Специальность: 09.02.02 «Компьютерные сети»

Дисциплина:

«Выполнение работ по одной или нескольким профессиям рабочих,должностям служащих» (3курс, 5 семестр)

Коммутаторы

Конспект лекций

Лекция 1
Назначение коммутаторов

Коммутаторы — это устройства, используемые для соединения нескольких устройств в одном локальном сегменте сети.

Коммутаторы локальной сети отвечают за направление потока данных и управление им на уровне доступа к сетевым ресурсам.

Коммутаторы обеспечивают сегментацию локальной сети, разделяя ее на несколько независимых коллизионных доменов.

Коммутаторы обеспечивают пользователем выделенную полосу пропускания.

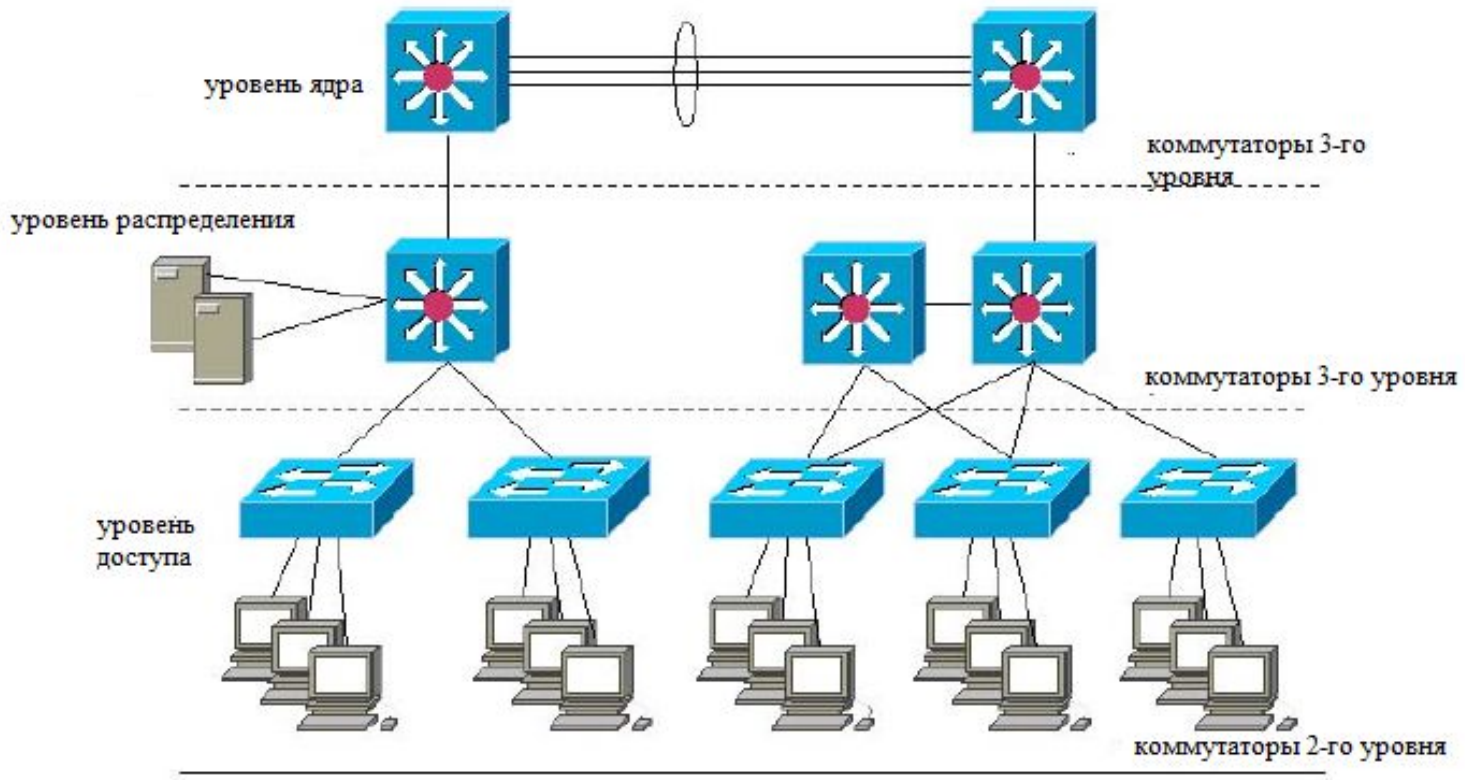
Благодаря микросегментации коммутаторы поддерживают высокую скорость передачи данных и имеют возможность предоставлять выделенную полосу пропускания приложениям, чувствительным к задержкам. *Коммутатор реализует политику обеспечения доступа и безопасности различных групп пользователей к сетевым сервисным службам на основе сетей VLAN. Каждый порт на коммутаторе представляет собой отдельный коллизионный домен и обеспечивает полную пропускную способность для одного или нескольких узлов, подключённых к этому порту.*

Лекция 2
Иерархическая структура коммутации данных пространства LAN

Иерархическая структура коммутации данных позволяет объединить через межсетевые устройства отдельные локальные сегменты, которые будут функционировать как единая сеть.

Модель иерархической структуры представлена на рисунке 1.

Рис.1


уровень ядра
коммутаторы 3-го уровня
уровень распределения
коммутаторы 3-го уровня
уровень доступа
коммутаторы 2-го уровня

Уровень доступа обеспечивает доступ к сети рабочей группе или отдельному пользователю.

Уровень распределения обеспечивает основанные на политиках подключения и контролирует границу между уровнями доступа и ядра.

Уровень ядра обеспечивает быструю передачу данных между коммутаторами-распределителями в рамках комплекса зданий предприятия.

Уровень доступа предоставляет следующие функциональные возможности:

Коммутация 2-го уровня.

Высокая доступность.

Функция безопасности портов.

Классификация и маркировка качества обслуживания (QoS) и границы доверия.

Проверка по протоколу ARP.

Виртуальные списки контроля доступа (VACL).
Связующее дерево.
Питание через Ethernet (PoE) и вспомогательные VLAN для VoIP.

Уровень распределения предоставляет следующие службы:
Агрегация каналов LAN или глобальной сети.

Безопасность на основе политик в форме списков контроля доступа (ACL) и фильтрации.

Сервисы маршрутизации между локальной сетями LAN и VLAN и между доменами маршрутизации (например от EIGRP к OSPF).

Избыточность и балансировка нагрузки.

Граница для агрегирования и суммирования маршрутов, настроенных на интерфейсах по направлению к уровню ядра.

Уровень ядра обеспечивает следующие функции:

Обеспечение высокоскоростной коммутации (технологии быстрой передачи данных).

Обеспечение надёжности и устойчивости к сбоям.

Масштабирование за счёт использования более быстродействующего оборудования, а не за счёт увеличения числа устройств.

Устранение операций с пакетами, требующих большой загрузки ЦП, которые порождаются процессами обеспечения безопасности, классификации качества обслуживания (QoS) или иными процессами.

Лекция 3
Классификация коммутаторов

Коммутаторы классифицируются по следующим признакам:

1. Конструктивному исполнению

В конструктивном отношении коммутаторы делятся на следующие типы:

>*Автономные коммутаторы с фиксированным количеством портов.*

Такой тип коммутаторов может иметь от 8 до 50 портов со скоростями 10,100,1000 Мбит/с, заключенных в корпус для настольной установки или монтажа в стойку.

>*Модульные коммутаторы на основе шасси.*

Модульные коммутаторы поставляются с шасси разного размера, что позволяет устанавливать разное количество модульных линейных плат.

Линейные платы содержат порты. Линейную плату вставляют в шасси коммутатора подобно тому, как платы расширения вставляют в ПК. Чем больше шасси, тем больше модулей он поддерживает.
Модульные коммутаторы чаще всего предназначены для применения на магистрали сети.

>*Стекируемые коммутаторы*
Стекируемые коммутаторы соединены между собой с помощью специального кабеля, обеспечивающего высокую пропускную способность между ними. Технология Cisco StackWise позволяет соединять до девяти коммутаторов. Помещённые в стек коммутаторы работают с эффективностью одиночного коммутатора больших размеров. Стекируемые коммутаторы рекомендуется использовать в задачах, где особые требования предъявляются к отказоустойчивости и доступности пропускной способности, а применение модульного коммутатора оказывается слишком дорогим.

Формфактор коммутаторов

Фиксированная конфигурация

Стекируемая конфигурация

Модульная конфигурация

2. функциям управления

По функциям управления можно выделить следующие типы коммутаторов:

>неуправляемые коммутаторы — функции управления и настройки не поддерживают (D-Link DES-1005D),
>управляемые коммутаторы — поддерживают широкий набор функций управления и настройки, включающие интерфейс командной строки (CLI), протокол Telnet, SSH, SNMP, Web интерфейс (D-Link DES-3200-28).

Лекция 4
Технические характеристики коммутаторов

Основными характеристиками являются следующие:

>*Стоимость* — стоимость коммутатора зависит от количества интерфейсов и их скорости, поддерживающих функций и возможностей расширения.

>*Плотность портов* — сетевые коммутаторы должны поддерживать соответствующее количество устройств в сети (5,8,16,24,48).

>*Скорость порта* — скорость подключения к сети является основным факторам выбора для всех конечных пользователей (10/100/1000 Мбит/с).

> *Питание* — точки доступа, IP-телефоны, компактные коммутаторы получают питание через Ethernet (PoE).

Ряд коммутаторов поддерживают резервные источники питания.

>*Надежность* — коммутатор должен обеспечивать непрерывный доступ к сети.

>*Масштабируемость* — коммутатор должен предоставлять возможность расширения сети.

>*Буферы кадров* — возможность коммутатора хранить кадры сети, где может возникнуть перегрузка портов на сервере или в других областях сети.

Лекция 5
Последовательность стадий загрузки коммутатора

После включения коммутатор Cisco проходит следующие стадии загрузки:

1. Коммутатор загружает программу самотестирования при включении питания (POST), хранящуюся в ПЗУ. POST проверяет ЦП подсистемы. Программа тестирует ЦП, оперативную динамическую память (DRAM) и часть флеш-устройств, составляющих файловую систему флеш-памяти.

2. После этого на коммутаторе запускается программное обеспечение начального загрузчика. Начальный загрузчик — это небольшая программа, которая хранится в ПЗУ и запускается сразу после успешного завершения проверки POST.

3. Начальный загрузчик выполняет низкоуровневую инициализацию ЦП. Он инициализирует регистры ЦП, которые контролируют физическую память, количество памяти и скорость.
4. Затем программа запускает файловую систему флеш-памяти на материнской плате.
5. Начальный загрузчик находит и загружает образ операционной системы IOS по умолчанию и передаёт ей управление коммутатором.

Затем операционная система IOS инициализирует интерфейсы, используя команды Cisco IOS из конфигурационного файла (startup-config), который хранится в энергонезависимом ОЗУ (NVRAM).
После успешного выполнения всех выше указанных стадий и загрузки конфигурационного файла в оперативную память, система переходит в режим ожидания вода команд.

На передней панели коммутатора имеются светодиодные индикаторы, которые отображают состояние коммутатора при включении питания, загрузки IOS, состояние портов при передачи данных.

Коммутаторы разных моделей и наборов функций будут иметь разные светодиоды, и их расположение на передней панели коммутатора также может отличаться.

На рисунке показаны светодиоды коммутатора и кнопка режима для коммутатора Cisco Catalyst 2960, а также их назначение.

