Построение корпоративных сетей

Доц. каф. ИиВМ Русакова М.С.

специальность «МОАИС»
3 курс, 6 семестр
36 часов лекций, 18 часов лаб. работ
зачет

Литература

- Материалы лекций
- Материалы лекций по курсу «Архитектура вычислительных систем и компьютерных сетей»
- Электронные ресурсы локальной академии Cisco в локальной сети СамГУ
- Ресурсы электронных библиотек в сети Интернет
- Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 3-е изд. – СПб.: Питер, 2007 (реком. МО) (29 экз)
- Олифер, Виктор Григорьевич. Сетевые операционные системы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. - 2-е изд. - СПб.: Питер, 2009. - 668 с.: ил., табл. - (Учебник для вузов). (Допущ. МО) (30 экз)
- Степанов, Анатолий Николаевич. Архитектура вычислительных систем и компьютерных сетей: Учебное пособие для вузов / А.Н. Степанов. - СПб: Питер, 2007. - 509 с.: ил. - (Учебное пособие). (Реком. МО) (150 экз)

Литература

- Таненбаум, Эндрю. Архитектура компьютера: Пер. с англ. / Э. Таненбаум. - 4-е изд. - СПб.: Питер, 2006. - 699 с. (1 экз)
- Таненбаум, Эндрю С. Компьютерные сети: Пер. с англ. / Э. Таненбаум. - 4-е изд. - СПб.: Питер, 2006. - 992 с.: ил. - (Классика computer science). (1 экз)
- Битнер, Владимир Иванович. Принципы и протоколы взаимодействия телекоммуникационных сетей: учеб. пособие для вузов / В.И. Битнер. - М.: Горячая линия-Телеком, 2008. - 272 с.: ил. - (Специальность). (Реком. УМО) (1 экз)
- Досталек, Либор. TCP/IP и DNS в теории и на практике: Полное руководство: Пер. с чеш. / Л. Досталек, А. Кабелова; Рус. изд. под ред. М. В. Финкова, А.В. Анисимова. - СПб: Наука и техника, 2006. - 608с.: ил. - (Полное руководство). (1 экз)
- Родичев, Юрий Андреевич. Компьютерные сети: Архитектура, технологии, защита: Учеб. пособие для вузов / Ю.А. Родичев; Самарский гос. ун-т. Каф. Безопасности информационных систем. - Самара: Универс-групп, 2006. - 466с. (50 экз)
- Никифоров, Сергей Васильевич. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие для вузов / С.В. Никифоров. - 2-е изд. - М.: Финансы и статистика, 2007. - 224 с.: ил. (Реком. УМО) (1 экз)

Литература

- Дроздова, Елена Николаевна. Компьютерные сети: компоненты, протоколы, технологии: Учебное пособие для вузов / Е.Н. Дроздова. - СПб.: Петербургский ин-т печати, 2006. - 160 с.: ил. (Реком. УМО) (1 экз)
- Основы построения систем и сетей передачи информации: учебное пособие для вузов / В.В. Ломовицкий [и др.]; Под ред. В.М. Щекотихина. - М.: Горячая линия - Телеком, 2005. - 382 с.: ил. - (Для высших учебных заведений. Специальность). (Реком. УМО) (1 экз)
- Лапонина, Ольга Робертовна. Межсетевое экранирование: учеб. пособие для вузов / О.Р. Лапонина. - М.: Интернет-Ун-т Информ. Технологий: Бином. Лаборатория знаний, 2007. - 343 с.: ил., табл. - (Основы информационных технологий). (7 экз)
- Одом, Уэнделл. Компьютерные сети. Первый шаг: пер. с англ. / У. Одом. - М.: Вильямс, 2006. - 432с: ил. - (Первый шаг).. - (Cisco Systems). (1 экз)
- Бигелоу, Стивен Дж. Сети: поиск неисправностей, поддержка и восстановление: Пер. с англ. / С.Дж. Бигелоу. - СПб: БХВ-Петербург, 2005. - 1200 с.: ил. - (Системный администратор). (1 экз)

