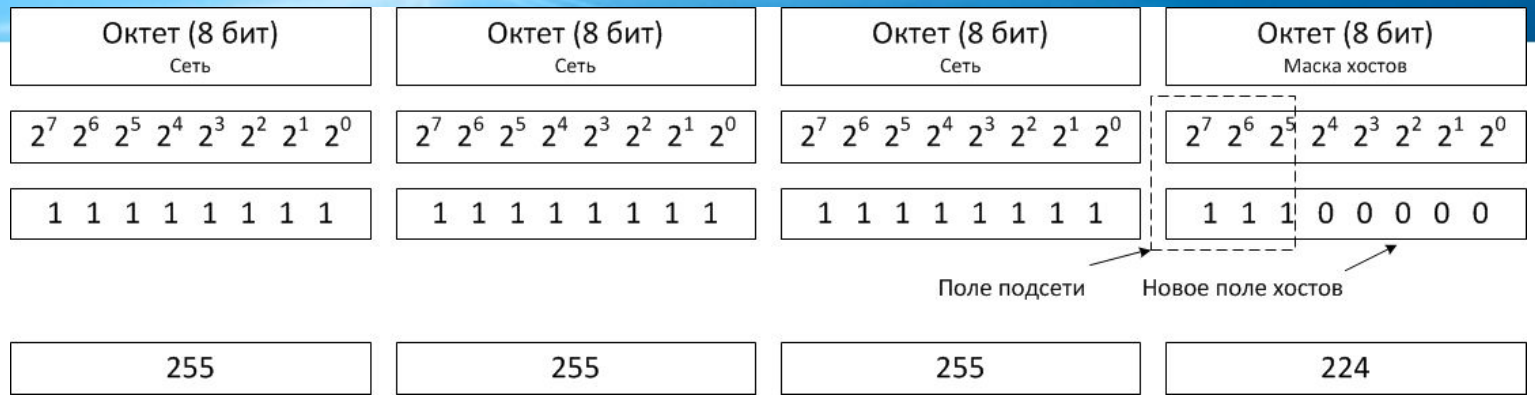
Класс A - составляют IP-адреса, зарезер-вированные для правительственных учреждений и крупных корпораций,
класс B - IP-адреса для компаний среднего уровня
класс C - для всех остальных организаций.
класс D - для групповой адресации
класс E - для исследований

IP-адресация

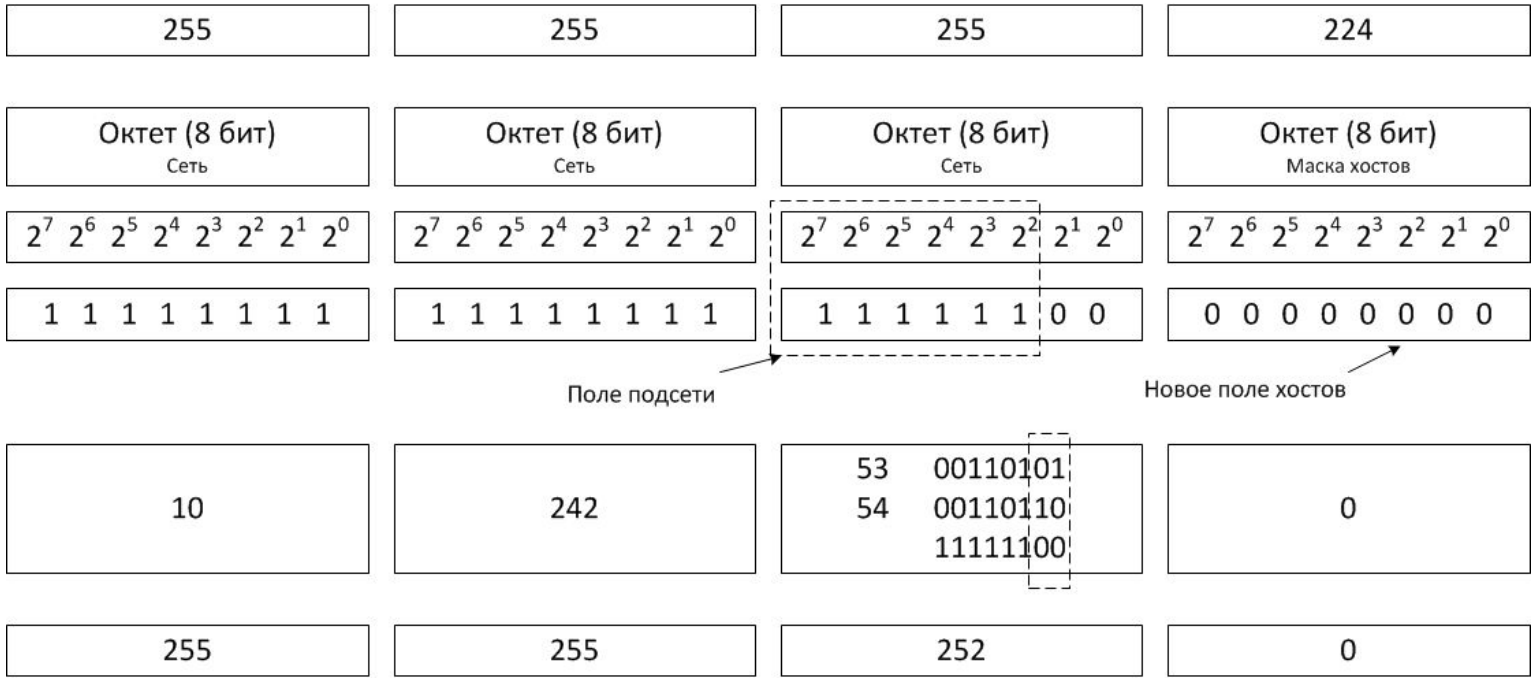


Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	192.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

IP-адресация



Пример образования маски подсети



Распределение IP-адресов, DHCP

DHCP (англ. *Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (обычно MAC-адресу) каждого клиентского компьютера определённый IP-адрес.

Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется *арендой адреса*. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым).

Система доменных имен DNS

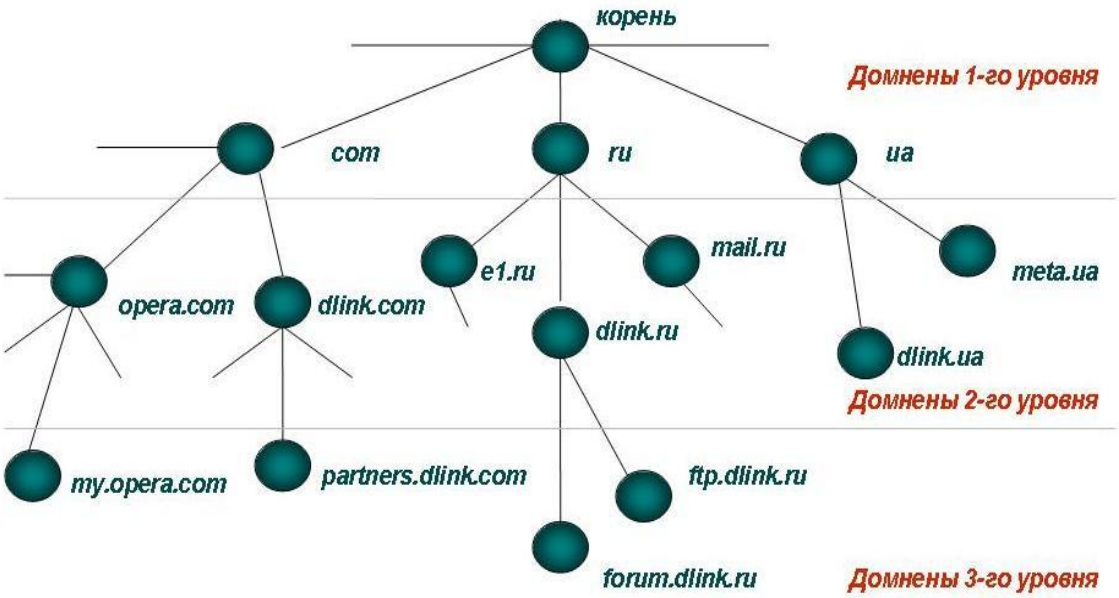
Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы. На раннем этапе развития Internet на каждом хосте вручную создавался текстовый файл с известным именем ***hosts***. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «IP-адрес - доменное имя», например:
207.232.83.10 - www.dlink.com

По мере роста Internet, файлы hosts также росли, и создание масштабируемого решения для разрешения имен стало необходимостью. Таким решением стала специальная служба - ***система доменных имен (Domain Name System, DNS).***

Система доменных имен DNS

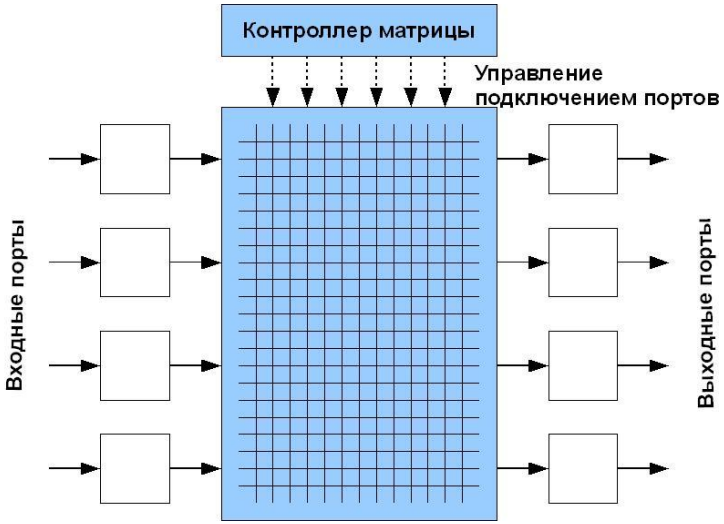
В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей.

Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. Составные части доменного имени отделяется друг от друга точкой. Например, в имени partnering.dlink.com составляющая partnering является именем одного из компьютеров в домене dlink.com.



Коммутаторы

Коммутатор (Switch) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю.



Коммутаторы

Коммутатор хранит в памяти таблицу, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры и, определив MAC-адрес хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя ещё не известен, то кадр будет продублирован на все интерфейсы. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Типы коммутаторов

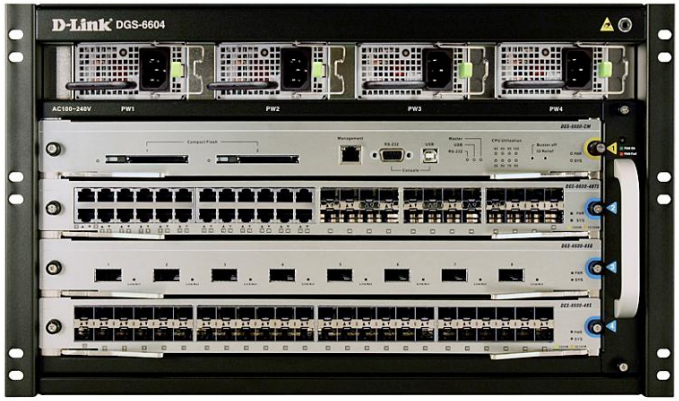
Неуправляемые коммутаторы, являются идеальным решением для развертывания сетей небольших рабочих групп или домашних сетей. Также их можно использовать на уровне доступа сетей малых предприятий.
Эти коммутаторы просты в установке и поддерживают, в зависимости от модели следующие функции – диагностика кабеля, управление потоком (IEEE 802.3x), автоматическое определение полярности (MDI/MDIX), возможность передачи Jumbo-фреймов и приоритезацию трафика.