Catalyst 2960 Switch LEDs			
1	The system LED	5	The port speed LED
2	The RPS LED (if RPS is supported on the switch)	6	The PoE status LED (if PoE is supported on the switch)
3	The port status LED (This is the default mode.)	7	The Mode button
4	The port duplex mode LED	8	The port LEDs

Кнопка Mode используется для переключения между состоянием порта, дуплексным режимом порта, скоростью порта и состоянием PoE (если поддерживается) светодиодных индикаторов порта. Далее описано назначение светодиодных индикаторов и значение их цветов:

Индикатор системы (1) - показывает, получает ли система питание и работает ли она правильно. Если светодиод не горит, это означает, что система не включена. Если светодиод горит зеленым, система работает нормально. Если индикатор горит желтым, система получает питание, но не работает должным образом.

Светодиод системы резервного питания (RPS) (2) - показывает состояние RPS. Если индикатор не горит, RPS выключен или подключен неправильно. Если индикатор горит зеленым, резервный источник питания подключен и готов предоставить резервное питание. Если светодиодный индикатор мигает зеленым, RPS подключен, но недоступен, так как он обеспечивает питание другого устройства. Если индикатор горит желтым, RPS находится в режиме ожидания или неисправен. Если светодиодный индикатор мигает желтым, это означает, что внутренний источник питания в коммутаторе неисправен, и резервный источник питания подает питание.

Индикатор состояния порта (3) - указывает, что режим состояния порта выбран, когда индикатор горит зеленым. Это режим "по умолчанию". При выборе этого параметра индикаторы портов будут отображать цвета с разными значениями. Если индикатор не горит, соединение отсутствует или порт отключен администратором. Если индикатор горит зеленым светом, связь присутствует. Если светодиодный индикатор мигает зеленым светом, это означает активность и порт отправляет или принимает данные. Если светодиодный индикатор горит зеленым и желтым светом, это означает неисправность соединения. Если индикатор горит желтым, порт заблокирован, чтобы гарантировать, что петля не существует в домене пересылки и не пересылает данные (обычно порты остаются в этом состоянии в течение первых 30 секунд после активации). Если индикатор мигает желтым, порт заблокирован, чтобы предотвратить возможное образование петли в домене пересылки.

Индикатор дуплексного режима порта (4) - указывает, что дуплексный режим порта выбран, когда индикатор горит зеленым цветом. При выборе этого параметра индикаторы порта, которые не горят, находятся в полудуплексном режиме. Если индикатор порта горит зеленым, порт находится в полнодуплексном режиме.

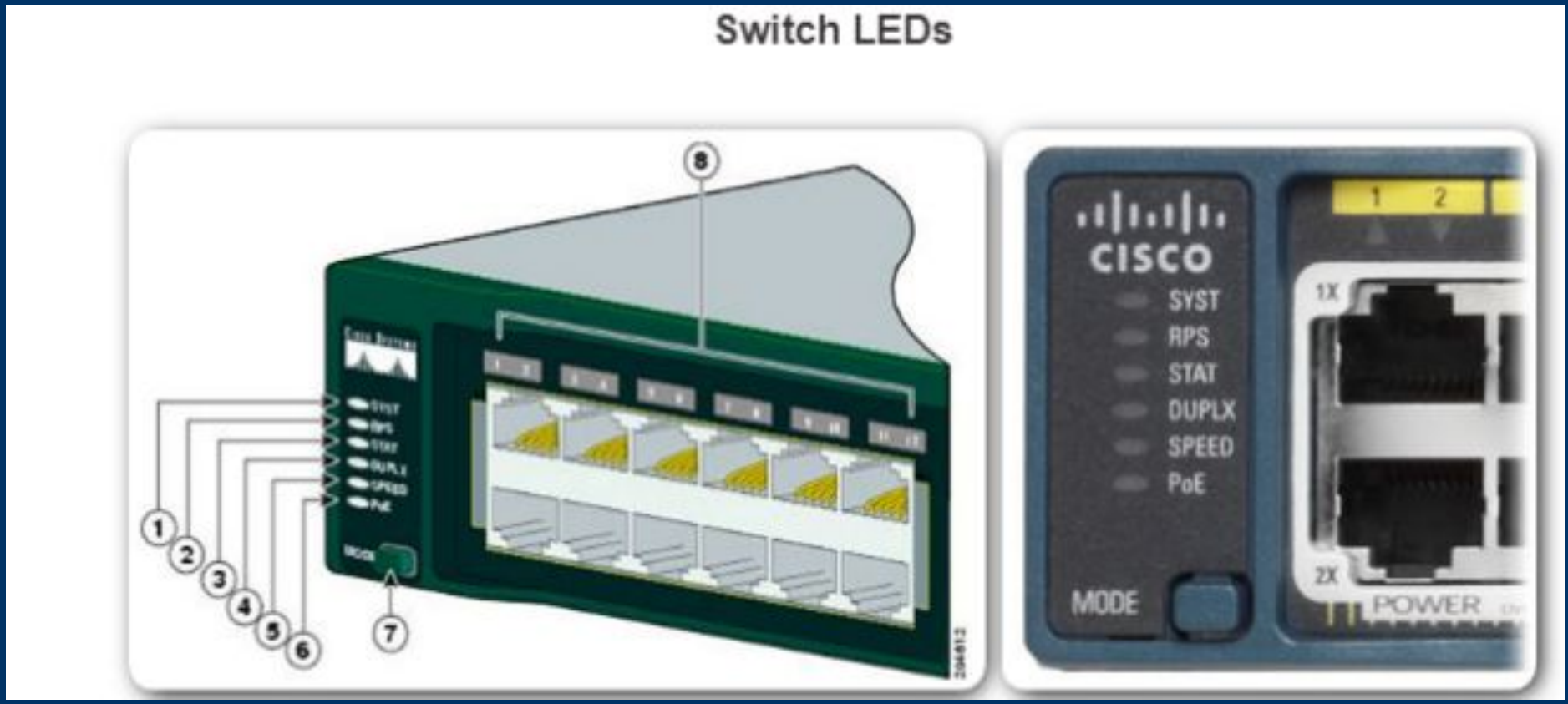
Индикатор скорости порта (5)- указывает, что выбран режим скорости порта. При выборе этого параметра индикаторы портов будут отображать цвета с разными значениями. Если светодиод не горит, порт работает со скоростью 10 Мбит / с. Если индикатор горит зеленым, порт работает со скоростью 100 Мбит / с. Если светодиод мигает зеленым, порт работает со скоростью 1000 Мбит / с.

Индикатор режима Power over Ethernet (PoE) (6) - если PoE поддерживается; загорится индикатор режима PoE. Если индикатор не горит, это означает, что режим PoE не выбран и ни один из портов не отключен от питания или не находится в неисправном состоянии. Если светодиодный индикатор мигает желтым, режим PoE не выбран, но по крайней мере один из портов отключен от питания или имеет сбой PoE.

Кнопка режима Mode (7) — испльзуется для сброса основных параметров коммутатора.

Индикаторы портов (8)

Передняя панель коммутатора



Лекция 6
Методы подключения к коммутатору

Перед тем как начать настройку коммутатора, необходимо установить физическое соединение между коммутатором и рабочей станцией.

Схема соединения представлена на рисунке 2.

Рис. 2

Существует два типа кабельного соединения, используемых для управления коммутатором.

Первый тип — непосредственного соединения рабочей станции с коммутатором посредством консольного кабеля.
Консольный кабель подключается к коммутатору через консольный порт.
Такой тип подключения используется для первоначальной настройки коммутатора.
Интерфейс передачи данных реализуется на основе протокола RS-232.
Параметры подключения по протоколу должны иметь следующие значения:
скорость передачи — 9600бит/с,
размер передаваемых данных — 8бит,
паритет — отсутствует,
стоповый бит — 1,
управление потоком — отсутствует.

Второй тип — удаленное подключение рабочей станции к коммутатору по витой паре.
При таком подключении используется порт Ethernet коммутатора.
Интерфейс между рабочей станцией и коммутатором осуществляется на основе технологии Ethernet.
Удаленное логическое подключение к коммутатору осуществляется по протоколам Telnet, SSH, HTTP, HTTPS.

Удаленное подключение к коммутатору необходимо для настройки его определенных функций, после первоначальной настройки.

Лекция 7
Первоначальная настройка параметров коммутатора

При первоначальной настройки задаются следующие параметры:

1. Системное имя коммутатора

Системное имя необходимо для однозначной идентификации коммутатора в физической топологии локальных сегментов. Оно позволяет отличить один коммутатор от другого.

По умолчанию системное имя **Switch**. Оно должно содержать не более 63 символов, начинаться с буквы и заканчиваться буквой или цифрой.

Для настройки имени задаются следующая команда в глобальном режиме: **hostname** *name.*

Для отмены имени используется команда **no hostname** в глобальном режиме.

2. Дата и время для коммутатора

Эти параметры необходимы для определения последовательности событий, происходящих в коммутаторе в течение заданного промежутка времени.
Анализ событий в заданном промежутке позволяет устранить ошибки конфигурации, а также ликвидировать проблемы с несанкционированным доступом.
Дату и время можно установить в ручную, либо синхронизировать с NTP сервером.
Время, установленную в ручную, сохраняется до следующей перезагрузки коммутатора.
Для установки даты и времени используется следующая команда: **clock set** *hh*:*mm*:*ss day month year, где*
day — дата дня месяца,
month — имя месяца,
year — год.

2. Дата и время для коммутатора

Эти параметры необходимы для определения последовательности событий, происходящих в коммутаторе в течение заданного промежутка времени.
Анализ событий в заданном промежутке позволяет устранить ошибки конфигурации, а также ликвидировать проблемы с несанкционированным доступом.
Дату и время можно установить в ручную, либо синхронизировать с NTP сервером.
Время, установленную в ручную, сохраняется до следующей перезагрузки коммутатора.
Для установки даты и времени используется следующая команда: **clock set** *hh*:*mm*:*ss day month year, где*
day — дата дня месяца,
month — имя месяца,
year — год.

Вывод времени и даты определяется командой ***show clock*** в привилегированном режиме.

3. *IP адрес коммутируемого виртуального интерфейса.*

Для удаленного доступа к коммутатору необходимо присвоить IP адрес коммутируемому виртуальному интерфейсу (SVI). Понятие SVI относится к сетям VLAN. Сети VLAN — это пронумерованные логические группы, которым можно присвоить физические порты. Конфигурации и настройки, которые применены к VLAN, также применяются ко всем портам, назначенным для этой VLAN.
По умолчанию коммутатор настроен для управления через VLAN 1.
Настройка IP адреса интерфейса SVI осуществляется в глобальном режиме следующими командами:
interface vlan *vlan-id* — конфигурация интерфейса VLAN с заданным идентификатором,

ip address *ip-address subnet-mask* — задание интерфейсу IP адреса и маски,
no shutdown — включение интерфейса VLAN,
end — возврат в привилегированный режим.

Для проверки настроек используется команда в привилегированном режиме **show running-config.**

Для сохранения настроек в стартовом конфигурационном файле используется команда в привилегированном режиме **copy running-config startup-config**.

Для отказа от IP адреса используется команда в глобальном режиме no ip address

Лекция 8
Настройка параметров доступа к коммутатору по консоли

Для зашиты коммутатора от несанкционированного доступа при консольном подключении, пользователь должен пройти процедуру аутентификации. Она включает в себя указание имени пользователя и пароля.