Литература

- Палмер, Майкл. Проектирование и внедрение компьютерных сетей: Учебный курс: Пер. с англ. / М. Палмер, Р.Б. Синклер. - 2 изд., пер. и доп. - СПб: БХВ-Петербург, 2004. - 752 с.: ил (1 экз)
- Заика, Александр Александрович. Компьютерные сети / А.А. Заика. - М.: ОЛМА-ПРЕСС, 2006. - 448 с. - (Стань профи!). (1 экз)
- Поляк-Брагинский А. Компьютерная сеть своими руками: популярный самоучитель. - СПб.: Питер, 2004. - 334 с. - (Популярный самоучитель). (5 экз)
- Поляк-Брагинский А. Обслуживание и модернизация локальных сетей / А. Поляк-Брагинский. - СПб.: Питер, 2005. - 350 с.: ил. - (Популярный самоучитель). (1экз)
- Поляк-Брагинский, Александр Владимирович. Сеть своими руками / А.В. Поляк-Брагинский. - 2-е изд.,перераб. и доп. - СПб: БХВ-Петербург, 2006. - 432 с.: ил. - (Создаем сеть дома и в офисе). (1 экз)
- Таненбаум Э. Эталонные сетевые модели // Мир Internet – 2002. – N10. – С.78-81, статья www.iworld.ru
- www.cisco.com – материалы компании Cisco

Обзор курса

- Основные понятия теории компьютерных сетей
  - понятие сети
  - топологии сетей
  - виды сетевых устройств
  - виды сетевых кабелей
  - модель OSI
  - физическая и логическая адресация
  - широковещательная рассылка
  - домен коллизий
  - IP-адресация
  - структура сообщения
- Описание корпоративной сети
- Планирование сетевой адресации
- Первоначальная настройка сетевых устройств
- Маршрутизация
- Коммутация
- Виртуальные локальные сети
- Адресация в корпоративной сети
- Каналы корпоративной сети WAN
- Списки контроля доступа
- Диагностика и устранение неполадок в сети

Основные понятия

- **Компьютерная сеть** - вычислительная система, в которой осуществляется независимое использование машин, объединенных линиями связи.
  - Это по сути распределенная система, в которой компьютеры используются независимым способом.
  - Связь осуществляется через так называемые **сетевые адаптеры** и пространственно протяженные **линии связи.**
  - Каждый подключенный к сети компьютер работает под управлением имеющей специальные сетевые возможности собственной ОС. Общая операционная система отсутствует.
  - Взаимодействие происходит при помощи **сообщений**, передаваемых по линиям связи. С их помощью передаются данные и запрашиваются необходимые ресурсы.

Основные понятия

- **Линии связи –** совокупность устройств, которые используются для передачи информации, выполняющих при этом операции кодирования, декодирования, преобразования, передачи или приема сообщений.
- Протяженная в пространстве среда, «через» которую осуществляется передача сообщения называется **каналом связи**. Канал является важнейшей составной частью внешней линии связи.

- **Кадром** называется совокупность битов, передаваемых по последовательной линии связи за один сеанс передачи. Эта совокупность содержит одну или несколько групп информационных битов, а также одну или несколько групп служебных битов обеспечивающих правильную передачу (адрес получателя, адрес отправителя, контрольные суммы и т.д.).