Типы коммутаторов

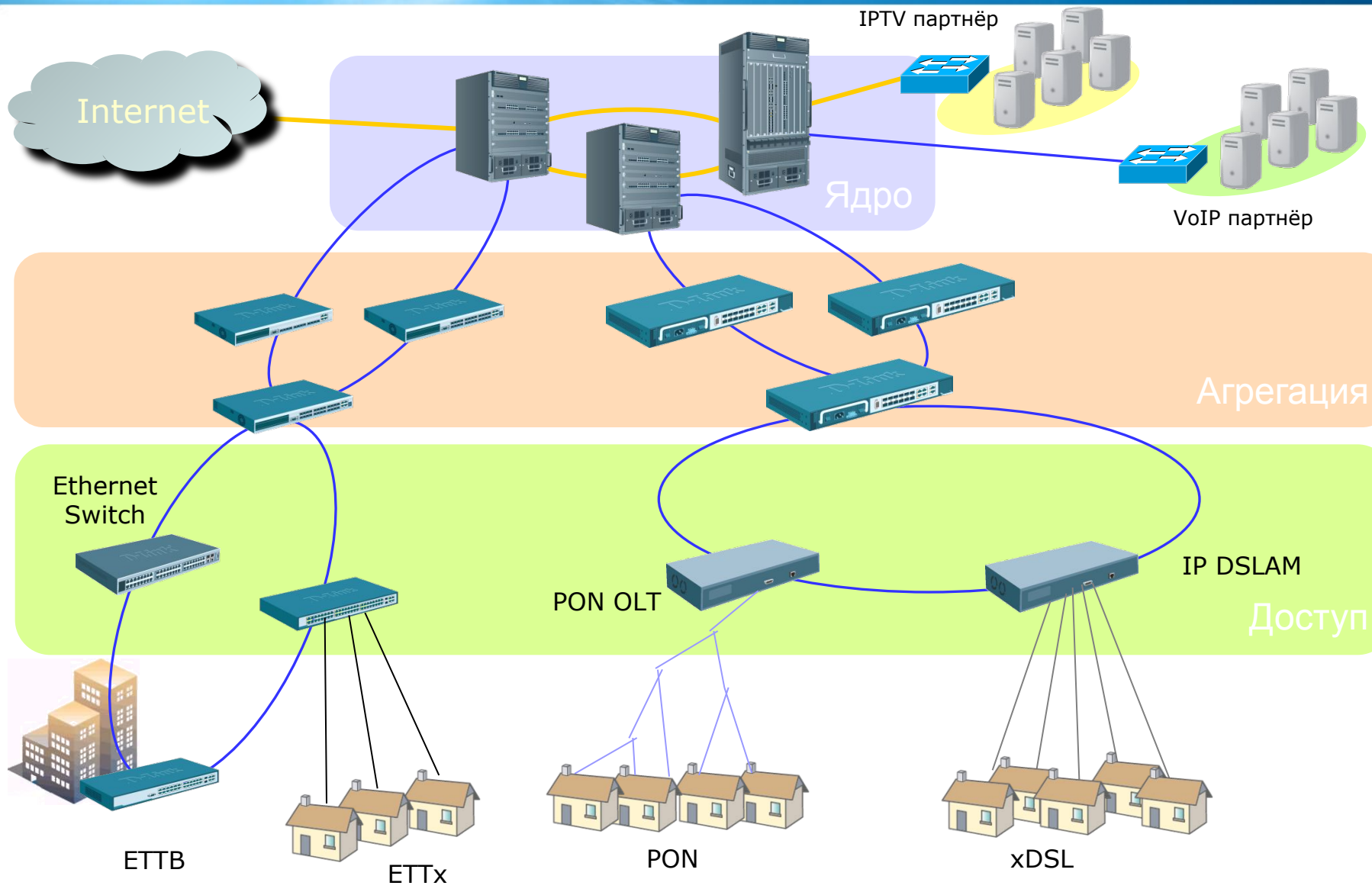
Настраиваемые коммутаторы (Smart) – данные коммутаторы имеют ограниченные возможности управления, чаще всего через Web-консоль иногда через telnet. Применяются в сетях SOHO, бюджетных решениях ISP-сетей (Internet Service Provider), в небольших корпоративных сетях. Отличаются небольшой стоимостью и легкостью настроек и интуитивно понятным интерфейсом.

Типы коммутаторов

Управляемые коммутаторы - коммутаторы, имеющие широкий набор функций управления и возможность получить максимально точные и необходимые настройки сети. Включающие в себя возможности управления через Web-интерфейс, через последовательный порт, с помощью сетевых консолей TELNET, SSH, протокола SNMP, имеют возможности удаленного мониторинга RMON. Область применения данных коммутаторов – ISP-сети, корпоративные сети средних и крупных предприятий и др.



Уровни организации сети



Уровень ядра сети

Уровень ядра сети (магистрали сети) отвечает за пропуск и быструю доставку сетевого трафика без задержек и потерь из одного региона агрегирования трафика в другой. Ввиду больших объемов трафика, его обработка (фильтрация, профилирование и т.п.) на уровне ядра, обычно, не выполняется.

В качестве коммутаторов ядра сети необходимо использовать маршрутизирующие коммутаторы, например DGS-6604 модульные шасси, либо стек из коммутаторов DGS-3600, DGS-3610 или DGS-3620.

Оба решения обладают полным функционалом уровня 3, а также функциями маршрутизации IP-трафика и протоколов многоадресной рассылки.

Использование маршрутизирующих коммутаторов существенно снижает нагрузку на устройство доступа в Интернет, а также позволяет ускорить коммутацию внутрисетевого трафика.

Уровень распределения

Выполняет следующие задачи:

- Объединение на одном узле соединений от нескольких коммутаторов уровня доступа.
- Внутрисетевая маршрутизация локального трафика, данные внутри сети не передаются на коммутатор/маршрутизатор ядра сети.
- При построении уровня распределения сети обычно используется топология «кольцо» - коммутаторы объединяются в кольцо по оптическому волокну на скорости 1 Гбит/с.

Уровень доступа

Уровень доступа предназначен для управления пользователями и рабочими группами при обращении к ресурсам объединенной сети.
Для уровня доступа характерны следующие функции:
Постоянный контроль (из уровня распределения) за доступом и политиками
Формирование независимых доменов конфликтов (сегментация)
Соединение рабочих групп с уровнем распределения

DGS-3420-XX – современное поколение гигабитных коммутаторов L2+ с встроенными портами 10G
Серия DGS-3120-XX - новое поколение коммутаторов агрегации/доступа L2 для сетей ISP и операторов связи
Коммутаторы Ethernet уровня доступа - серия Smart III

Виртуальные Локальные Сети - VLAN

VLAN — представляет собой группу компьютеров с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.
VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям, группироваться вместе, даже если они не находятся в одной физической сети.

- Трафик, включая и широковещательный, полностью изолирован на канальном уровне от других узлов сети.
- Повышению производительности сети, локализуя широковещательный трафик в пределах виртуальной сети и создавая барьер на пути широковещательного шторма.
- Обеспечение безопасности и разделения доступа к ресурсам

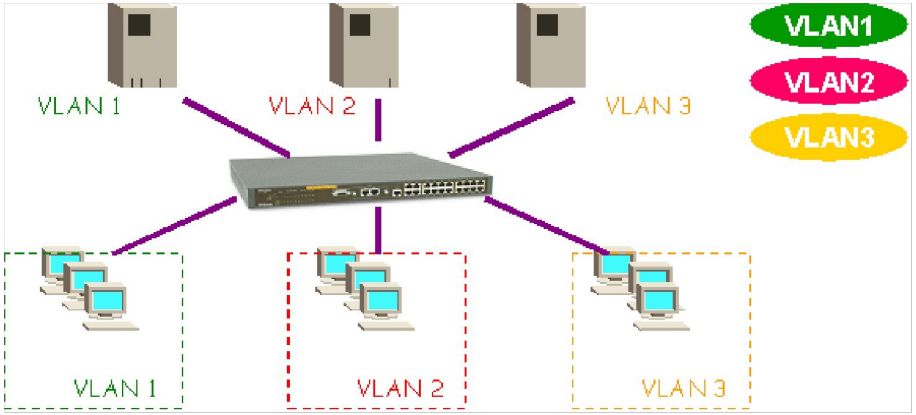
D-Link
Building Networks for People

Типы VLAN

- VLAN на базе портов
- VLAN на базе меток IEEE 802.1q
- VLAN на базе протоколов IEEE 802.1v

VLAN на основе портов

При использовании VLAN на основе портов, каждый порт назначается в определенную VLAN, независимо от того, какой пользователь или компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную.



Преимущества IEEE 802.1q VLAN

- Гибкость и удобство настройки и изменения
- Возможность работы протокола Spanning Tree
- Возможность работы с сетевыми устройствами, которые не распознают метки
- Устройства разных производителей, могут работать вместе
- Не нужно применять маршрутизаторы, чтобы связать подсети

Виртуальные Локальные Сети - VLAN

D-Link
Building Networks for People

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)

Маркированный кадр 802.1p/802.1Q

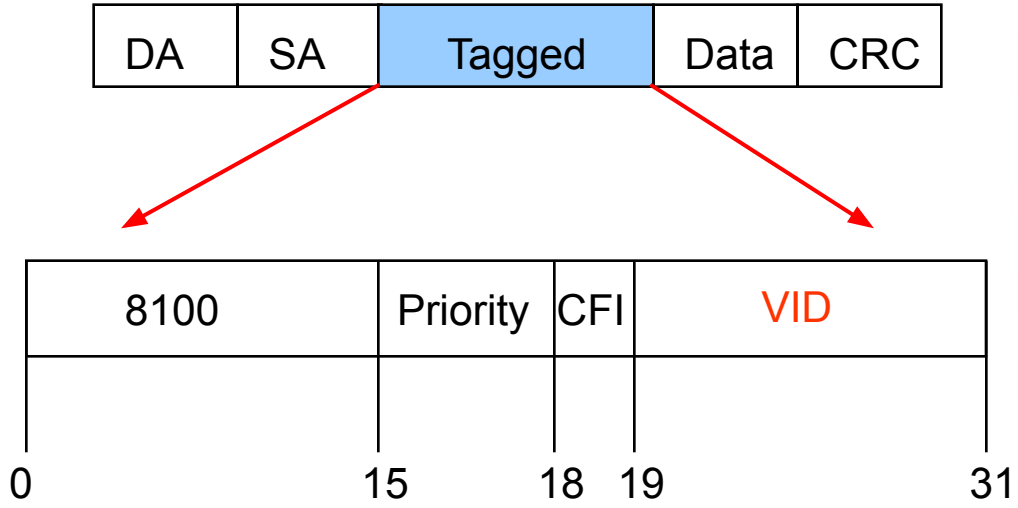
Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Данные (Data)	Контрольная последовательность кадра (CRC)

8100	Приоритет (Priority)	Индикатор канонического формата (CFI)	**Идентификатор VLAN (VID)**

Маркированные кадры-Tagged Frame

- 12-бит VLAN маркер
- Идентифицирует кадр, как принадлежащий VLAN

- Max. Размер маркированного кадра Ethernet 1522 байт
- Немаркированный кадр это кадр без VLAN маркера