Все пароли должны быть зашифрованы, чтобы злоумышленник не мог понять их истинный смысл.

Для доступа в привилегированный режим настройки коммутатора необходимо задать пароль следующей командой:

enable password *password , где параметр password определяется строкой алфавитноцифровых символов от 1 до 25, не может начинаться с цифры и чувствителен к регистру.*

Для отказа от пароля используется команда в глобальном режиме **no enable password**.
Для задания имени пользователя и пароля используются следующие команды в глобальном режиме:
username *name* [**privilege** *level*] {**password** *encryption-type password*},
где имя представляется как одно слово,
уровень привилегий находится в диапазоне 0-15, уровень 15 дает выполнение исполняемых команд в привилегированном режиме, уровень 1 дает пользовательский режим выполнения команд, пароль должен быть от 1 до 25 символов,
параметр тип шифрования: 0 — незашифрованный пароль, 7 — скрытый пароль,
line console 0 — параметры аутентификации применяются к линии консоли,
login local — задает сохранения параметров в локальной базе данных коммутатора,
end — возврат в привилегированный исполняемый режим.

Для шифрования паролей используется команда **service password-encryption**.

Для проверки настроенных параметров выполните команду в привилегированном режиме **show running-config**.
Параметры настройки с копируйте в стартовый файл командой **copy running-config startup-config**.

Лекция 9
Настройка удаленного доступа к коммутатору по протоколу Telnet

Для удаленного доступа к коммутатору можно использовать протокол Telnet.

Протокол Telnet функционирует на прикладном уровне модели OSI и использует порт 23/TCP. В протоколе не предусмотрено использование шифрования данных, поэтому перехваченные данные легко прочесть. Он уязвим к любым атакам, поэтому в настоящее его не рекомендуется использовать.

Для коммутатора предусмотрена процедура аутентификации при удаленном доступе к нему по протоколу Telnet.

Параметры аутентификации задается в глобальном режиме следующими командами:

username name [privilege level]
{password encryption-type password}, где
name — имя пользователя, представляется как одно слово,
privilege level — уровень привилегий пользователя, находится в диапазоне 0-15, 1 — дает пользовательский режим выполнения команд, 15 — дает выполнение исполняемых команд в привилегированном режиме, уровень 1 дает пользовательский режим выполнения исполняемых команд,
encryption-type — тип шифрования, 0 — незашифрованный пароль, 7 — скрытый пароль,
password — пароль, должен быть от 1 до 25 символов,
line vty 0 15 — параметры аутентификации применяются к линии виртуального терминала,
login local - задает сохранения параметров в локальной базе данных коммутатора,
end - возврат в привилегированный исполняемый режим.

Для шифрования паролей используется команда **service password-encryption**.

Для проверки настроенных параметров выполните команду в привилегированном режиме **show running-config**.
Параметры настройки с копируйте в стартовый файл командой **copy running-config startup-config**.

Лекция 10
Настройка защищенного удаленного доступа к коммутатору по протоколу SSH

- SSH (англ. Secure Shell — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление коммутатором. Реализует TCP-соединение по порту 22. Похож по функциональности с протоколом Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования.

Также SSH может использовать сжатие передаваемых данных для последующего их шифрования.

В настоящее время используется версия протокола SSH-2.

Для доступа к коммутатору по протоколу используется процедура аутентификация.

Для настройки протокола SSH применяются следующие команды:
hostname *hostname — задание имени для коммутатора,*
ip *domain-name* *domain_name* — определение доменного имени для коммутатора,
crypto key generate rsa — генерация пары ключей для прохождения процедуры аутентификации (рекомендуется модуль 1024бит),
ip ssh {**timeout** *seconds* | **authentication-retries** *number*} — настройка времени ожидания ввода пароля до прерывания сессии (по умолчанию 120с), число попыток повторной аутентификации (по умолчанию 3),
username *name* [**privilege** *level*]{**password** *encryption-type password*} — установка параметров аутентификации:имени пользователя и пароля,
line vty *line_number*[*ending_line_number*] — установка линии виртуального терминала (число возможных подключаемых пользователей, диапазон 0-15),
transport input ssh — доступ к коммутатору только по протоколу SSH,

end — возврат в привилегированный режим.

Проверьте настройки и статус SSH:

show ip ssh — параметры настройки протокола,
show ssh — состояние протокола.

Параметры настройки с копируйте в стартовый файл командой copy running-config startup-config.

Замечание.
Модулю генерации ключей необходим для создания пары открытого и закрытого ключей.
При аутентификации по ключевой паре предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. На компьютере, с которой требуется произвести подключение, хранится закрытый ключ, а на удалённом компьютере — открытый. Эти файлы не передаются при аутентификации, система лишь проверяет, что владелец открытого ключа также владеет и закрытым. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.
Чем длиннее модуль генерации ключей (2048 бит и более), тем сложнее декодировать ключи и получить их истинный смысл.
Системы шифрования на основе RSA считаются надёжными, если длина ключа не менее 1024 бит.

Лекция 11
Настройка баннеров на коммутаторе CISCO

Баннер — графическое изображение рекламного характера. В общем может быть текстом или анимированным изображением. В коммутаторе CISCO используются текстовые баннеры. Баннеры должны использоваться уместным образом. Когда баннеры используется, он ни в коем случае не должен приветствовать кого-либо, пытающегося получить доступ к коммутатору. Баннер должно детализировать тот факт, что только авторизованному персоналу позволено получать доступ к устройству. Кроме того, баннер может включать запланированные завершения работы системы и другую информацию, которая касается всех сетевых пользователей.

1. Баннер **MOTD** — сообщения дня.

Он часто используется для юридического уведомления, потому что он выводится на экран для всех подключенных терминалов.
Для создания баннера необходимо выполнить команду **banner motd *c message c***

Требует использования разделителей, идентифицирующих контент сообщения баннера. За командой banner motd следует пробел и символ-разделитель. Затем выводится одна или более строк текста, составляющих сообщение баннера. Второй символ-разделитель обозначает конец сообщения. Затем необходимо нажать клавишу **Return**.
Символ-разделитель может быть любым символом, который не встречается в сообщении. Поэтому часто используется такой символ как "#".
Длина сообщения до 255 символов.
Как только команда будет выполнена, баннер будет выводиться на экран при всех последующих попытках получить доступ к устройству, пока баннер не будет удален.

2. Баннер login - баннера входа в систему (регистрации).

Для создания баннера необходимо выполнить команду ***banner login*** *c message c* ***.***

Требует разделителей как и баннер MOTD.
Символ-разделитель может быть любым символом, который не встречается в сообщении. Поэтому часто используется такой символ как "#".
Длина сообщения до 255 символов.

Можно настроить баннер регистрации для вывода на всех подключенных терминалах. Этот баннер появляется после баннера MOTD, но перед приглашением регистрации (входа в систему). Баннер регистрации нельзя отменить для отдельной линии. Для полного отказа от баннера регистрации следует удалить его командой ***no banner login.***

Лекция 12
Настройка Ethernet интерфейсов коммутатора CISCO

Ethernet интерфейсы реализуют передачу данных между сетевыми узлами, подключенными к коммутатору. Физически интерфейсы реализованы в виде портов с разъемом RJ45.

На портах коммутатора можно настроить параметры скорости и режима передачи данных.

Настроить параметры скорости можно на основе следующих команд:

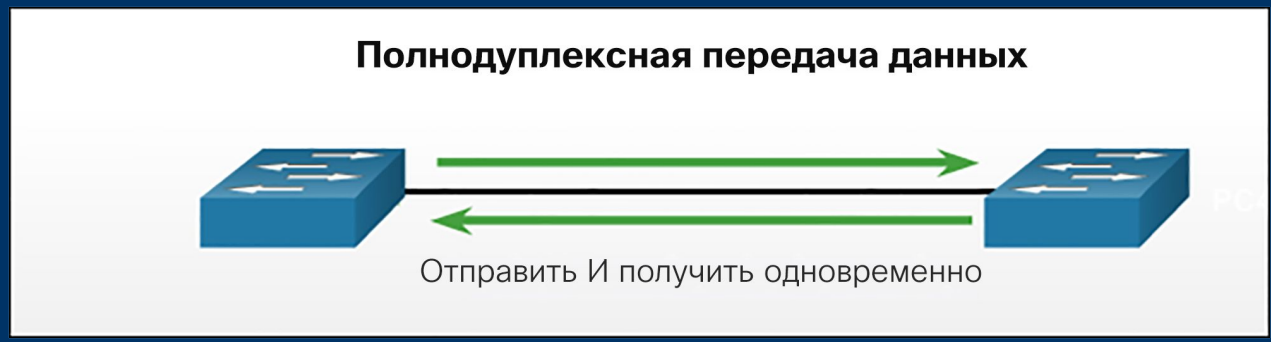
interface *interface-id* — определяется конкретный номер интерфейса коммутатора,

speed {**10** | **100** | **1000** | **auto** — определяется конкретный параметр скорости 10,100,1000 мбит/с, auto — автосогласование параметра.

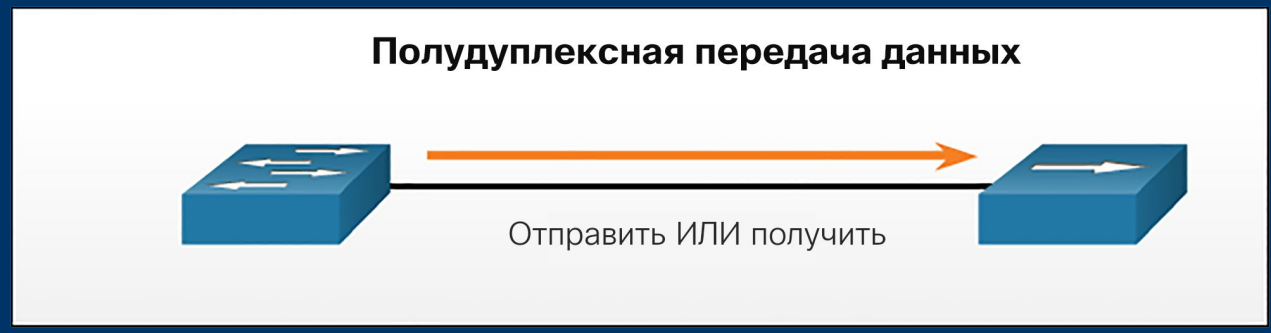
Дуплексная связь представлена на следующим рисунке

- Для работы полнодуплексных соединений требуются сетевые интерфейсные платы, поддерживающие Gigabit Ethernet и 10Gb Ethernet.

Двусторонняя связь



Однонаправленная связь



Полнодуплексная связь улучшает производительность коммутируемой локальной сети. Полнодуплексная связь увеличивает эффективную полосу пропускания, позволяя обоим концам соединения одновременно передавать и принимать данные. Это также известно как двунаправленное. Этот метод оптимизации производительности сети требует микросегментации. Микросегментированная LAN создается, когда к порту коммутатора подключено только одно устройство и работает в полнодуплексном режиме. Это приводит к возникновению области коллизий микропроцессора одного устройства. Поскольку подключено только одно устройство, микросегментированная локальная сеть не имеет конфликтов.

В отличие от полнодуплексной связи, полудуплексная связь является однонаправленной. Отправка и получение данных не происходит одновременно. Полудуплексная связь создает проблемы с производительностью, поскольку данные могут передаваться только в одном направлении за раз, что часто приводит к конфликтам. Полудуплексные соединения обычно используются в более старом оборудовании, таком как концентраторы. Полнодуплексная связь заменила полудуплекс в большинстве аппаратных средств.