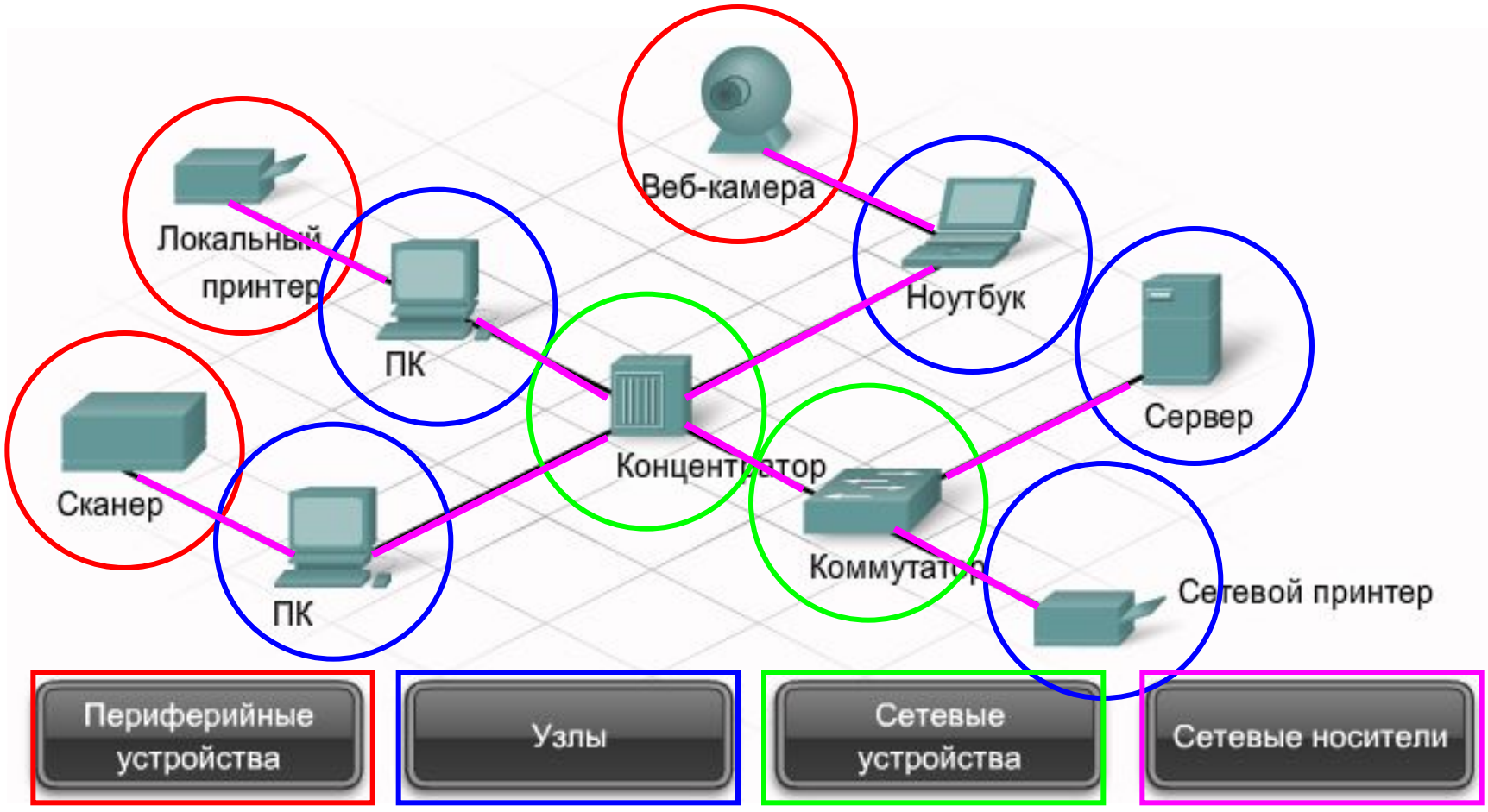
Поля кадра стандарта IEEE 802.3 Ethernet

Байт	Имя поля
7	Преамбула
1	Признак начала кадра
6	MAC-адрес получателя
6	MAC-адрес отправителя
2	Поле Длина/тип
с 46 по 1500	Инкапсулированные данные
4	Контрольная последовательность кадра (циклическая контрольная сумма пакета (CRC))

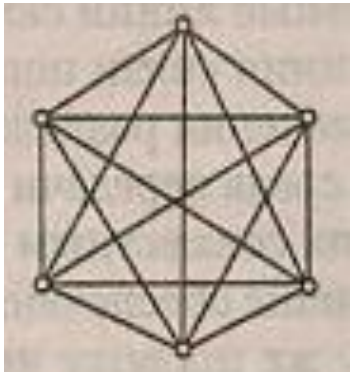
Основные понятия

- **Интерфейсом** называется стандартизированный и унифицированный набор аппаратных и программных средств, а также набор правил передачи информации по линиям связи.
- По протяженности компьютерные сети часто подразделяют на несколько основных групп:
  - **Локальные сети** (**ЛВС** — Локальная Вычислительная Сеть или **LAN** — Local Area Network)
  - **Городские сети** (**MAN** — Metropolitan Area Network)
  - **Территориальные** или **региональные** сети (**WAN** — Wide Area Network)
  - **Глобальные сети** (ГВС — Глобальная Вычислительная Сеть, global network).