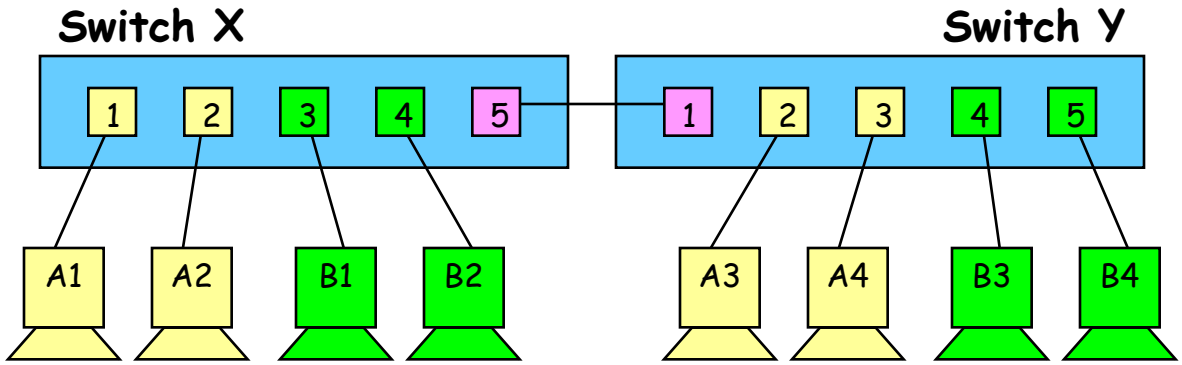
Виртуальные Локальные Сети - VLAN

Разделение сети, построенной на 2-х коммутаторах на две VLAN

VLAN A :
Computer A1, A2, A3 & A4

Switch X
VID : 2
Tag Egress : Port 5
Untag Egress : Port 1 & 2
Port 1 & 2 assign PVID = 2

Switch Y
VID : 2
Tag Egress : Port 1
Untag Egress : Port 2 & 3
Port 2 & 3 assign PVID = 2

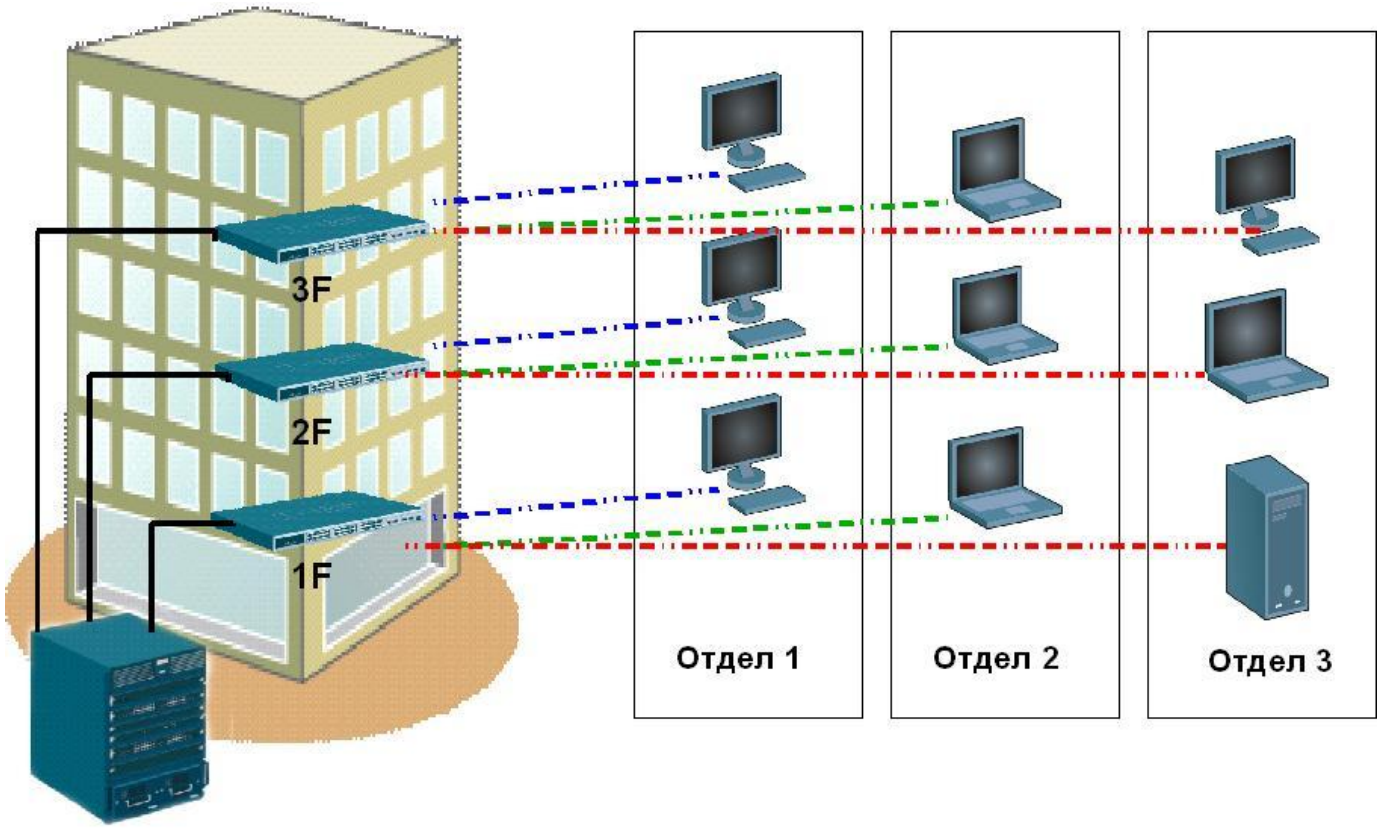


VLAN B : Computer B1, B2, B3 & B4

Switch X
VID : 3
Tag Egress : Port 5
Untag Egress : Port 3 & 4
Port 3 & 4 assign PVID = 3

Switch Y
VID : 3
Tag Egress : Port 1
Untag Egress : Port 4 & 5
Port 4 & 5 assign PVID = 3

Виртуальные Локальные Сети - VLAN



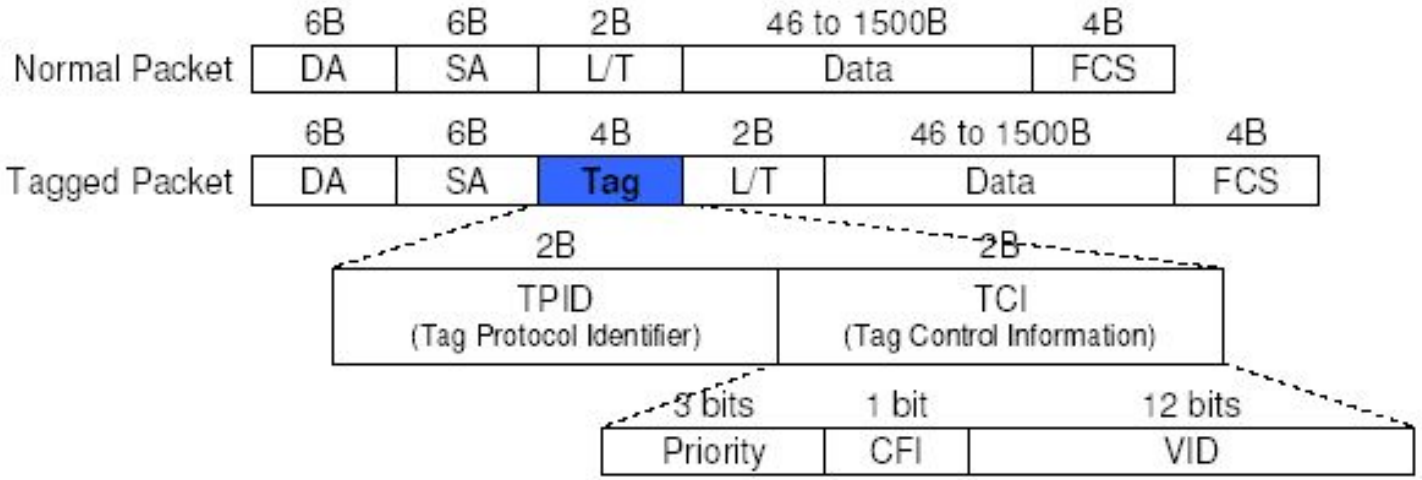
Приоритеты 802.1p и QoS – качество обслуживания

Протокол IEEE 802.1P

Стандарт IEEE 802.1p определяет приоритет пакета при помощи тэга в его заголовке. Можно задать до 8 уровней приоритета от 0 до 7. Уровень 7 определяет самый высокий приоритет.

Коммутаторы поддерживают 4 очереди Class of Service на каждом порту. Для маркированных пакетов приоритет может быть изменен на одну из четырех очередей CoS. Для немаркированных пакетов приоритет выставляется исходя из приоритета, выставленного на данном порту.

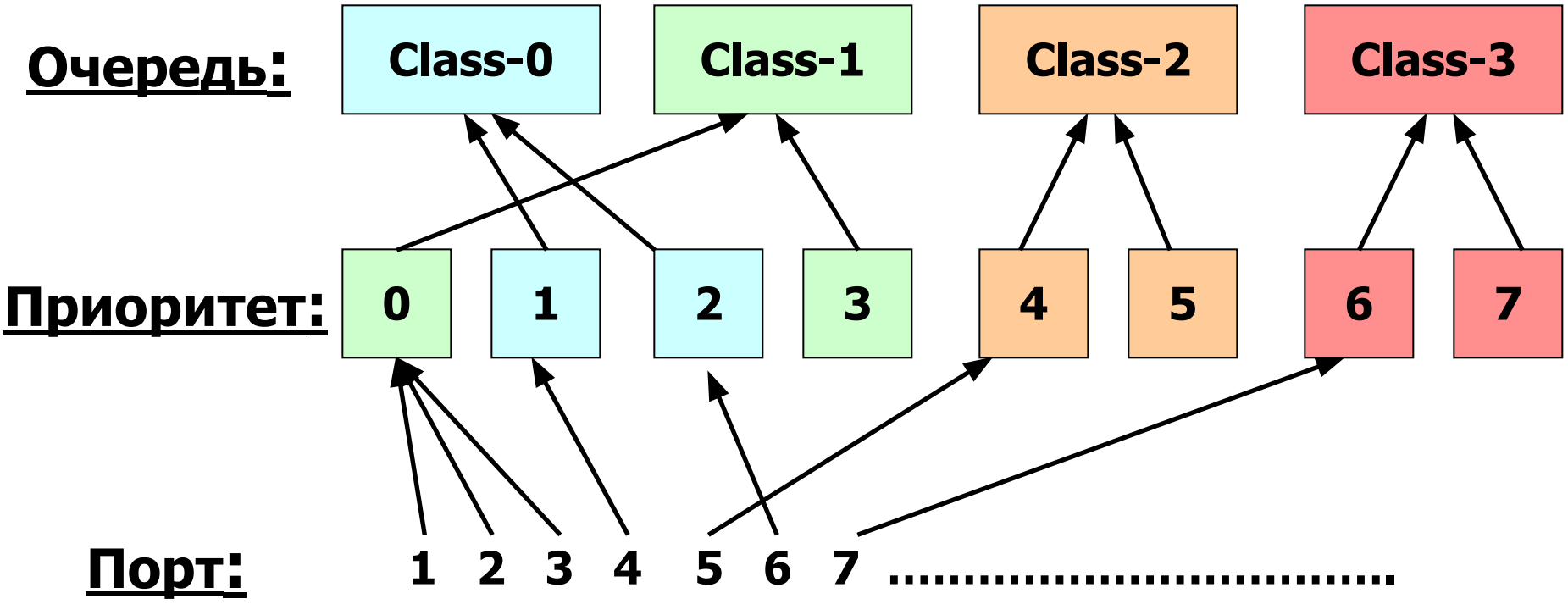
Протокол IEEE 802.1P



Внимание:
Несмотря на то, что поле приоритета 802.1p находится в теге стандарта IEEE802.1Q, 802.1p можно использовать и при отсутствии виртуальной локальной сети. Для этого значение идентификатора VID необходимо установить равным 0.

Как работает 802.1p

4 очереди приоритета



Классификация пакетов

Для обеспечения дифференцированного обслуживания трафика, коммутаторы поддерживают в зависимости от модели от 4 до 8 аппаратных очередей приоритетов на каждом из своих портов. Для обеспечения требуемой очередности передачи пакетов в коммутаторе необходимо настроить алгоритм обслуживания очередей и карту привязки приоритетов 802.1p, ToS, DSCP к очередям.