Настроить параметры режима дуплекса можно на основе следующих команд:

interface *interface-id* — определяется конкретный номер интерфейса коммутатора,

duplex {auto | full | half}, где параметры означают автосогласование, полный дуплекс, полудуплекс.

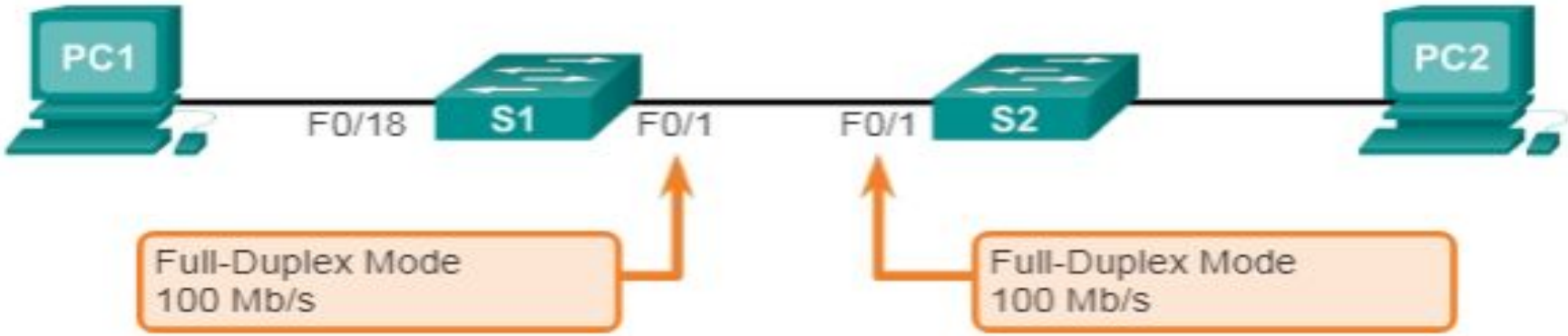
Замечание:

Режим полдуплекса можно установить только для скоростей 10 или 100mb/s.

Вы не можете установить режим полдуплекса для интерфейса, функционирующего на скорости 1000mb/s.

Настройки дуплекса и скорости иллюстрированы на рисунке

Настройки дуплекса и скорости



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

По умолчанию на коммутаторах Cisco Catalyst 2960 и 3560 настройки дуплексного режима и скорости выставлены в режим Auto. Автосогласование полезно, когда настройки скорости и дуплекса для устройства, подключенного к порту, неизвестны или могут меняться. При подключении к известным устройствам, таким как серверы, выделенные рабочие станции или сетевые устройства, рекомендуется вручную задавать параметры скорости и дуплекса. Можно задать описание интерфейса, для определения его назначения.
interface *interface-id* — определяется интерфейс, для которого задается описание,
description *string* — описание интерфейса (не более 240 символов).

Для задания диапазона значений скорости и режима передачи данных используется команда:
interface range *port-range,* где port — номер порта, range — конечное значение диапазона (диапазон ограничен 5 портами).

определения типа кабеля по разводке контактов (auto-MDIX). При включенной функции auto-MDIX интерфейс распознаёт требуемый тип кабельного соединения (прямое или кроссовое) и настраивает подключение соответствующим образом. В случае подключения к коммутаторам без функции auto-MDIX для соединения серверов, рабочих станций или маршрутизаторов следует использовать прямые кабели, тогда как для подключения к другим коммутаторам или повторителям используются кроссовые кабели.
Включённая функция auto-MDIX позволяет использовать любой тип кабеля для подключения к другим устройствам, а интерфейс автоматически настраивается для успешного взаимодействия.
По умолчанию функция auto-MDIX включена. При использовании функции auto-MDIX на интерфейсе скорость интерфейса и дуплексный режим должны быть настроены в режим auto, чтобы функция работала должным образом.
Для включения функции auto-MDIX необходимо задать следующие команды:

***interface interface-id* —** режим настройки заданного интерфейса,
***speed auto* —** задание скорости интерфейса,
***duplex auto* —** задание режима передачи данных на интерфейсе,
***mdix auto* —** включение функции auto-MDIX,
***end* —** возвращение в привилегированный режим,
***show controllers ethernet-controller interface-id phy* —** проверка состояния функции auto-MDIX.

В коммутаторе cisco реализована функция «управления потоком», для временной приостановки передачи кадров в случае перегрузки канала. При этом коммутатор может только получать кадр паузу, которая приостанавливает передачу до восстановления нормального состояния канала.
Для задания функции «управления потоком» надо задать команды:
interface *interface-id* — режим настройки заданного интерфейса,

***flowcontrol receive on* —** включение функции «управления потоком»,
end — возвращение в привилегированный режим,
copy running-config startup-config — сохранение настроек в стартовом конфигурационном файле.

По умолчанию функция **flowcontrol** выключена.

Для проверки функционирования портов коммутатора используйте команду **show interfaces** *interface_id*, где *interface_id* — тип и номер порта интерфейса.

Выполнение команды представлено на рисунке.

Состояние интерфейса

Layer 1
OK

Layer 2
OK

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
(bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

Результатом выполнения команды являются следующие параметры:

- Состояние интерфейса
- Состояние протокола линии
- Скорость передачи данных
- Режим передачи данных
- Тип среды передачи (стандарт Ethernet) и другие.

Лекция 13
Управление таблицей MAC коммутатора

Основная концепция коммутации заключается в принятии устройством решения на основе двух критериев:

- входной порт
- адрес назначения

Решение, принимаемое коммутатором, основывается на данных о входном порте и адресе назначения данного сообщения.

Коммутатор LAN ведёт таблицу MAC адресов, с помощью которой определяет, как пересылать трафик через коммутатор. Коммутаторы используют MAC-адреса для направления сетевой передачи данных через коммутатор к соответствующему порту до места назначения.

Коммутаторы LAN определяют способ обработки входящих кадров путём ведения таблицы MAC-адресов. Коммутатор создаёт свою таблицу MAC-адресов, записывая MAC-адрес каждого устройства, подключённого к каждому из своих портов. Коммутатор использует данные из таблицы MAC-адресов для отправления кадров, предназначенных для конкретного устройства из порта, который был назначен этому устройству.

Коммутатор заполняет таблицу MAC-адресов на основе MAC-адресов источника. Когда коммутатор принимает входящий кадр с MAC-адресом назначения, который не содержится в таблице MAC-адресов, коммутатор пересылает кадр из всех портов (лавинная рассылка), за исключением входного порта этого кадра. Когда устройство назначения отвечает, коммутатор добавляет MAC-адрес источника кадра и порта, на котором был получен кадр, в таблицу MAC-адресов.

Процесс формирования таблицы MAC адресов показан на следующих рисунках.

На рисунке 1 хост A отправляет трафик на хост B. Коммутатор получает кадры и ищет MAC-адрес назначения в своей таблице MAC-адресов. Если коммутатор не может найти MAC-адрес назначения в таблице MAC-адресов, коммутатор затем копирует кадр и выполняет лавинную рассылку (широковещательную рассылку) из каждого порта коммутатора Port2, Port3, кроме порта, на котором он был получен Port1.

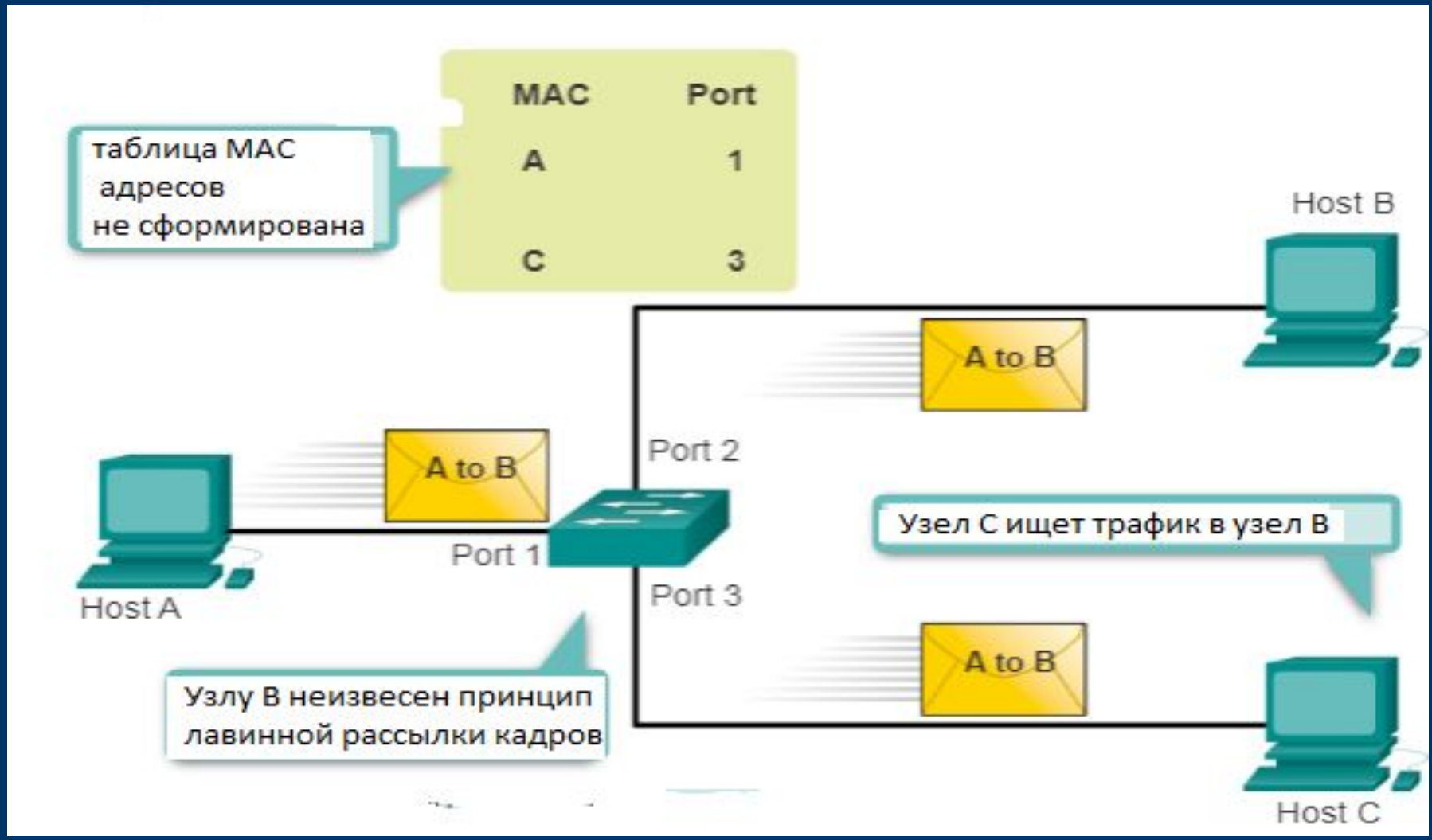

MAC
Port
A
1
C
3
таблица MAC адресов не сформирована
Host B
A to B
Port 2
A to B
Узел C ищет трафик в узел B
Port 1
Port 3
Host A
Узлу B неизвесен принцип лавинной рассылки кадров
A to B
Host C

Рис. 1

На рисунке 2 хост B получает кадр и отправляет ответ хосту A. Затем коммутатор узнает, что MAC-адрес хоста B расположен на порту 2, и записывает эту информацию в таблицу MAC-адресов.