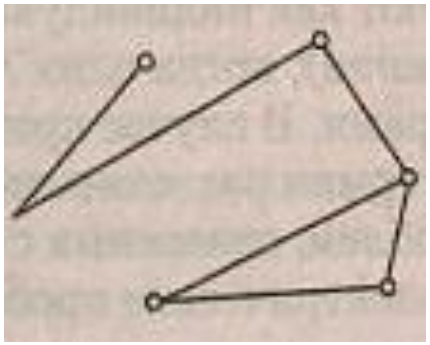
Категории компонентов сети



Топология сети - способ организации физических соединений между компьютерами сети

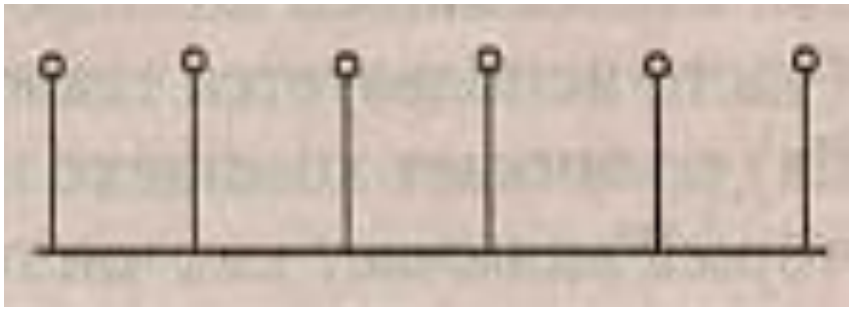


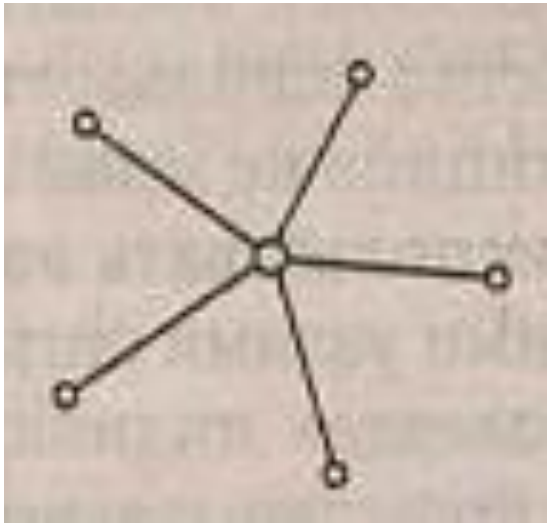
- **Полносвязная** топология — сеть, в которой каждый компьютер сети связан индивидуальной линией со всеми остальными узлами. Полносвязная топология плохо масштабируемая и дорогая. Нужен отдельный порт и отдельная линия для связи каждого узла сети с каждым другим узлом. Применяется в многомашинных системах и в сетях с небольшим количеством узлов.



- **Ячеистая** топология. Из полносвязной топологии удаляются линии, с низким объёмом передаваемой информации. Ячеистая топология характерна для глобальных сетей.

Топологии сети





- Топология **общей шины**.