По умолчанию в коммутаторах D-Link используются следующие карты привязки пользовательских приоритетов 802.1p к очередям:

4 очереди приоритетов

Приоритет	Номер очереди
1	Q1
2	Q0
3	Q0
4	Q1
5	Q2
6	Q2
7	Q3
8	Q3

8 очередей приоритетов

Приоритет	Номер очереди
1	Q2
2	Q0
3	Q1
4	Q3
5	Q4
6	Q5
7	Q6
8	Q6

Обработка приоритетов - Строгий режим (Strict Priority)

Обработка приоритетов производится в соответствии с одним из методов, строгий или по весу.

При **строгом** методе, кадры в очередях с высоким приоритетом обрабатываются первыми. Только тогда, когда эти очереди пусты, могут быть обработаны кадры с более низким приоритетом. Кадры с высоким приоритетом всегда получают предпочтение независимо от количества кадров в других очередях в буфере и времени, прошедшего с момента передачи последнего кадра с низким приоритетом. По умолчанию коммутатор настроен как раз на этот режим.

Проблема: Пакеты в очередях с низким приоритетом могут долго не обрабатываться.

Обработка приоритетов – Взвешенный круговой режим (Weighted Round-Robin)

Для использования обработки приоритетов по весу, восемь очередей приоритета в коммутаторе могут быть сконфигурированы в взвешенном круговом режиме (***WRR***) так, чтобы кадры в буфере надолго не задерживались – обработка начинается с очереди с наивысшим приоритетом, потом переходит к более низкому и т.д., а в конце возвращается к наивысшему приоритету, и всё повторяется опять.
Такой режим исключает главный недостаток строгого режима. Очередь с минимальным приоритетом уже не страдают от переполнения, поскольку всем очередям предоставляется часть пропускной способности для передачи. Это достигается заданием максимального числа кадров, которые можно передать из данной очереди приоритетов, перед тем как перейти к следующей. Это устанавливает класс обслуживания (Class of Service (CoS)) для каждой из 8-ми очередей коммутатора.
Команда **config scheduling** может быть использована для настройки взвешенного кругового режима (***WRR***), который сокращает все 8 очередей приоритетов на коммутаторе. Для использования этой схемы, параметры *max_packets* не должны иметь значение *0*. Параметр **max_packet** задаёт максимальное количество кадров в определённой очереди, которое может быть передано за один раз (цикл). Это обеспечивает поддержку CoS, между тем даёт возможность передавать кадры из всех очередей. Это значение можно изменять в диапазоне от 0 до 15 кадров для каждой очереди приоритетов.

config scheduling <class_id 0-6> {max_packet <value 0-15>}

Протоколы «покрывающего дерева»
Spanning Tree Protocols

802.1d (STP)
802.1w (RSTP)
802.1s (MSTP)

Протокол Spanning Tree

Зачем нужен протокол Spanning Tree?

- Исключение петель
- Резервные связи

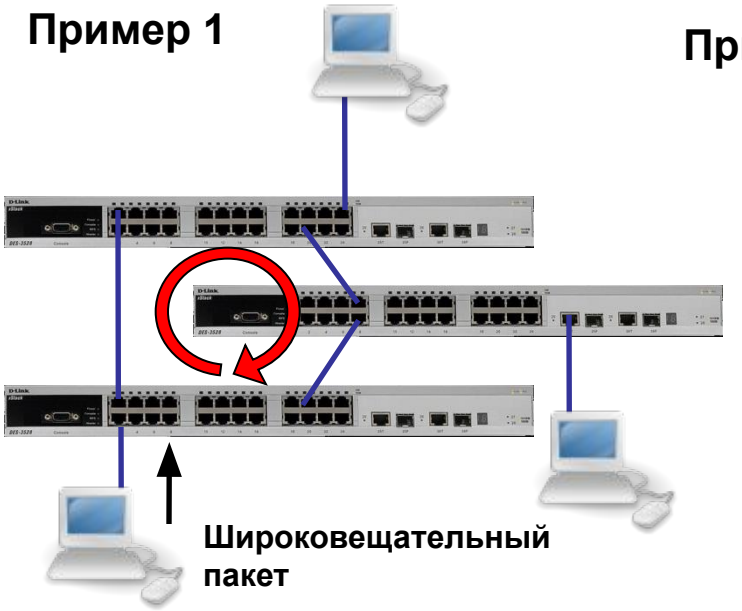
Версии:

- IEEE 802.1d Spanning Tree Protocol, STP
- IEEE 802.1w Rapid Spanning Tree Protocol, RSTP
- IEEE 802.1s Multiple Spanning Tree Protocol, MSTP

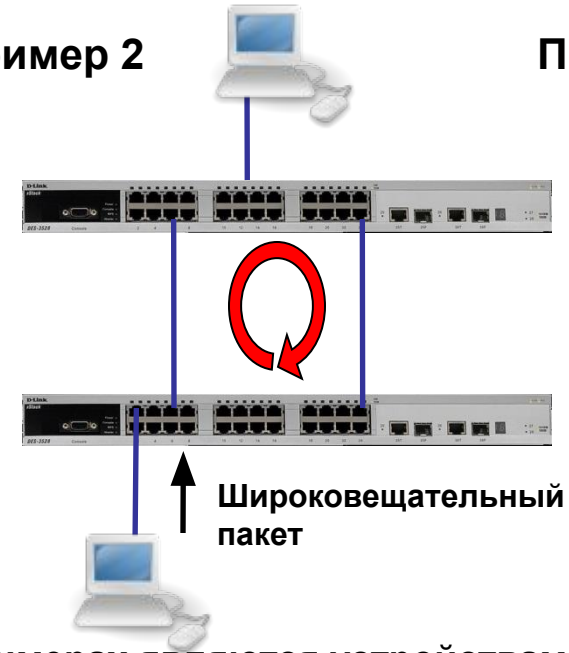
Что такое сетевая петля L2

Коммутаторы (L2), объединённые в кольцо, образуют одну или несколько сетевых петель

Пример 1



Пример 2

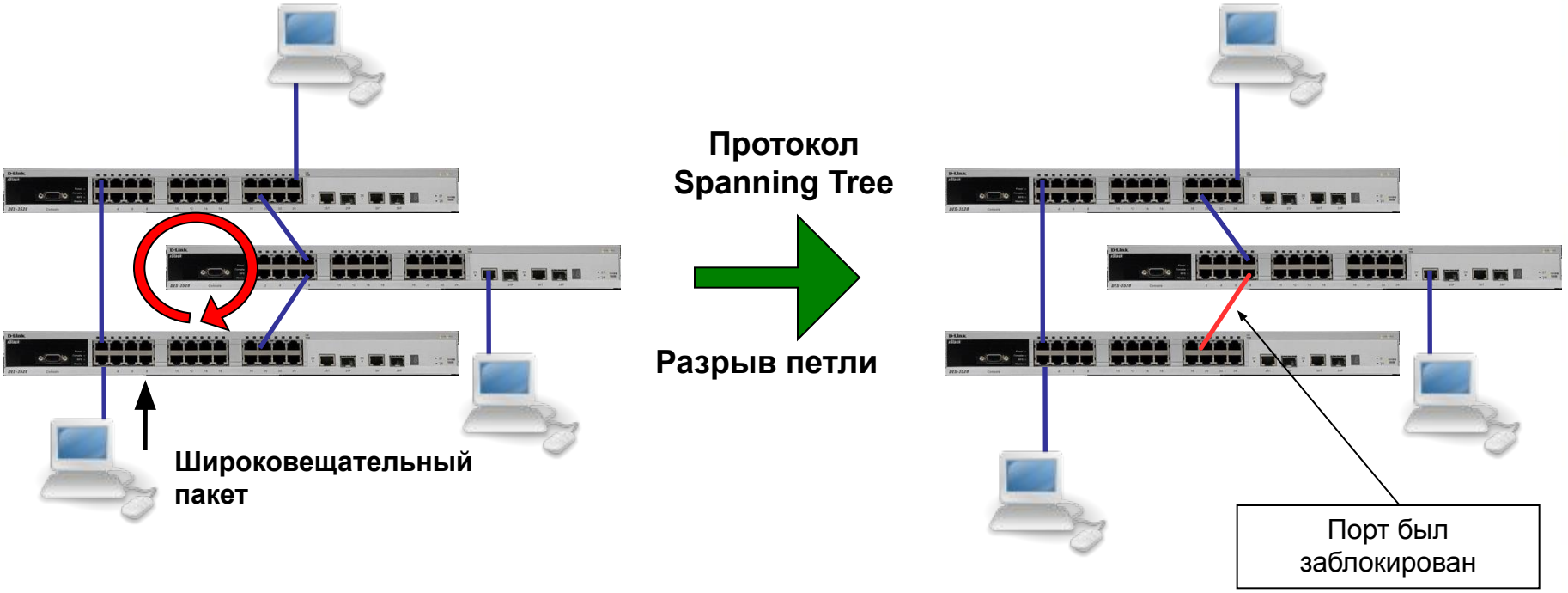


Пример 3

Примечание: Коммутаторы в этих примерах являются устройствами L2, VLAN на них не настроены, и протокол Spanning Tree не включен.

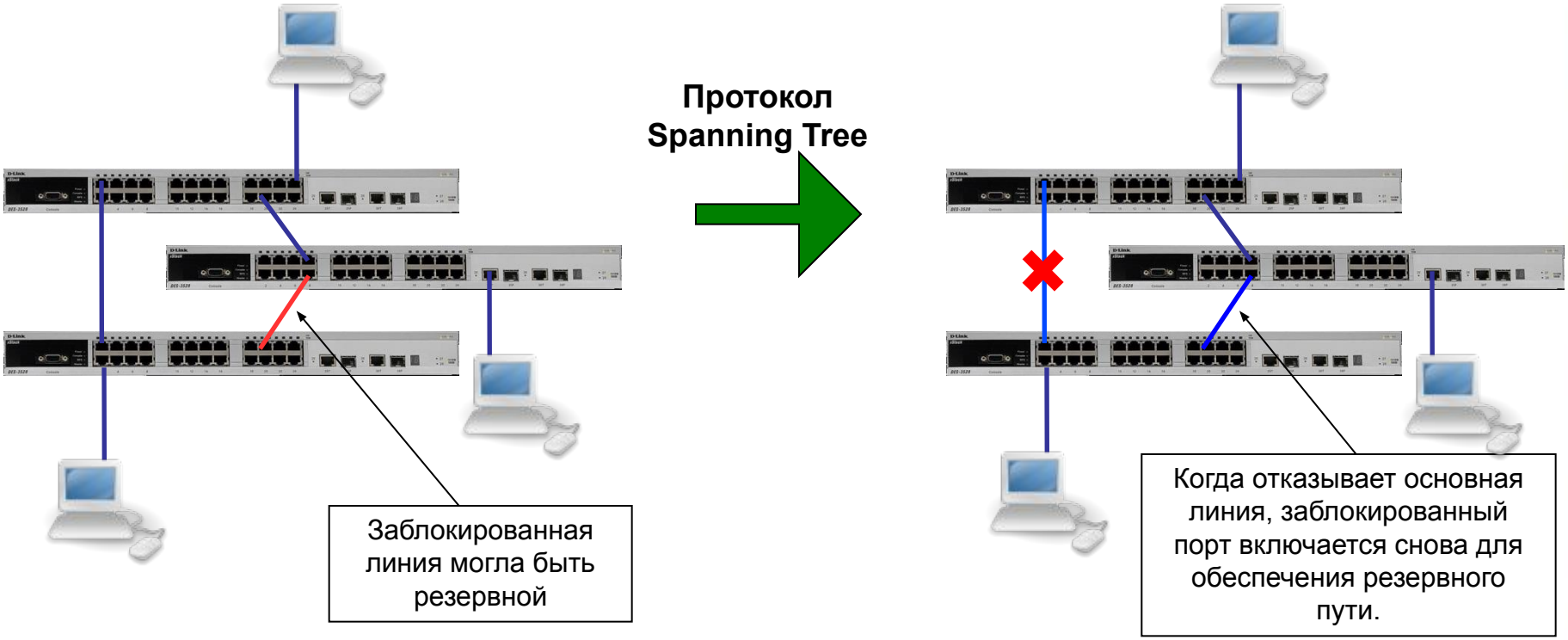
Проблема: В сети L2 Ethernet не допускаются петли. Если они есть, то это может вызвать Широковещательный шторм (Broadcast Storm).