Хост C также получает кадр от хоста A к хосту B, но поскольку MAC-адрес назначения этого кадра - хост B, хост C отбрасывает этот кадр.

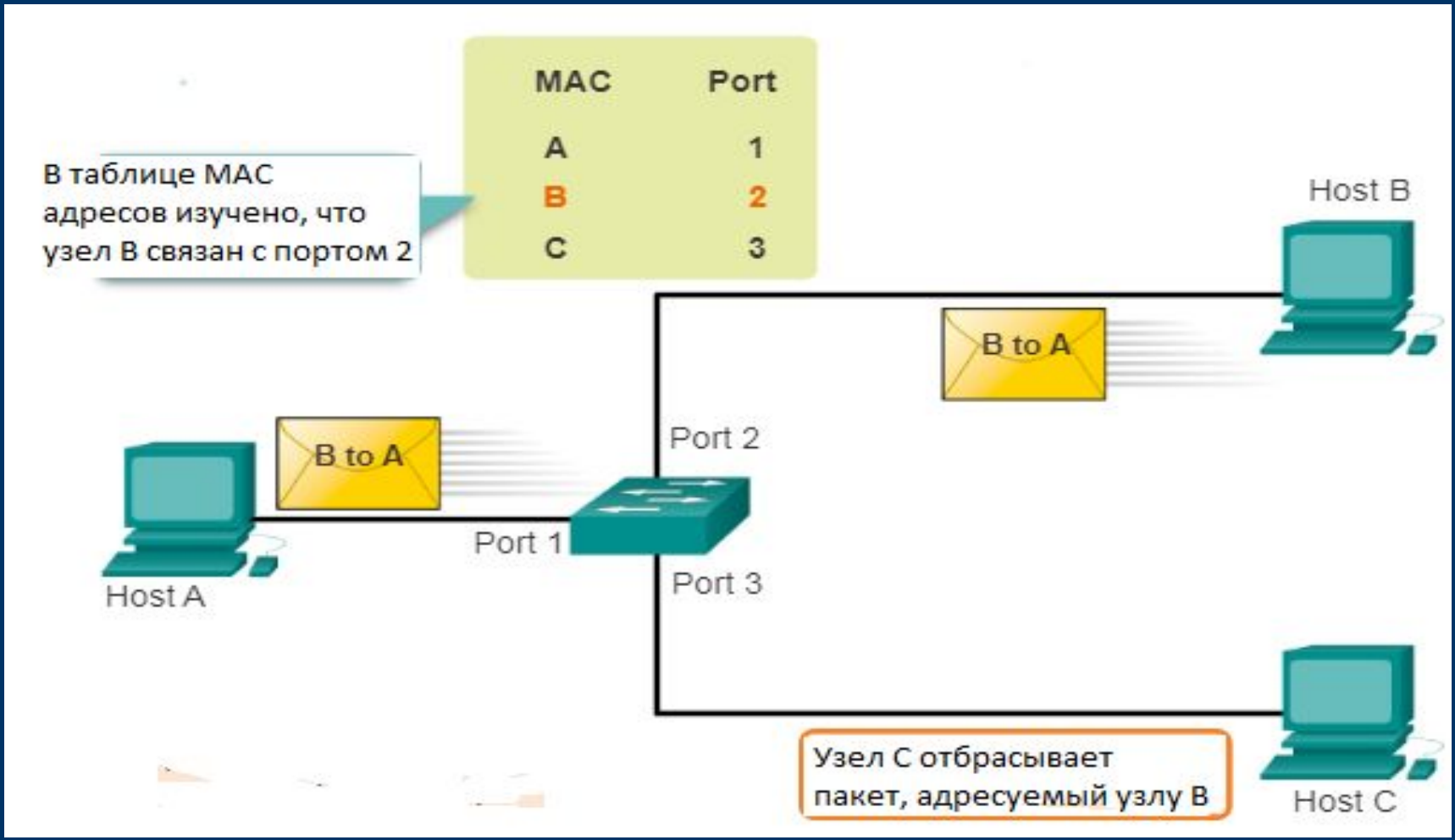

MAC
Port
A
1
B
2
C
3
В таблице MAC адресов изучено, что узел B связан с портом 2
Host B
B to A
B to A
Port 2
Port 1
Port 3
Host A
Узел C отбрасывает пакет, адресуемый узлу B
Host C

Рис. 2

Как показано на рисунке 3, любой кадр, отправленный хостом A (или любым другим хостом) на хост B, пересылается на порт 2 коммутатора, а не транслируется через каждый порт.

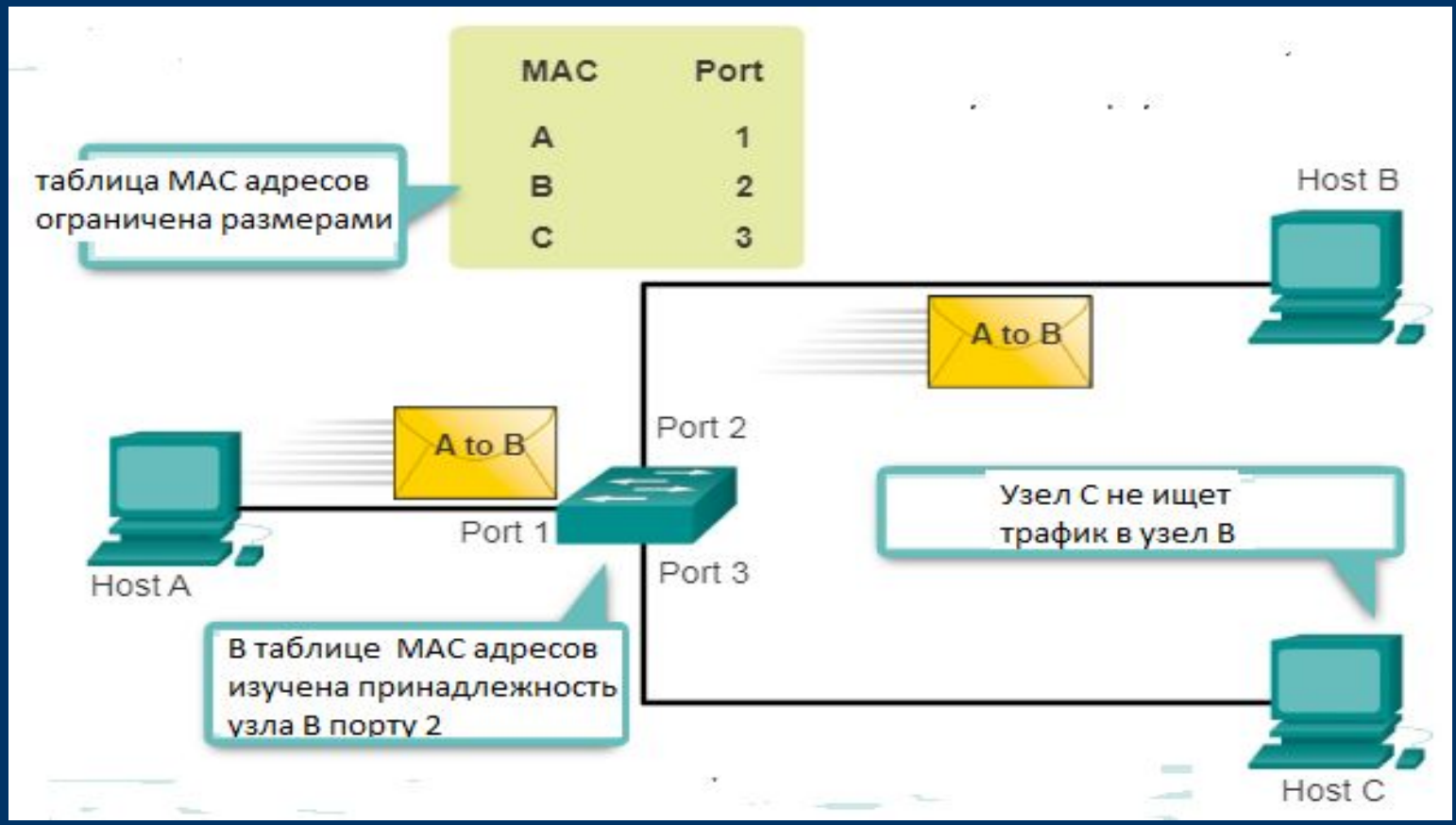


Таблица MAC-адресов содержит два типа адресов:
динамические адреса: MAC-адрес источника изучается в режиме реального времени и обновляется, если не используется (по умолчанию время обновления через **300** с).

Для очистки всех динамических MAC-адресов используется команда clear mac address-table dynamic в привилегированном режиме.
Также можно удалить конкретный динамический MAC-адрес командой clear mac address-table dynamic address mac-address.
статические адреса: создаются и удаляются в ручную, могут быть одноадресными и групповыми, не обновляются и сохраняются после перезагрузки коммутатора.
Создаются командой mac address-table static mac-addr vlan vlan-id interface interface-id, где vlan-id — идентификатор vlan с заданным MAC-адресом, interface-id — идентификатор интерфейса, связанного с заданным MAC-адресом.
Статические MAC-адреса можно просмотреть командой show mac address-table static.

Удаление статического MAC-адреса реализуется командой **no mac address-table static** *mac-addr* **vlan** *vlan-id* в глобальном режиме.

Кадры с динамическим MAC адресом поступающие на порт с привязанным статическим MAC адресом отбрасываются, таким образом реализуется фильтрация кадров.

Лекция 14
Виртульные локальные сети коммутатора CISCO

Предоставление доступа в локальный сетевой сегмент обеспечивается коммутатором уровня доступа. Для уменьшения размера широковещательных доменов на коммутаторе 2-го уровня, как и на устройстве 3-го уровня создаются сети VLAN.