Основные достоинства шинной топологии:

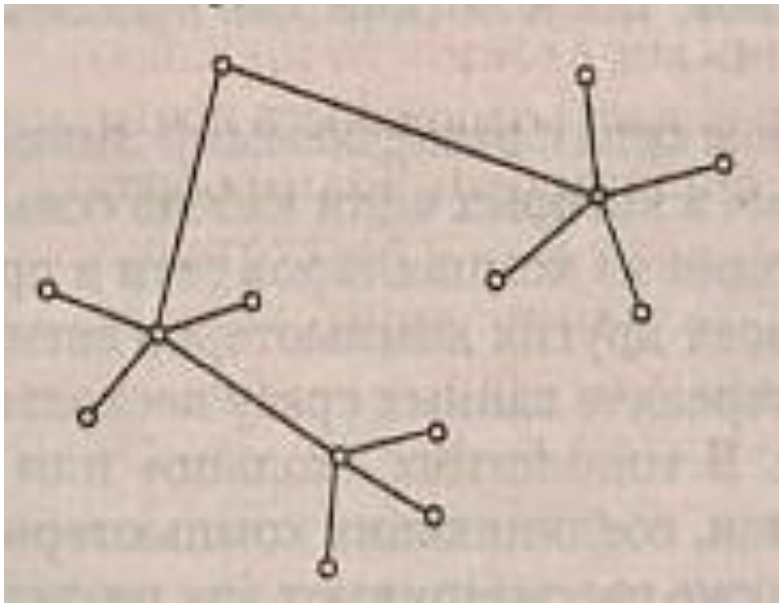
- низкая стоимость монтажа;
- унифицированный способ подключения;
- хорошая масштабируемость;
- мгновенный широковещательный режим передачи.

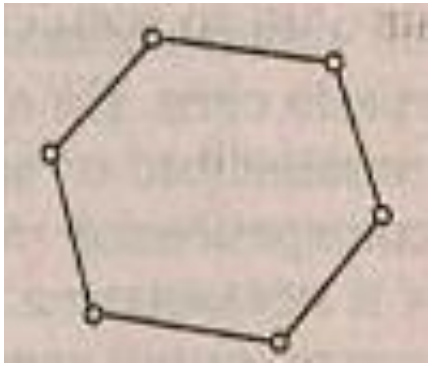
- Топология **звезда**.

Основные достоинства звезды:

- более высокая надёжность по сравнению с шинной топологией;
- высокая конфиденциальность с помощью организации контроля за поступающими в центральное устройство сообщениями.

Топологии сети





- Топология **иерархическая звезда**.

- Топология **кольцо**. Данные передаются по замкнутым в кольцо линям связи от одного узла к другому. Это похоже на шинную топологию, в которой концы шины соединены друг с другом. Свойства также похожи на шинную топологию. Удобно при необходимости организовывать обратную связь между узлами.