Исключение петель



Решение: Протокол Spanning Tree (STP, RSTP, MSTP) может исключить петлю или петли.

Резервная(ые) связь(и)



Если происходит отказ основной линии, протокол Spanning Tree может включить заблокированный порт для обеспечения резервного пути.

Пакеты BPDU содержат информацию для построения топологии сети без петель

Пакеты BPDU помещаются в поле данных кадров канального уровня, например, кадров Ethernet. Они содержат несколько полей, определяющих работу STP. Среди них наиболее важные:

- Идентификатор коммутатора
- Расстояние до корневого коммутатора
- Идентификатор порта

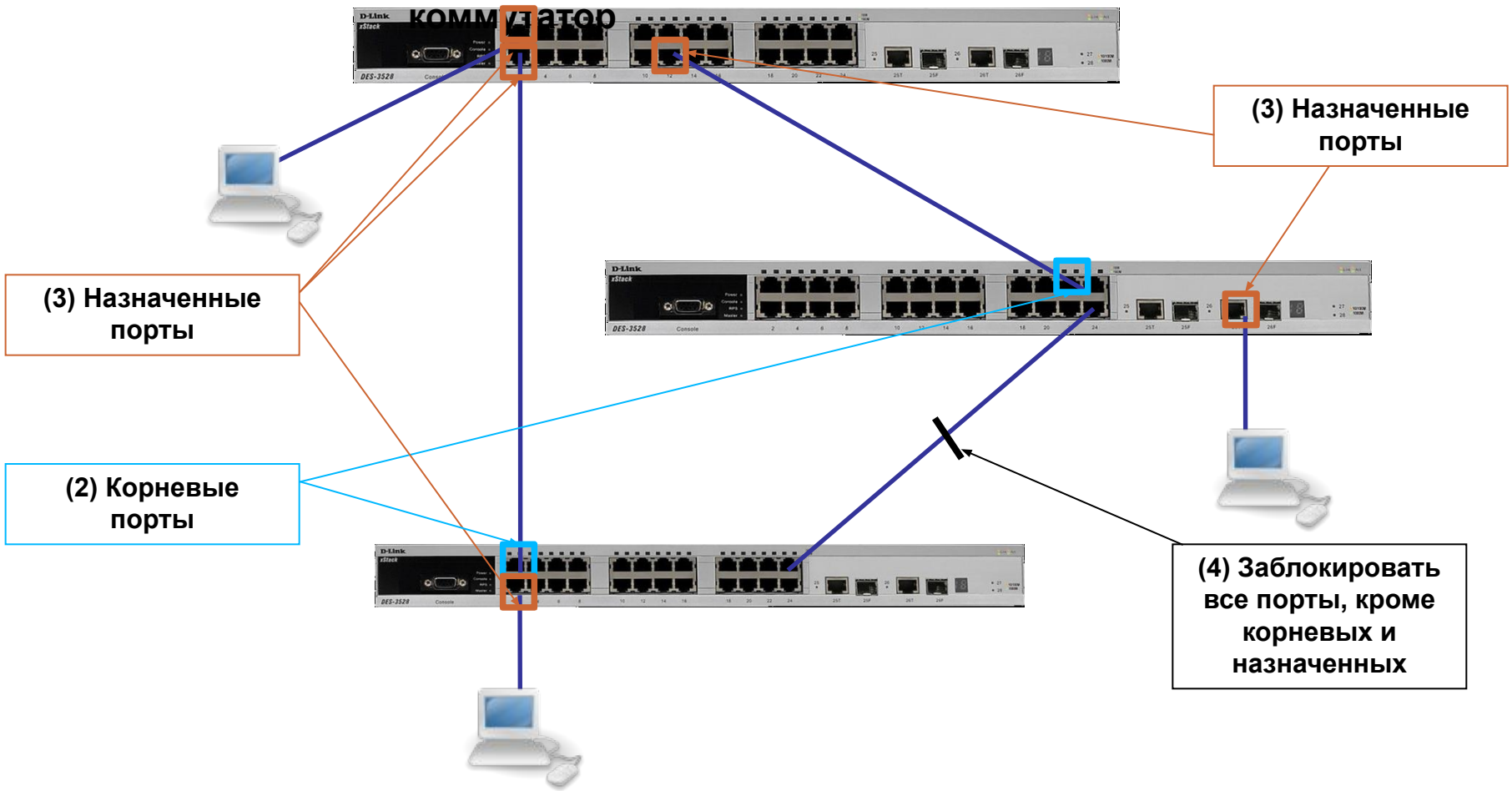
IEEE 802.1d, STP

D-Link
Building Networks for People

Как работает STP (802.1d):

1. Выбирается Корневой коммутатор (*Root Bridge)*. Коммутатор с наименьшим ID становится корневым. Он должен быть один в коммутируемой сети LAN.
2. Определяется Корневой порт (*Root Port)* для каждого коммутатора. Порт коммутатора с наименьшим значением Стоимости пути до корневого коммутатора (Root Path Cost) назначается корневым портом. Он должен быть один у каждого коммутатора.
3. Определяется Назначенный порт (*Designated Port)* для каждого сегмента LAN. Порт, по которому значение стоимости пути до корневого коммутатора для сегмента LAN минимально, выбирается назначенным для данного сегмента. Каждый сегмент LAN иметь только один назначенный порт.
4. Блокируются все порты, не являющиеся корневыми или назначенными.

Как работает STP



Недостатки STP

Основной недостаток 802.1d STP:

Большое время сходимости. Протоколу STP (802.1d) обычно для этого требуется от 30 до 60 секунд.

Решение:

IEEE 802.1w: Протокол Rapid Spanning Tree, RSTP.

Протокол Rapid Spanning Tree, RSTP

D-Link
Building Networks for People

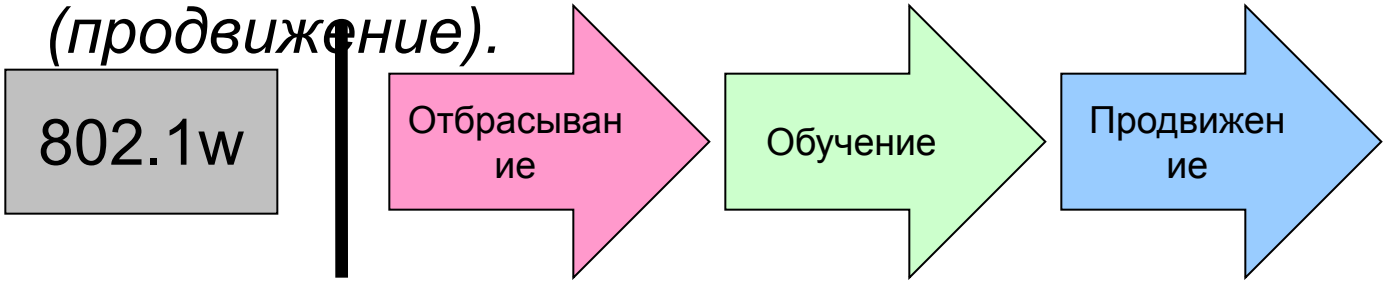
- Стандартизирован IEEE 802.1w

  Обеспечивает серьёзный прирост скорости сходимости коммутируемой сети моментальным переводом корневых и назначенных портов в состояние продвижения кадров

Состояния портов

- В стандарте 802.1d определено 4 различных состояния портов: *blocking (заблокирован), listening (прослушивание), learning (обучение), и forwarding (продвижение).*

- В стандарте 802.1w определено 3 различных состояния портов 802.1w: *discarding (отбрасывание), learning (обучение), и forwarding (продвижение).*



Соответствие состояния портов между 802.1d и 802.1w

STP (802.1d) Состояние порта	RSTP (802.1w) Состояние порта	Порт входит в активную топологию?	Порт изучает MAC-адреса?
Отключён	Отбрасывание	Нет	Нет
Заблокирован	Отбрасывание	Нет	Нет
Прослушивание	Отбрасывание	Нет	Нет
Обучение	Обучение	Нет	Да
Продвижение	Продвижение	Да	Да

Роли портов

- Роли корневых портов
- Роли назначенных портов
- Роли альтернативных портов
- Роли резервных портов

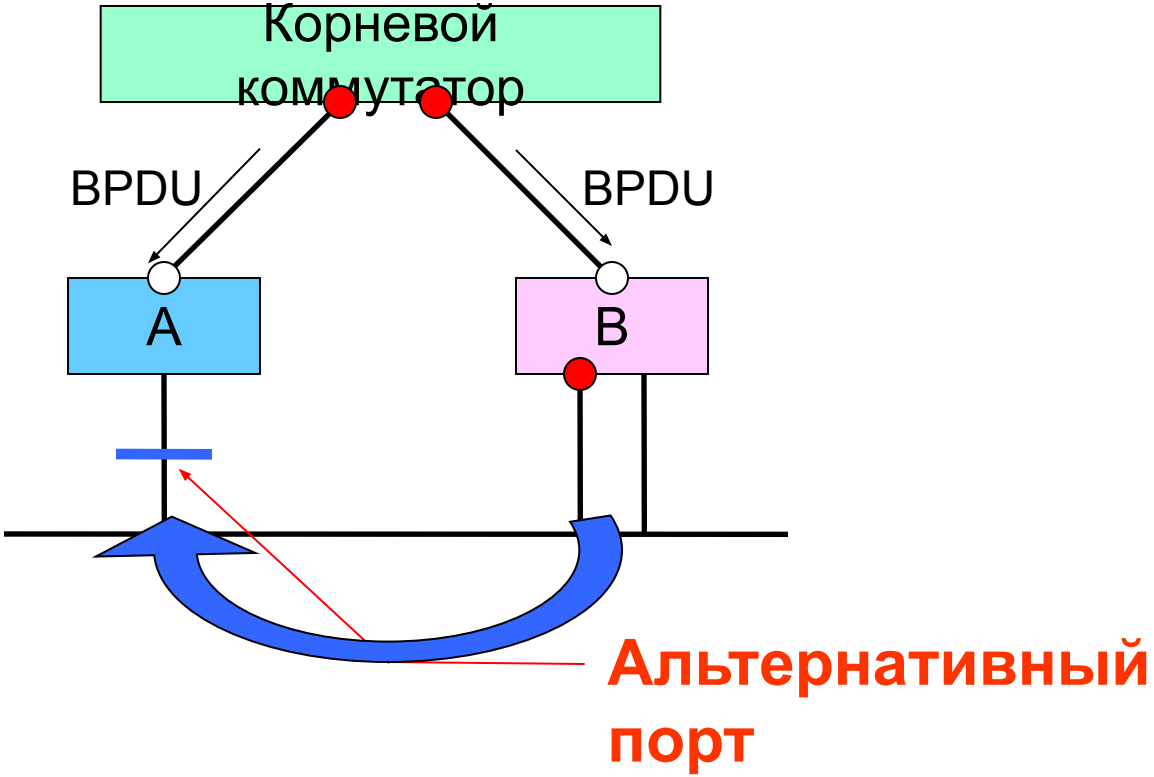
Роли портов

- Роли альтернативных и резервных портов
  - Эти две роли соответствуют заблокированному состоянию по стандарту 802.1d.
  - Для заблокированного порта важнее получать BPDU, чем отсылать их в свой сегмент. Порту необходимо получать BPDU для того, чтобы оставаться заблокированным. В RSTP есть для этого две роли.