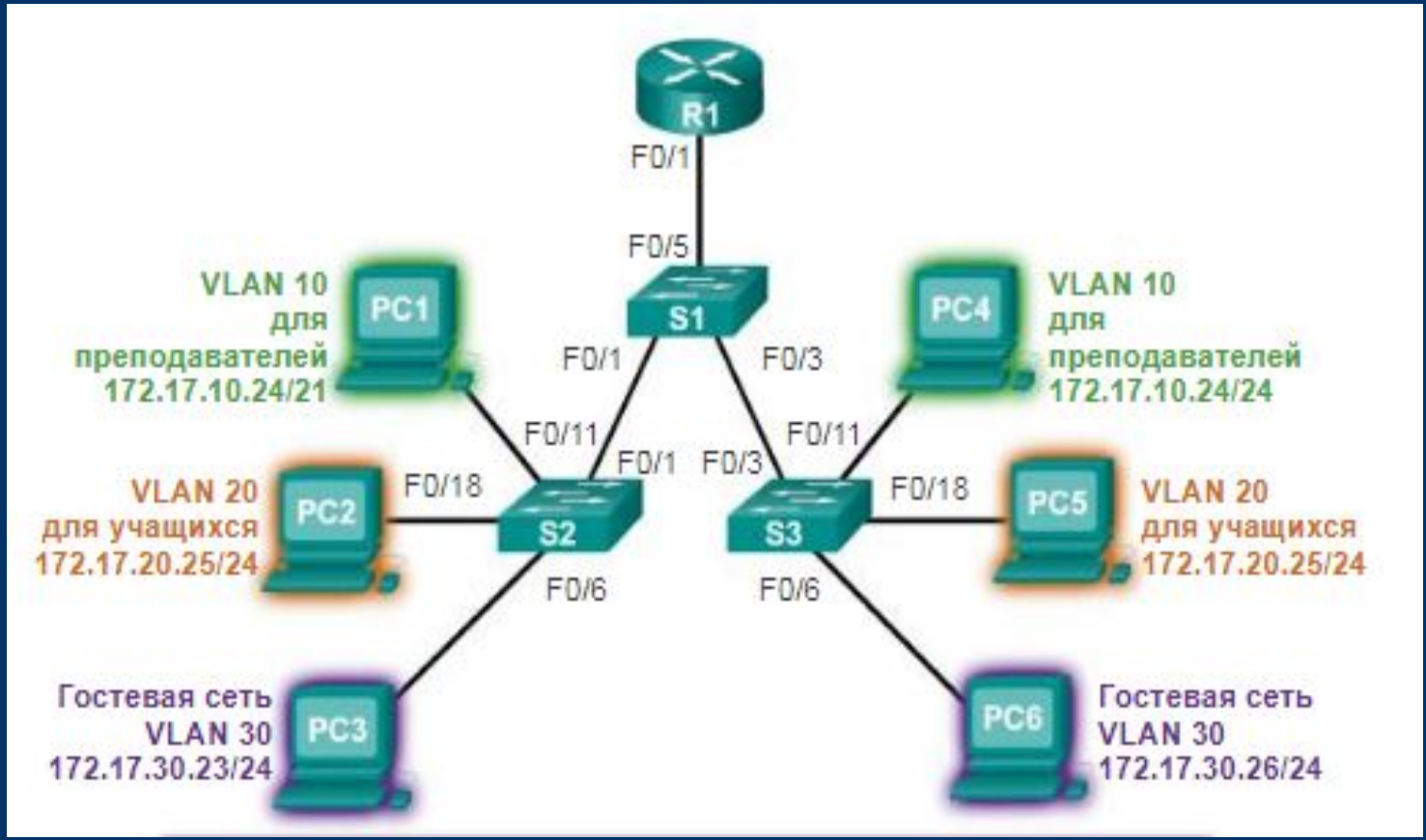
Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях.

Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов.

Виртуальные локальные сети создают следующие преимущества функционирования локальных сегментов:
повышенный уровень безопасности,
снижение затрат,
повышение производительности,
уменьшение размера широковещательного домена,
эффективность управления.

Каждая VLAN в коммутируемой сети соответствует IP-сети; поэтому при проектировании VLAN необходимо учитывать реализацию иерархической схемы сетевой адресации. Иерархическая сетевая адресация означает, что номера IP-сетей применяются к сегментам сети или виртуальным локальным сетям упорядоченным образом с учетом сети в целом. Блоки смежных сетевых адресов зарезервированы и настроены для устройств в определенной области сети, как показано на рисунке.

Топология VLAN представлена на следующем рисунке:



В современных сетях используется несколько различных типов VLAN. Некоторые типы VLAN определяются классами трафика. Другие типы VLAN определяются конкретной функцией, которую они обслуживают.

Данные VLAN

VLAN данных - это VLAN, настроенная для передачи пользовательского трафика. VLAN, передающая голосовой или управляющий трафик, не будет частью VLAN для передачи данных. Распространенной практикой является отделение голосового трафика и трафика управления от трафика данных. VLAN данных иногда называют пользовательской VLAN. Сети VLAN данных используются для разделения сети на группы пользователей или устройств.

VLAN по умолчанию

Все порты коммутатора становятся частью VLAN по умолчанию после начальной загрузки коммутатора, загружающего конфигурацию по умолчанию. Порты коммутатора, которые участвуют в VLAN по умолчанию, являются частью того же широковещательного домена. Это позволяет любому устройству, подключенному к любому порту коммутатора, взаимодействовать с другими устройствами на других портах коммутатора. VLAN по умолчанию для коммутаторов Cisco - VLAN 1.

На рисунке команда ***show vlan brief*** была выдана на коммутаторе с конфигурацией по умолчанию. Обратите внимание, что все порты по умолчанию назначены VLAN 1.

VLAN 1 имеет все функции любой VLAN, за исключением того, что ее нельзя переименовать или удалить. По умолчанию весь управляющий трафик уровня 2 связан с VLAN 1.