Адресация в сетях

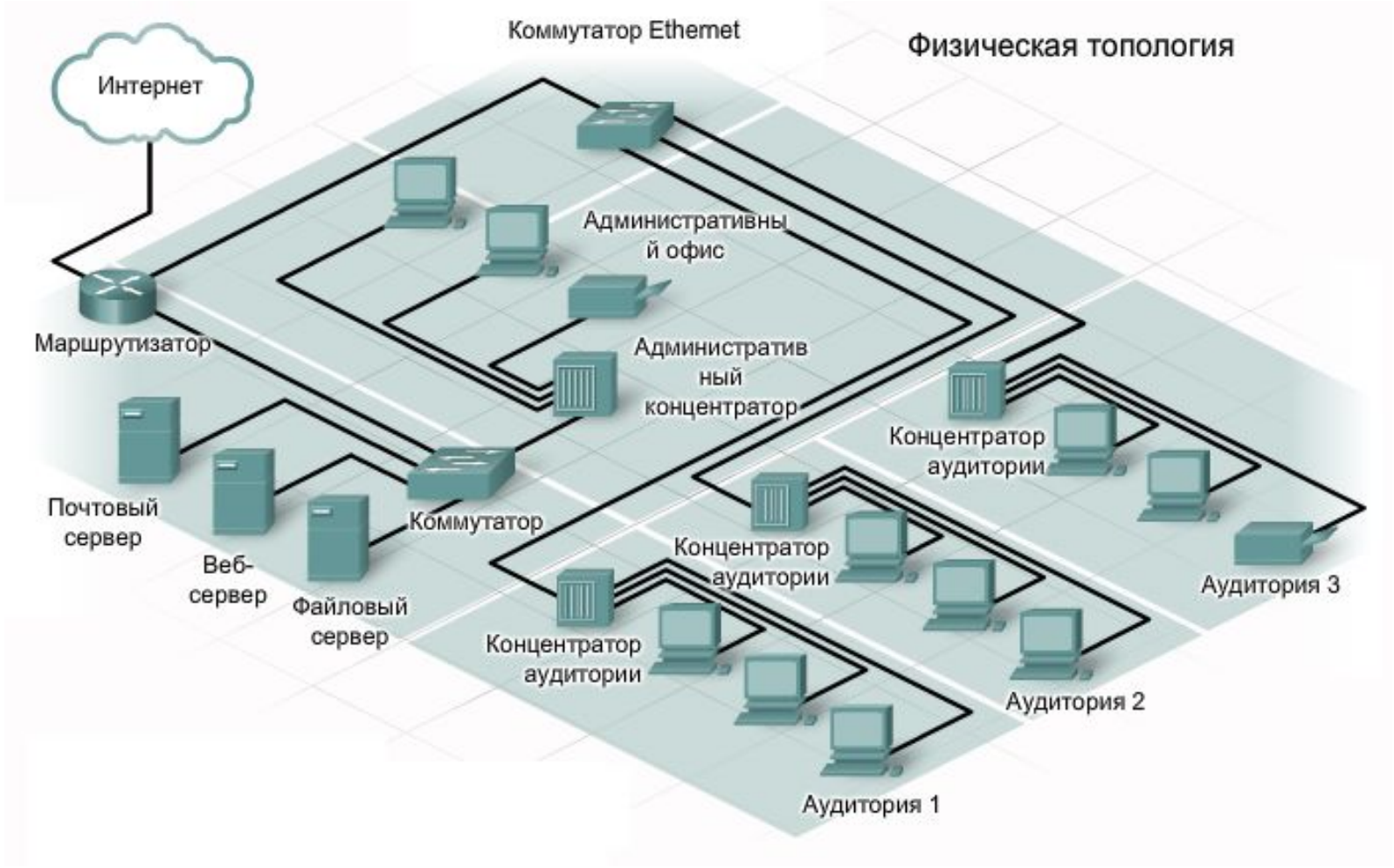
- Адрес узла сети должен удовлетворять следующим требованиям:
  - уникальность любого компьютера в сети любого масштаба и типа;
  - минимум вероятности дублирования имён;
  - удобство работы;
  - компактность;
  - иерархическая структура (наподобие почтового адреса).

Основные схемы адресации

- **Аппаратная** (физическая) адресация в двоичной или шестнадцатеричной системе.
  - Пример аппаратного адреса: 009AF917718DCA700, 00-1B-77-C3-1C-3A (так называемый, MAC-адрес – адрес управления доступом к среде).
  - Используется в малых и средних по количеству узлов сетях.
  - Адреса не имеют иерархической структуры. Формируются и используются аппаратурой автоматически либо фиксируются на заводе изготовителе.
  - Недостаток: при необходимости замены части оборудования может возникнуть потребность в серьезной перестройке сети.
- **Имена** или **символьные адреса** (логическая адресация).
  - Примеры адресов: Newton, Star, Mars, Jupiter.
  - Могут иметь иерархическую структуру ─ доменная адресация в сети Интернет: ssu.samara.ru.
  - Удобны для использования людьми, так как обычно имеют смысловую нагрузку. Назначаются администраторами локальных и глобальных сетей.
- **Числовые составные адреса** (логическая адресация).
  - Пример: 219.09.154.21. Это IP ─ адресация в сети Интернет.
  - Фактически пользователь задает доменный, символический адрес. Сервер DNS переводит его в IP-адрес, а на конечном этапе, в локальной сети аппаратура использует аппаратную схему адресации.