Роли портов

- Роли альтернативных портов

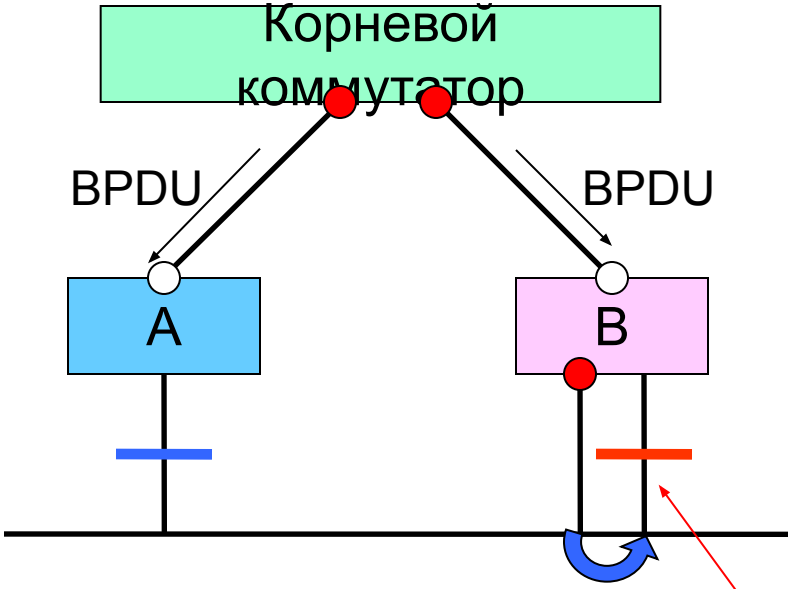
Альтернативный порт – это порт заблокированный в результате получения более предпочтительных BPDU от другого коммутатора.



Роли портов

- Роли резервных портов

Резервный порт – это порт заблокированный в результате получения более предпочтительных BPDU от того же самого коммутатора, которому он принадлежит.



Резервный порт

Роли портов

- Роли альтернативных и резервных портов в протоколе RSTP
  - Альтернативный порт – порт, который может заменить корневой порт при выходе его из строя
  - Резервный порт – порт, который может заменить назначенный порт при выходе его из строя
  - При отказе корневого порта, RSTP-коммутатор может практически сразу переключить альтернативный порт в корневой порт
  - При выходе из строя назначенного порта, резервный порт может быть также быстро переведён в назначенный

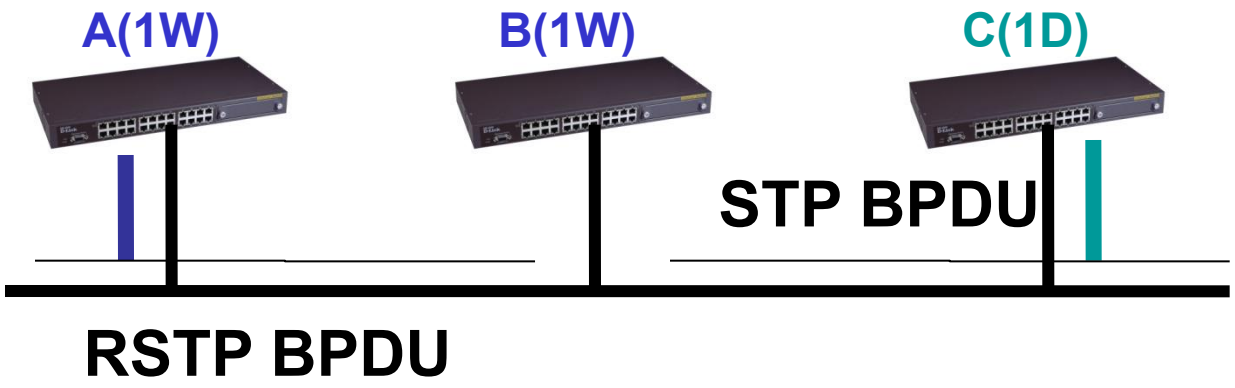
Быстрый перевод портов в состояние продвижения

Новый протокол RSTP позволяет перевести порт в состояние продвижения кадров без учёта каких-либо таймеров. Таким образом появился реальный механизм обратной связи для совместимых с протоколом RSTP устройств. Для обеспечения быстрой сходимости сети, протокол оперирует двумя понятиями – пограничные порты и тип линии.

1. Пограничные порты
   - **Все порты, к которым напрямую подсоединены рабочие станции не могу создать петель в сети и, соответственно, могут быть переведены в состояние продвижения практически сразу без перехода в состояния прослушивания и обучения.**
1. Тип линии (точка-точка или разделяемая)
   - **Порт функционирующий в режиме полного дуплекса рассматривается как соединение точка-точка.**
   - **Порт в режиме полудуплекса воспринимается, по умолчанию, как разделяемое соединение.**
   - **Быстрая сходимость сети достигается на соединениях точка-точка.**

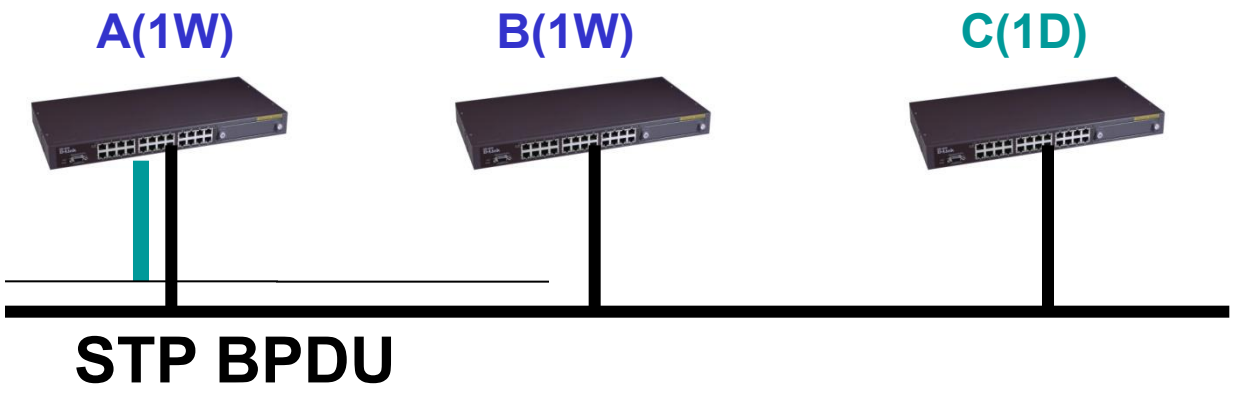
Совместимость с 802.1d

Например, коммутаторы A и B на схеме поддерживают RSTP, и коммутатор A является выделенным для данного сегмента. Устаревший коммутатор C, поддерживающий только STP также присутствует в сети. Так как коммутаторы 802.1d игнорируют RSTP BPDU и отбрасывают их, C считает, что в сегменте нет других коммутаторов и начинает посылать его BPDU формата 802.1d.



Совместимость с 802.1d

Коммутатор A получает эти BPDU и, максимум через два интервала Hello (таймер задержки переключения), изменяет режим на 802.1d только на этом порту. В результате, C может теперь понимать BPDU A и соглашается с тем, что A является выделенным коммутатором для данного сегмента.



Таймеры протокола STP

Существует несколько таймеров STP:

- **hello:** Интервал hello – это время между Bridge Protocol Data Unit (BPDU), отсылаемыми с портов коммутатора. По умолчанию это 2 секунды, но может быть задан в диапазоне от 1 до 10 секунд.
- **forward delay:** Forward delay (задержка продвижения) это время в двух состояниях – прослушивание и обучение. По умолчанию это 15 секунд, но может быть настроена в диапазоне от 4 до 30 секунд.
- **max age**: Max age (максимальное возраст) – таймер, контролирующий время, в течение которого порт коммутатора хранит информацию о конфигурации BPDU. Это 20 секунд по умолчанию и может быть изменено в диапазоне от 6 до 40 секунд.

Эти три параметра содержатся в каждом BPDU конфигурации. Также есть дополнительный временной параметр в каждой конфигурации BPDU, известный как Возраст сообщения (Message Age). Возраст сообщения это не фиксированная величина. Она представляет собой временной интервал с момента первой посылки BPDU корневым коммутатором. Корневой коммутатор будет посылать все свои BPDU с возрастом сообщения равным нулю, и все другие коммутаторы на пути BPDU будут добавлять к нему 1. В реальности, этот параметр означает как далеко Вы находитесь от корневого коммутатора, получая этот BPDU.

Максимальный диаметр сети

Разница между 802.1d и 802.1w заключается в том, как инкрементируется параметр Возраст Сообщения. В 802.1d Возраст Сообщения – это счётчик, поддерживаемый корневым портом коммутатора и инкрементируемый им на 1. В 802.1w, значение инкрементируется на величину большую 1/16 Максимального Возраста но меньшую 1, округлённую до ближайшего целого.

Предельный диаметр сети достигается, когда:
((MessageAge+HelloTime)>=MaxAge)

Например, при умолчальных значениях MaxAge(20 с) и Hello (2 с), максимальный диаметр сети равен 18 переходам от корневого коммутатора, тем самым обеспечивая 37 коммутаторов в цепочке или кольце, при условии, что корневой коммутатор находится в центре.

Общие выводы: STP и RSTP

- Сходимость:

STP, 802.1d: 30 с.
RSTP, 802.1w: 2-3 с.

- Диаметр:

STP, 802.1d: 7 переходов
RSTP, 802.1w: 18 переходов

- 802.1w обратно совместим с 802.1d. Тем не менее, преимущество быстрой сходимости будет утеряно.

Ограничение RSTP

Ограничение RSTP:
В сети может быть только одна копия **Spanning Tree** (одно дерево). Если на коммутаторе сконфигурировано несколько VLAN, то все они используют одну копия этого протокола. Это значит, что все VLAN образуют одну логическую топологию, не обладающую достаточной гибкостью. Этот протокол не может поддерживать своё «дерево» для каждого VLAN.

Решение: Протокол Multiple Spanning Tree, MSTP (IEEE 802.1s)

Протокол Multiple Spanning Tree, MSTP

D-Link
Building Networks for People

- Стандартизирован IEEE 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.
- Также MSTP предоставляет возможность распределения нагрузки.
- Каждая копия (покрывающее дерево) MSTP также использует протокол RSTP для более быстрой сходимости сети.