VLAN 1

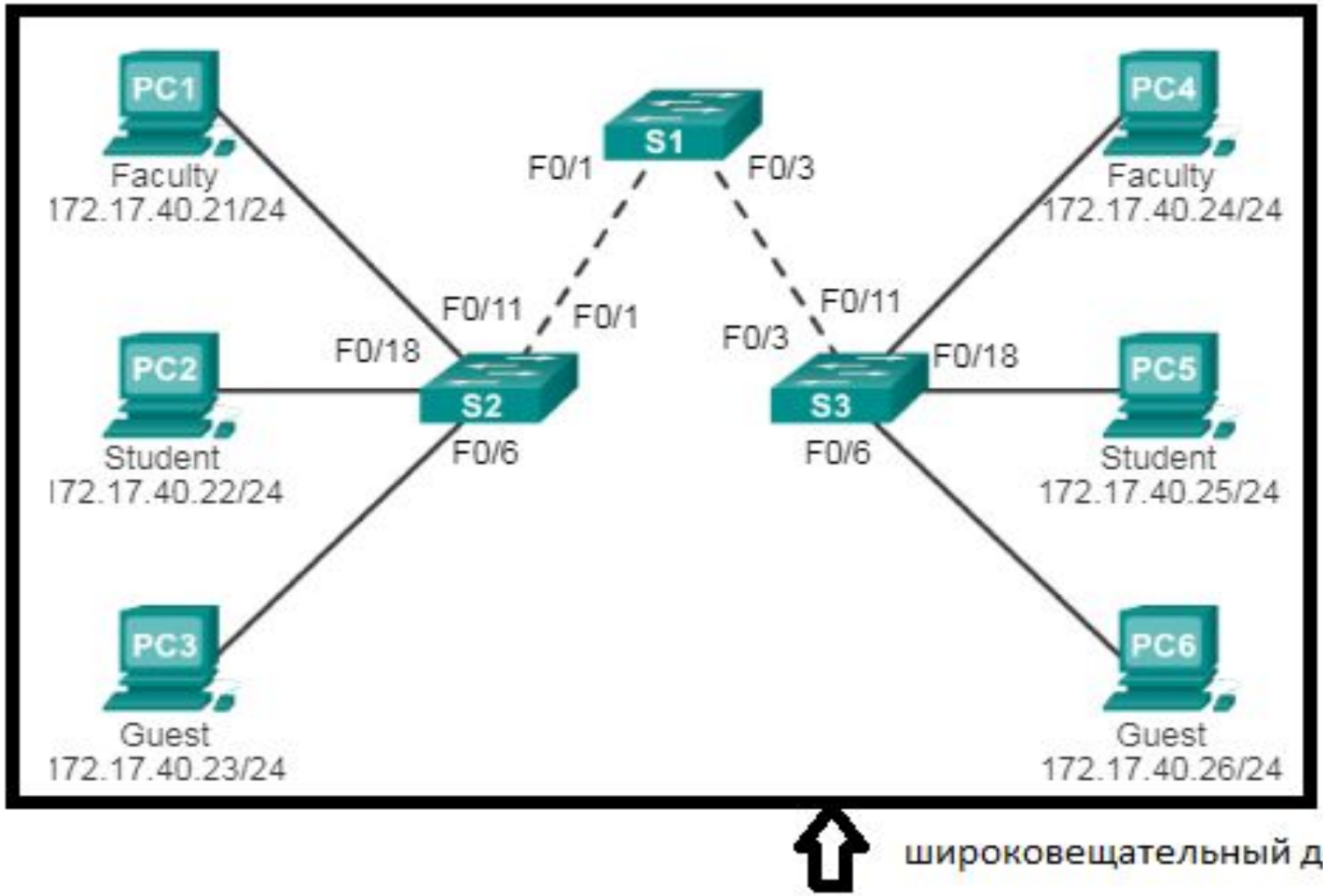
```
Switch# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -----------------------
1    default              active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                    Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                    Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1,  Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

- Все порты присоединены к VLAN1 по умолчанию для пересылки данных
- Собственная VLAN - VLAN1 по умолчанию
- Управляющая VLAN - VLAN1 по умолчанию
- VLAN1 не может быть переименована или удалена

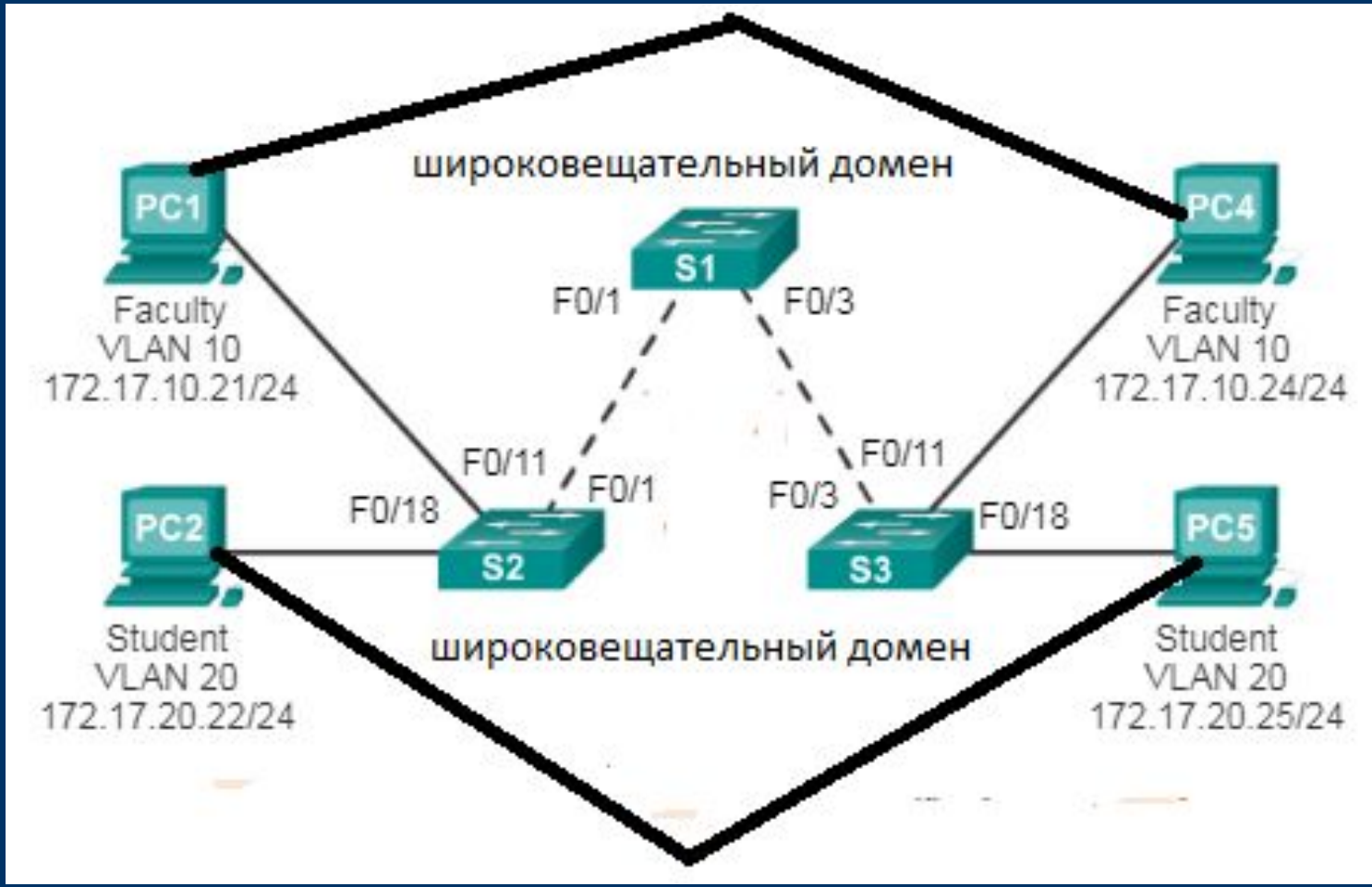
Сеть без VLAN

В нормальном режиме работы, когда коммутатор получает кадр широковещательной рассылки на один из своих портов, он пересылает этот кадр на все остальные порты, кроме порта, на котором была получена широковещательная передача. На рисунке вся сеть настроена в одной подсети (172.17.40.0/24), и никакие VLAN не настроены. В результате, когда преподавательский компьютер (ПК1) отправляет широковещательный кадр, коммутатор S2 отправляет этот широковещательный кадр на все свои порты. В конце концов, вся сеть принимает широковещательную передачу, потому что сеть является одним широковещательным доменом.


PC1
Faculty
172.17.40.21/24
PC2
Student
172.17.40.22/24
PC3
Guest
172.17.40.23/24
S1
F0/1
F0/3
S2
F0/11
F0/1
F0/18
F0/6
S3
F0/3
F0/11
F0/18
F0/6
PC4
Faculty
172.17.40.24/24
PC5
Student
172.17.40.25/24
PC6
Guest
172.17.40.26/24
широковещательный домен

Сеть с VLAN

Как показано на рисунке, сеть была сегментирована с использованием двух VLAN:
устройства преподавателей назначаются VLAN 10, а устройства студентов - VLAN 20. Когда широковещательный кадр отправляется с компьютера преподавателя, PC1, на коммутатор S2. , коммутатор пересылает этот широковещательный кадр только на те порты коммутатора, которые настроены для поддержки VLAN 10.


широковещательный домен
PC1
PC4
S1
F0/1
F0/3
Faculty
VLAN 10
172.17.10.21/24
Faculty
VLAN 10
172.17.10.24/24
F0/11
F0/11
F0/1
F0/3
F0/18
F0/18
PC2
PC5
S2
S3
Student
VLAN 20
172.17.20.22/24
широковещательный домен
Student
VLAN 20
172.17.20.25/24

Когда S1 получает широковещательный кадр через порт F0 / 1, S1 пересылает этот широковещательный кадр из единственного другого порта, настроенного для поддержки VLAN 10, то есть порта F0 / 3. Когда S3 принимает широковещательный кадр через порт F0 / 3, он пересылает этот широковещательный кадр из единственного другого порта, настроенного для поддержки VLAN 10, то есть порта F0 / 11. Широковещательный кадр поступает на единственный другой компьютер в сети, настроенный в VLAN 10, которым является компьютер ПК4.

Когда VLAN реализованы на коммутаторе, передача одноадресного, многоадресного и широковещательного трафика от хоста в конкретной VLAN ограничивается устройствами, которые находятся в этой VLAN.

Настройка VLAN

Различные коммутаторы Cisco Catalyst поддерживают разное количество виртуальных локальных сетей. Количество поддерживаемых VLAN достаточно велико, чтобы удовлетворить потребности большинства организаций. Например, коммутаторы Catalyst 2960 Series поддерживают более 4000 VLAN.

VLAN с нормальным диапазоном на этих коммутаторах пронумерованы от 1 до 1 005, а VLAN с расширенным диапазоном - от 1 006 до 4 094.

VLAN нормального диапазона

Используется в сетях малого и среднего бизнеса, а также в корпоративных сетях.
Идентифицируется идентификатором VLAN от 1 до 1005.
Идентификаторы с 1002 по 1005 зарезервированы для сетей Token Ring и FDDI VLAN.
Идентификаторы 1 и 1002–1005 создаются автоматически и не могут быть удалены.
Конфигурации хранятся в файле базы данных VLAN, который называется vlan.dat. Файл vlan.dat находится во флэш-памяти коммутатора.

Сети VLAN с расширенным диапазоном

Позвольте поставщикам услуг расширить свою инфраструктуру для большего числа клиентов. Некоторые глобальные предприятия могут быть достаточно большими, чтобы нуждаться в идентификаторах VLAN с расширенным диапазоном.
Идентифицируются идентификатором VLAN от 1006 до 4094.
Конфигурации не записываются в файл vlan.dat.
Поддерживает меньшее количество функций VLAN, чем VLAN обычного диапазона.
По умолчанию сохраняются в текущем файле конфигурации.

При настройке сетей VLAN нормального диапазона сведения о конфигурации сохраняются во флэш-памяти коммутатора в файле с именем vlan.dat. Флэш-память является постоянной и не требует команды copy running-config startup-config . Однако, поскольку другие детали часто настраиваются на коммутаторе Cisco одновременно с созданием сетей VLAN, рекомендуется сохранять текущие изменения конфигурации в стартовой конфигурации.

Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1 с именем default. Каждый Ethernet VLAN должен иметь уникальный идентификатор в диапазоне 1-1001 и имя.
Для задания числового идентификатора и имени необходимо задать следующие команды в глобальном режиме настройки:
vlan *vlan-id* — задание числового идентификатора,
name *vlan-name* — присвоение имени.

Далее необходимо возвратиться в привилегированный режим командой **end** и проверить созданные VLAN командой **show vlan**.

Следующим шагом после создания сети VLAN является назначение портов сетям VLAN. Порт доступа может одновременно принадлежать только одной VLAN.
Для реализации указанной задачи необходимо задать команды в глобальном режиме:

interface interface-id — режим настройки интерфейса с заданным идентификатором,
switchport mode access — перевод порта в режим доступа,
switchport access vlan *vlan-id* — назначение порта данной VLAN.

Далее возвратиться в привилегированный режим командой **end** и проверить режим портов, присоединенных к VLAN командой **show running-config interface** *interface-id*.

Затем необходимо сохранить настройка VLAN в постоянной памяти командой **copy running-config startup config**.

Для проверки настроек VLAN используйте следующие команды:

show interfaces vlan *vlan-id* - выводит характеристики всех интерфейсов для заданной VLAN

show vlan id *vlan-id* — выводит параметры заданной VLAN

Для удаления VLAN используйте команду **no vlan** *vlan-id*.

Лекция 15
Магистральные каналы VLAN