Регионы MSTP

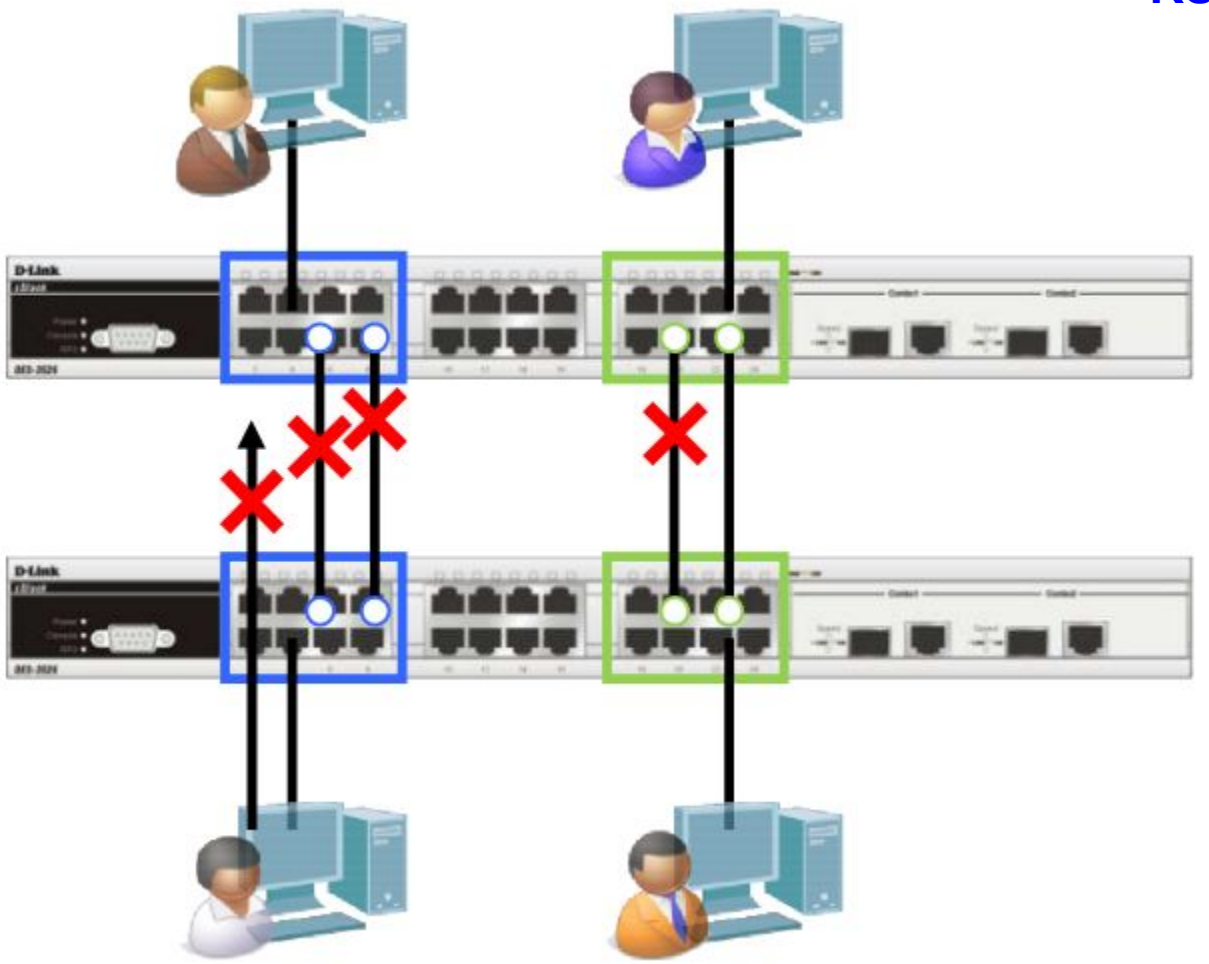
- Регион MSTP это связанная группа коммутаторов с поддержкой MSTP с одинаковой конфигурацией MST.

- Преимущества MSTP могут быть использованы только внутри региона. В разных регионах используется только одна копия STP для всех VLAN.

- Для того, чтобы добиться одинаковой конфигурации MST нужно задать следующие одинаковые параметры:
  1. Конфигурационное имя
  2. Конфигурационный номер ревизии
  3. Карту привязки VLAN к копиям STP

Пример работы MSTP

RSTP



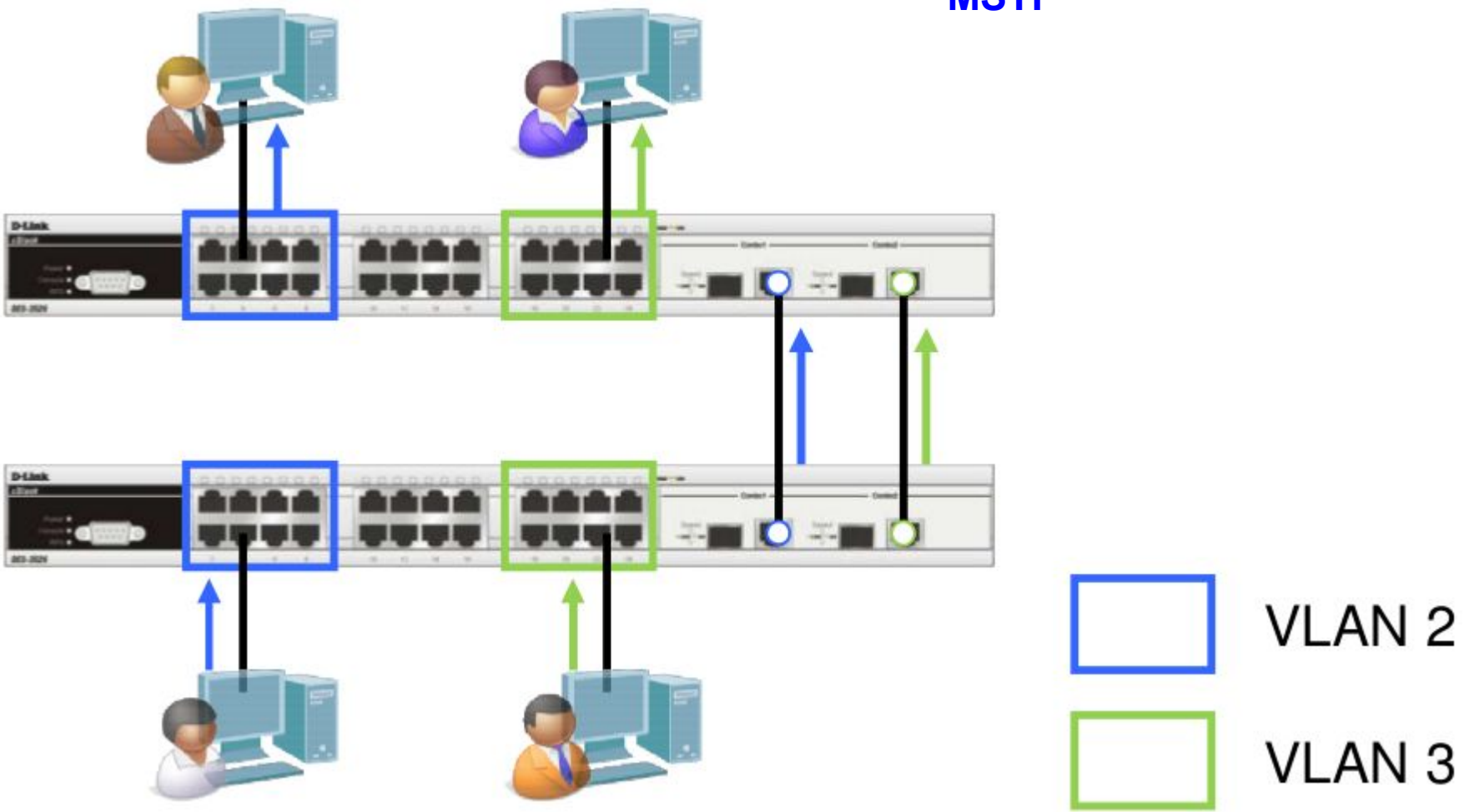
VLAN 2

VLAN 3

Пример работы MSTP

- 802.1S решает поставленную задачу:
- Если назначить VLAN 2 на копию MSTP под номером 2, а VLAN 3 сопоставить с копией 3.
- Т.о. получится две независимых топологии дерева STP.
- 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



Агрегирование портов

Статическое
802.3ad LACP

Агрегирование портов

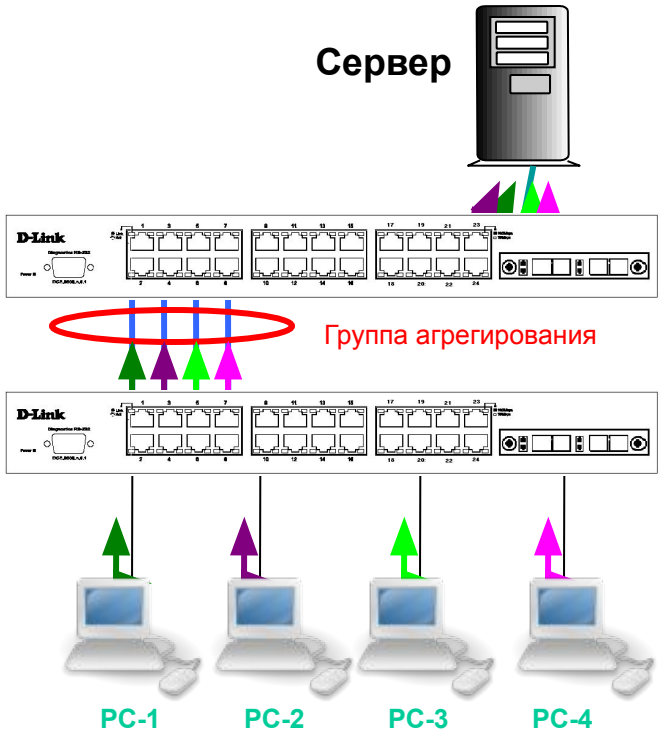
Агрегирование портов используется для объединения некоторого количества портов вместе для организации одного канала с высокой пропускной способностью. Такие порты называются членами группы агрегирования, а один из портов назначается мастером группы (**master port)**.

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.

DES-3226S поддерживает группы агрегирования, каждая из которых может содержать от 2-ух до 8-ми портов, кроме группы агрегирования Gigabit, которая состоит из 2-ух (дополнительных) портов Gigabit Ethernet на модуле расширения.

Агрегирование портов - Пример

В сети есть 4 клиентских PC с доступом к общему серверу. Трафик может быть разделён по 4-м агрегированным портам, посредством алгоритмов распределения нагрузки на основе MAC-адресов.



Описание:

Трафик между PC-1 и сервером через первый агрегированный порт.
Трафик между PC-2 и сервером через второй агрегированный порт.
Трафик между PC-3 и сервером через третий агрегированный порт.
Трафик между PC-4 и сервером через четвёртый агрегированный порт.

Два метода агрегирования портов

1. **Статический**
   (поддерживался первыми коммутаторами D-Link)
1. **IEEE 802.3ad**
   LACP, динамический (новый)

Статическое агрегирование портов по сравнению с LACP

Протокол управления агрегированным каналом – Link Aggregation Control Protocol IEEE 802.3ad (LACP) используется для организации динамического агрегированного канала между коммутаторам и другим сетевым устройством. Для статических агрегированных каналов (по умолчанию они являются статическими) соединяемые коммутаторы должны быть настроены вручную, и они не допускают динамических изменений в агрегированной группе. Для динамических агрегированных каналов (назначенные LACP-совместимые порты) коммутаторы должны быть совместимы с LACP для автосогласования этих каналов. Динамический агрегированный канал обладает функцией автосогласования, если с одной стороны агрегированная группа настроена как активная (active), а с другой – как пассивная (passive).

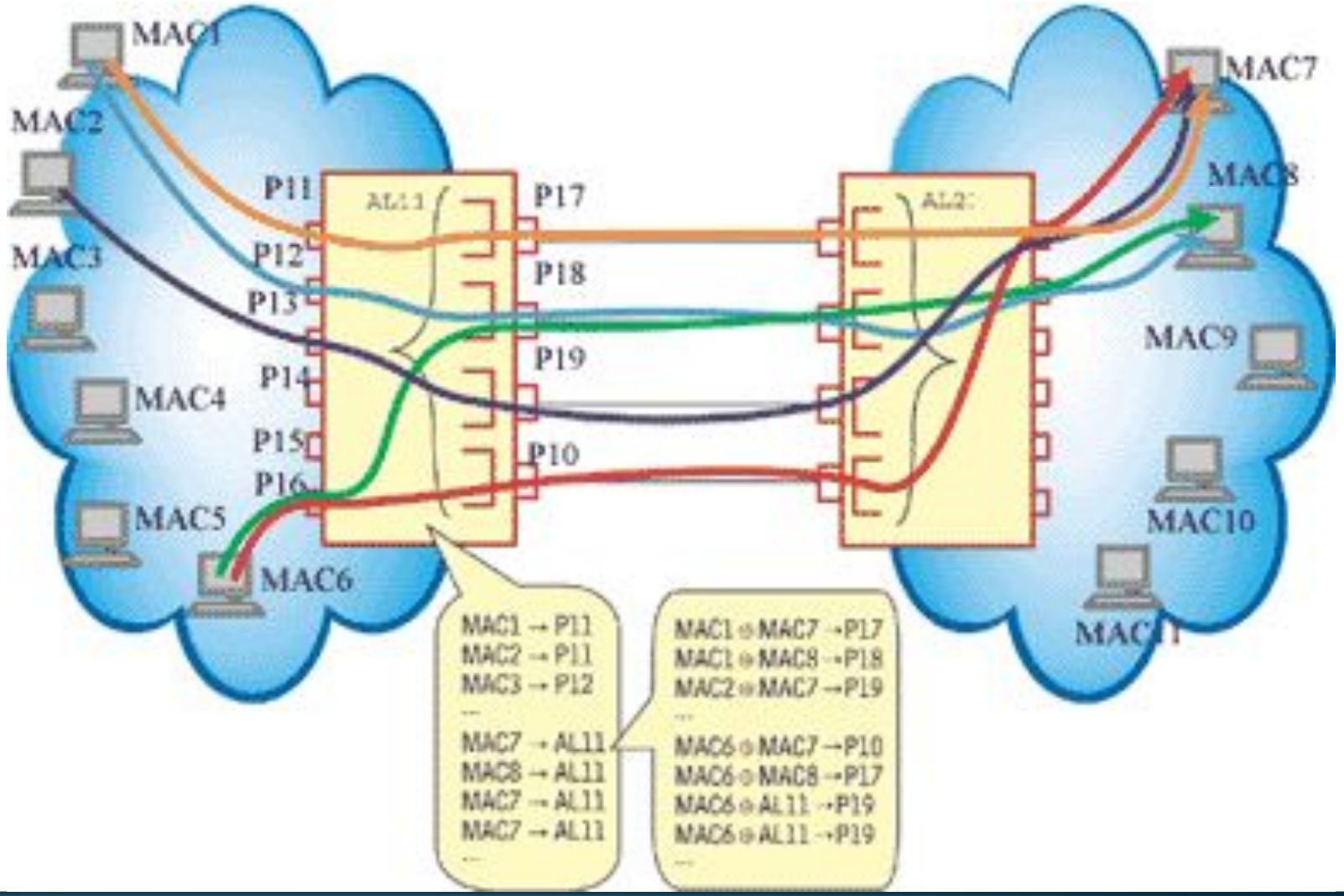
Если тип канала явно не указан, то это статическое агрегирование. Агрегированные порты могут быть либо *LACP* либо *Static*. LACP означает, что порты совместимы с LACP, т.е. могут быть подключены только к LACP-совместимому устройству. Порты в статической группе не могут динамически менять конфигурацию, и оба устройства, соединённые посредством такой группы, должны быть настроены вручную, если меняется состав группы и т.д.

Алгоритм агрегирования каналов

Этот алгоритм (на каждом устройстве) применяется для определения того, какой порт в группе используется для передачи определённых пакетов. Существует 6 алгоритмов. По умолчанию это MAC-source.

1. mac_source (по MAC-адресу источника)
2. mac_destination (по MAC-адресу назначения)
3. mac_source_dest (по MAC-адресам источника и назначения)
4. ip_source (по IP-адресу источника)
5. ip_destination (по IP-адресу назначения)
6. ip_source_dest (по IP-адресу источника и назначения)

Распределение потоков по каналам транков



Замечания:

1. Если на одном конце канала настроен LACP, на втором конце тоже должен быть LACP. Если с одной стороны LACP, а с другой статическая группа – канал работать не будет.
2. Если коммутатор, поддерживающий 802.3ad, должен быть соединён по агрегированному каналу с коммутатором, поддерживающим только статическое агрегирование, он должен быть тоже настроен в статическом режиме.
3. Если устаревший коммутатор D-Link, должен работать по агрегированному каналу с коммутатором Cisco, то коммутатор Cisco должен быть сконфигурирован в режиме “802.1q trunk” (например, Cisco 3600).

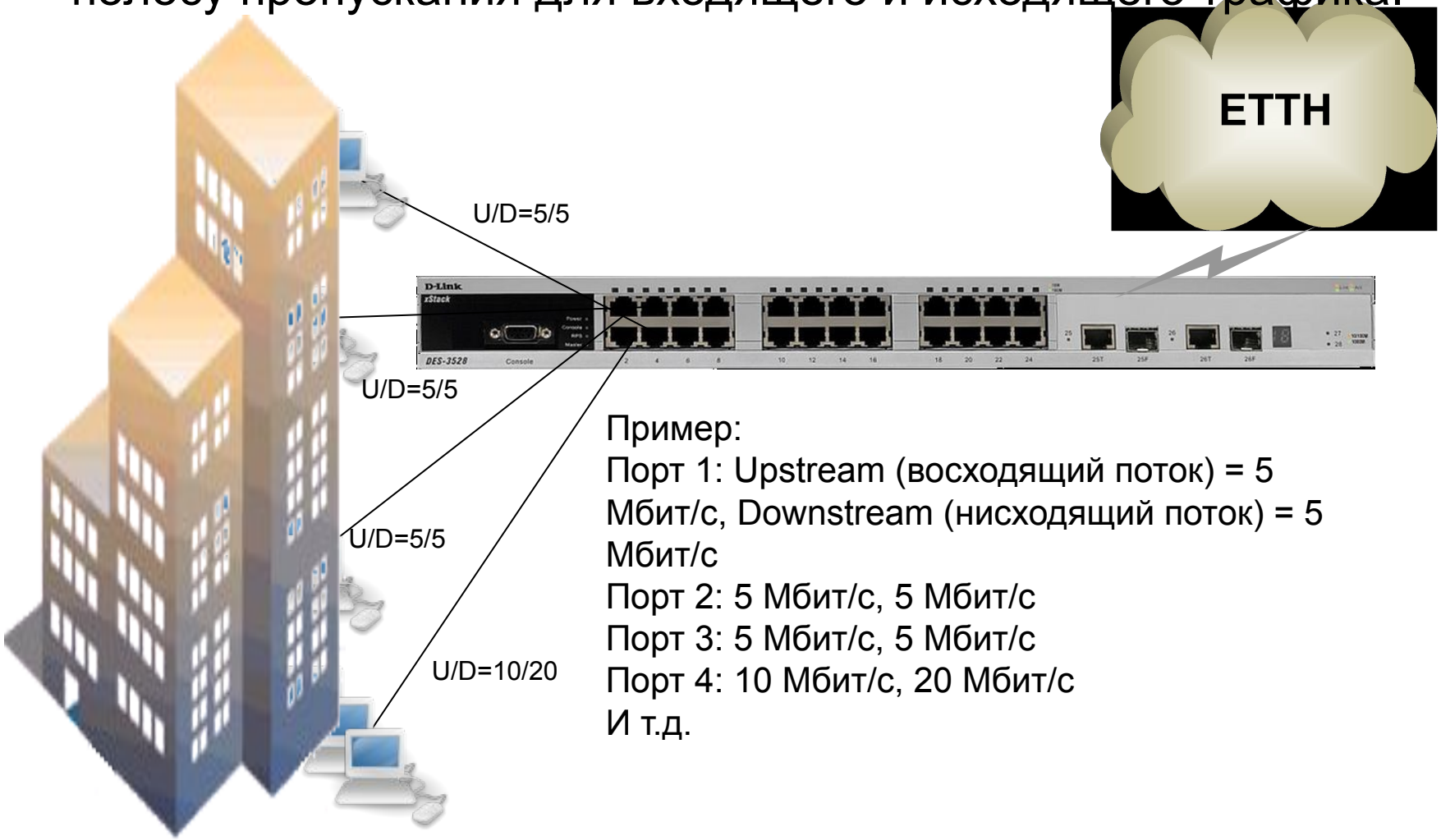
Контроль полосы пропускания

Шаг настройки полосы пропускания на коммутаторах D-Link

Модель коммутатора	Шаг полосы пропускания на портах 100Base-TX	Шаг полосы пропускания на портах 1000Base-T
	1 Мбит/с	8 Мбит/с
D  4XX, 28/52, DGS-31XX	64 Кбит/с	64 Кбит/с
	64 Кбит/с: до 2 Мбит/с 1 Мбит/с: от 2 Мбит/с до 100 Мбит/с	8 Мбит/с

Контроль полосы пропускания

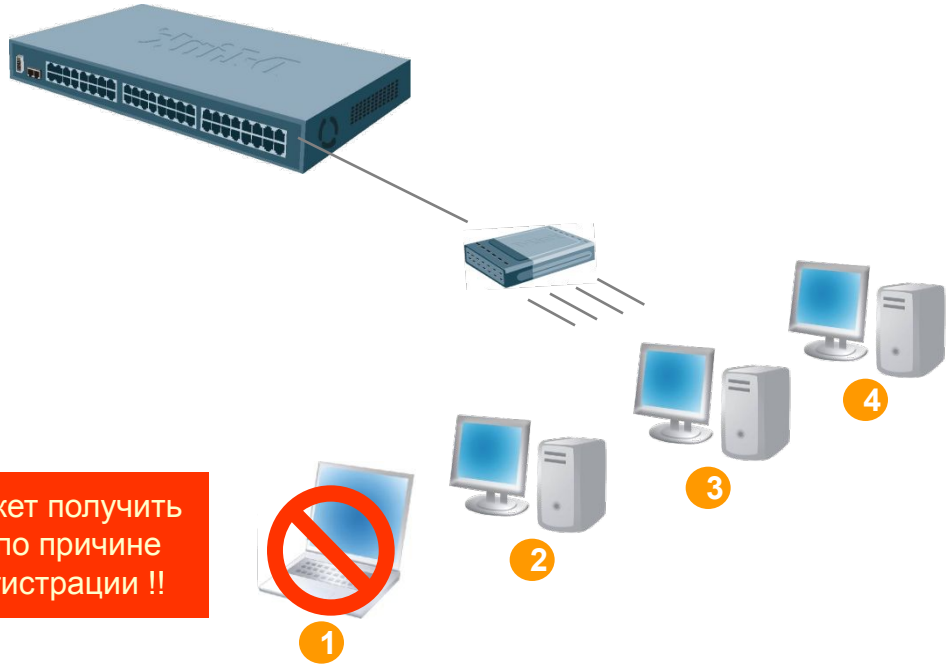
Для каждого порта Ethernet, допускается ограничивать полосу пропускания для входящего и исходящего трафика.



Пример:
Порт 1: Upstream (восходящий поток) = 5 Мбит/с, Downstream (нисходящий поток) = 5 Мбит/с
Порт 2: 5 Мбит/с, 5 Мбит/с
Порт 3: 5 Мбит/с, 5 Мбит/с
Порт 4: 10 Мбит/с, 20 Мбит/с
И т.д.

Port security

Функция *port security* позволяет определить, какое количество и какие MAC-адреса будут обслуживаться на определённом порту. При включении этой функции, коммутатор запомнит от 1 до N MAC-адресов и будет обслуживать на этом порту только их. Это позволяет количество пользователей за портом коммутатора



Всё ещё не может получить доступ к сети по причине отсутствия регистрации !!

Превышено количество допустимых компьютеров. Поэтому не может получить доступ к сети !

Storm control

При превышении заданного количества пакетов на порту включается режим ограничения.
Причины – через мерная активность пользователя, например torrent вирусы и т.д. и т.п.

Режимы работы:
Drop – пакеты при превышении порога отбрасываются
Shutdown – порт отключается при превышении порога, и периодически включается для проверки изменения ситуации.

D-Link®
Building Networks for People

Спасибо!

Владимир Музыка
D-Link Россия, Краснодар
Региональный представитель
vmuzyka@dlink.ru