Магистраль VLAN, или магистраль, представляет собой двухточечный канал между двумя сетевыми устройствами, по которому передается более одной VLAN. Магистраль VLAN расширяет VLAN по всей сети. Cisco поддерживает протокол IEEE 802.1Q для координации соединительных линий на интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

Магистрали VLAN позволяют всему трафику VLAN распространяться между коммутаторами, так что устройства, которые находятся в одной VLAN, но подключены к разным коммутаторам, могут обмениваться данными без вмешательства маршрутизатора.

Магистраль VLAN не принадлежит определенной VLAN; скорее, это канал для нескольких VLAN между коммутаторами и маршрутизаторами. Магистраль также может использоваться между сетевым устройством и сервером или другим устройством, оснащенным соответствующей сетевой картой с поддержкой 802.1Q. По умолчанию на коммутаторе Cisco Catalyst все сети VLAN поддерживаются магистральным портом.

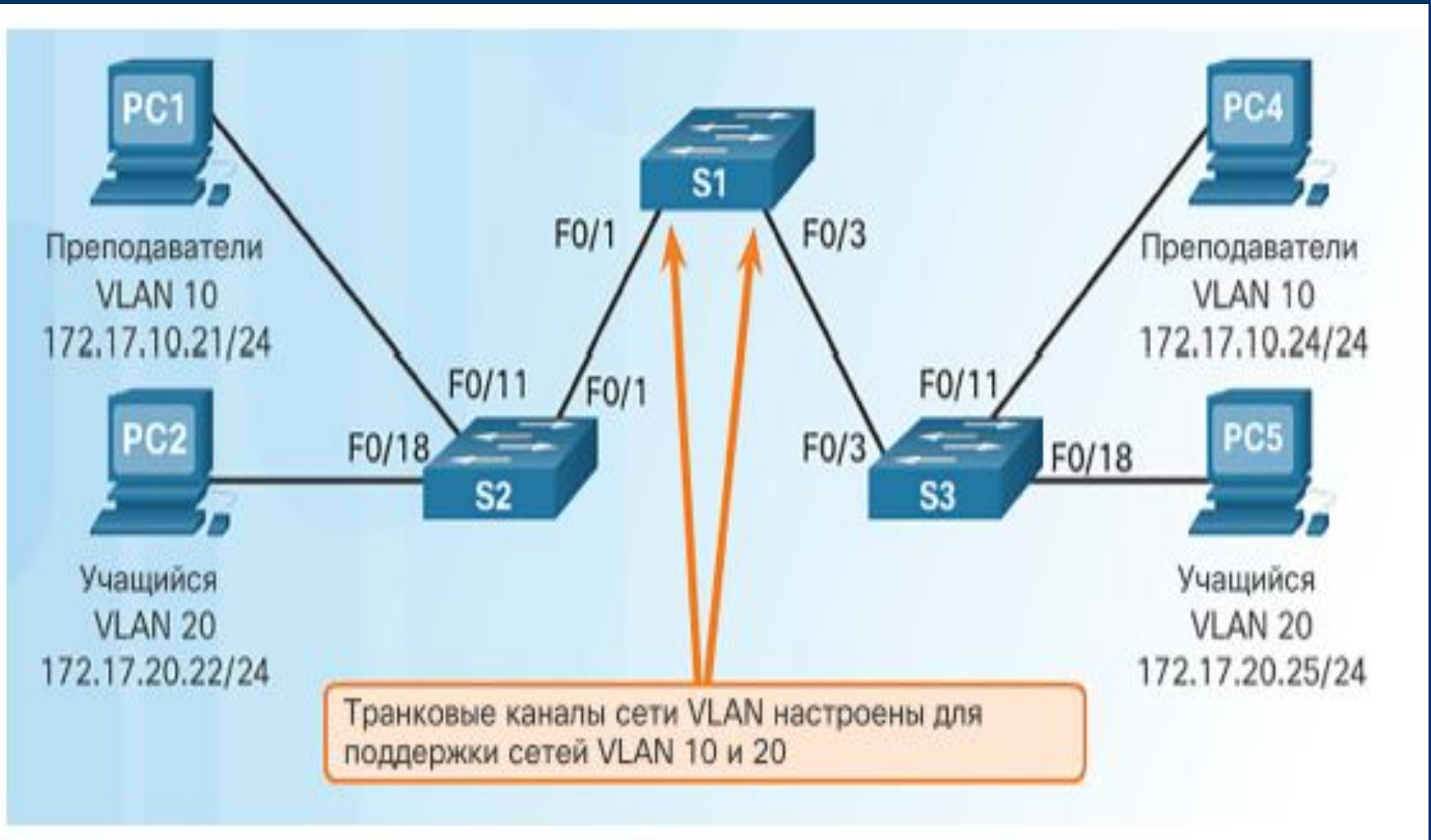
Преподаватели/сотрудники VLAN 10 – 172.17.10.0/24
Студенты VLAN 20 – 172.17.20.0/24
Посетители VLAN 30 – 172.17.30.0/24
Управление и нетегированный трафик VLAN 99 – 172.17.99.0/24

F0/1-5 – магистральные интерфейсы 802.1Q в сети VLAN 99 с нетегированным трафиком.
F0/11-17 находятся в VLAN 10.
F0/18-24 находятся в VLAN 20.
F0/6-10 находятся в VLAN 30.

На рисунке каналы между коммутаторами S1 и S2, а также S1 и S3 настроены для передачи трафика, поступающего из VLAN 10, 20, 30 и 99 по сети. Эта сеть не могла бы функционировать без соединительных линий VLAN.

На рисунке компьютер PC1 в сети VLAN 10 отправляет фрейм широковещательной рассылки.

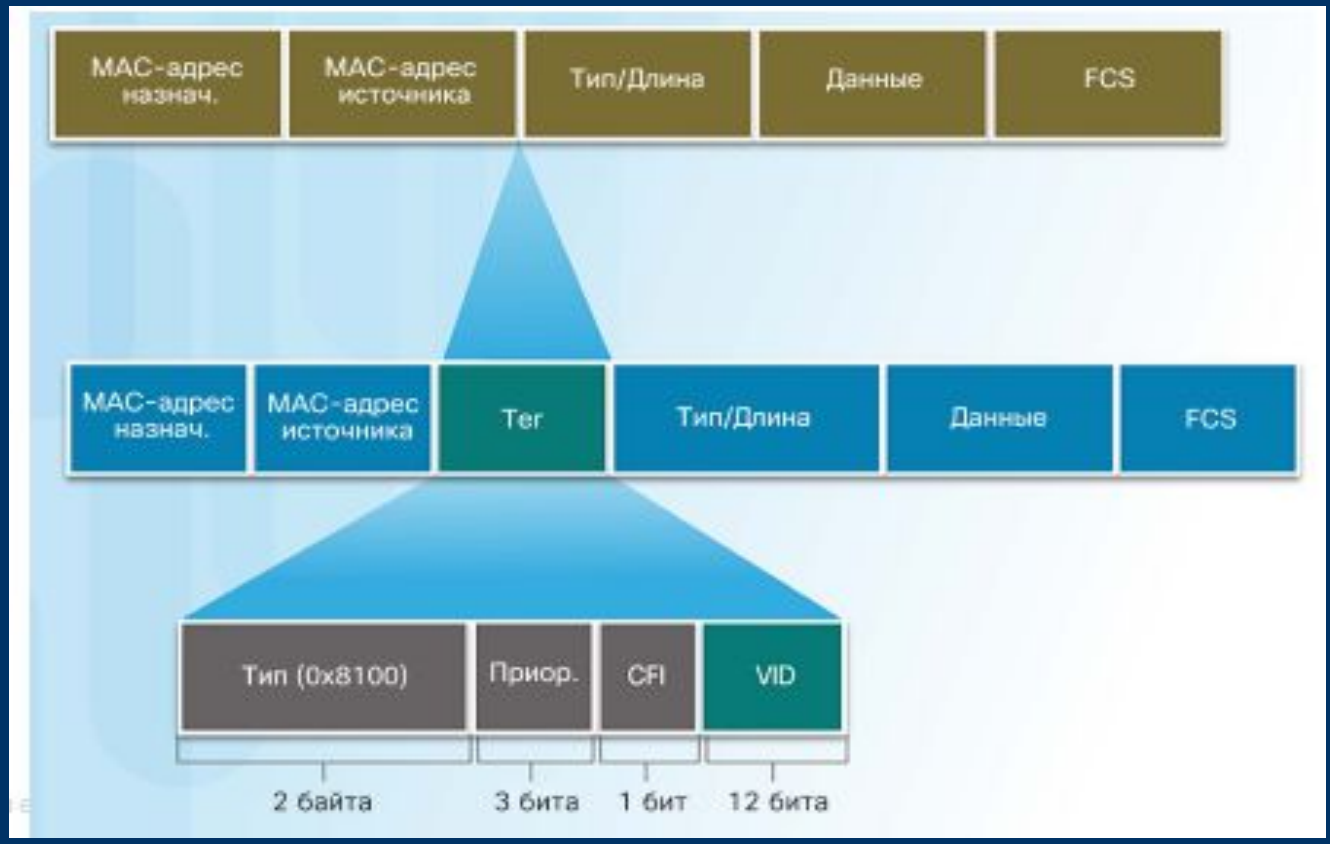
- Магистральные каналы между коммутаторами S2–S1 и S1–S3 выполняют широковещательную рассылку на другие устройства в сети VLAN 10.
- Поскольку эту широковещательную рассылку получают только устройства, которые находятся в этой сети VLAN, ее получит и компьютер PC4.


PC1
Преподаватели
VLAN 10
172.17.10.21/24
PC2
Учащийся
VLAN 20
172.17.20.22/24
S1
F0/1
F0/3
F0/11
F0/1
F0/18
S2
F0/11
F0/3
S3
F0/18
PC4
Преподаватели
VLAN 10
172.17.10.24/24
PC5
Учащийся
VLAN 20
172.17.20.25/24
Транковые каналы сети VLAN настроены для
поддержки сетей VLAN 10 и 20

Коммутаторы Catalyst серии 2960 являются устройствами уровня 2. Они используют информацию заголовка кадра Ethernet для пересылки пакетов. У них нет таблиц маршрутизации. Стандартный заголовок кадра Ethernet не содержит информации о VLAN, которой принадлежит кадр; таким образом, когда кадры Ethernet помещаются в магистраль, необходимо добавить информацию о VLAN, к которым они принадлежат. Этот процесс, называемый тегированием (маркированием), выполняется с помощью заголовка протокола IEEE 802.1Q, указанного в стандарте IEEE 802.1Q. Заголовок 802.1Q включает 4-байтовый тег, вставленный в исходный заголовок кадра Ethernet, определяющий VLAN, к которой принадлежит кадр.

Когда коммутатор получает кадр на порт, настроенный в режиме доступа и которому назначена VLAN, коммутатор вставляет тег VLAN в заголовок кадра, пересчитывает FCS и отправляет тегированный кадр из магистрального порта.

Формат кадра Ethernet с протоколом 802.1Q иллюстрирован на рисунке.



Поле тега VLAN состоит из поля типа, поля информации управления тегом и поля FCS:

Тип - 2-байтовое значение, называемое значением идентификатора протокола тегов (TPID). Для Ethernet это шестнадцатеричное значение 0x8100.
Приоритет пользователя - 3-битное значение, поддерживающее реализацию уровня или службы.
Идентификатор канонического формата (CFI) - 1-битный идентификатор, который позволяет передавать кадры Token Ring по каналам Ethernet.
VLAN ID (VID) - 12-битный идентификационный номер VLAN, который поддерживает до 4096 идентификаторов VLAN.
После того, как коммутатор вставляет поля информации управления типом и тегом, он повторно вычисляет значения FCS и вставляет новый FCS в кадр.

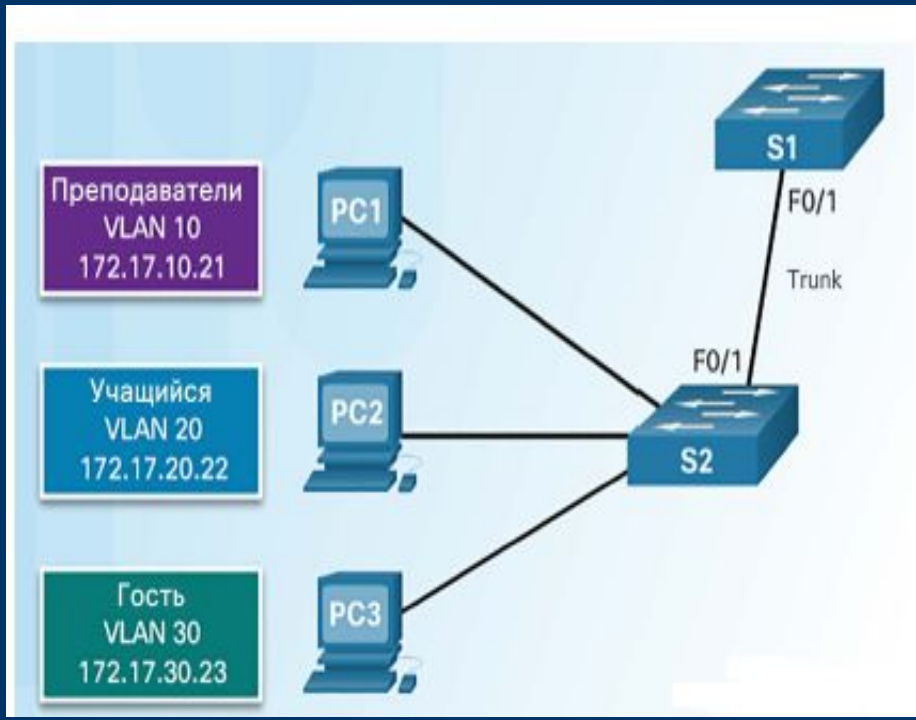
Настройка магистральных портов коммутатора

Магистраль VLAN - это канал OSI уровня 2 между двумя коммутаторами, по которому передается трафик для всех VLAN (если список разрешенных VLAN не ограничен вручную или динамически). Чтобы включить магистральные каналы, настройте порты на обоих концах физического канала с помощью параллельных наборов команд.

Для настройки магистральных портов выполните следующие действия:

- зайдите в глобальный режим — **configure terminal**,
- укажите интерфейс для конфигурации магистрального порта — **interface interface_id**,
- настройте канал в качестве магистрального — **switchport mode trunk**,
- укажите список сетей VLAN, которым разрешен доступ в магистральный канал — **switchport trunk allowed vlan** *vlan_list*,
- возвратитесь в привилегированный режим — **end**,
- просмотрите настройки и сохраните — **copy running-config startup config**.

На рисунке VLAN 10, 20 и 30 поддерживают компьютеры преподавателей, студентов и гостевые компьютеры (ПК1, ПК2 и ПК3). Порт F0 / 1 на коммутаторе S1 настроен как магистральный порт и пересылает трафик для VLAN 10, 20 и 30.




```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Примечание . Эта конфигурация предполагает использование коммутаторов Cisco Catalyst 2960, которые автоматически используют инкапсуляцию 802.1Q на магистральных каналах. Для других коммутаторов может потребоваться ручная настройка инкапсуляции.

На рисунке представлены команды для сброса магистрали в состояние по умолчанию.

Команды коммутатора Cisco под управлением ОС IOS

Войдите в режим глобальной настройки.	`S1# configure terminal`
Войдите в режим интерфейсной конфигурации.	`S1(config)# interface interface id`
Разрешите доступ к магистральному каналу для всех сетей VLAN.	`S1(config-if)# no switchport trunk allowed vlan`
Вернитесь в привилегированный исполнительский режим.	`S1(config-if)# end`

Настройка магистрали проверяется с помощью команды **switchport show interfaces** *interface_id*.

Верхняя выделенная область на рисунке показывает, что порт F0 / 1 имеет административный режим, установленный на магистральный . Порт находится в транкинговом режиме. Далее в выходных данных нижняя выделенная область показывает, что все VLAN включены на магистрали.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```