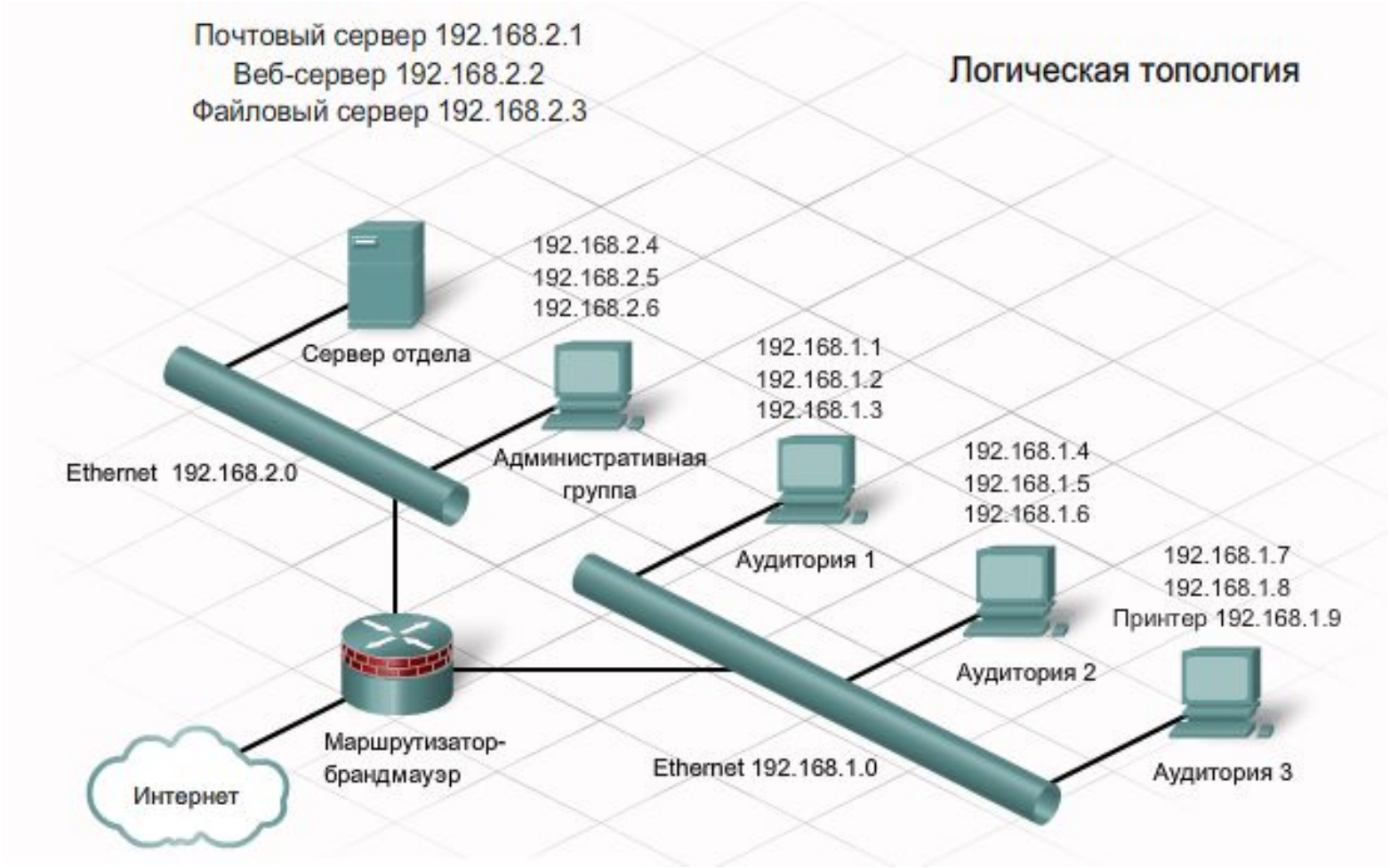
Физическая и логическая структуризация сетей

- При монтаже сетей составляется карта физической топологии, на которой указано положение каждого узла и его подключения к сети. Кроме того, там помечены все провода и сетевые устройства, соединяющие узлы.



Физическая и логическая структуризация сетей

- Помимо топологической карты физических устройств, иногда приходится строить логическое представление топологии сети. На логической топологической карте узлы группируются по методам использования сети, независимо от местоположения. На такой карте можно указать имена и адреса узлов, информацию о группах и приложениях.

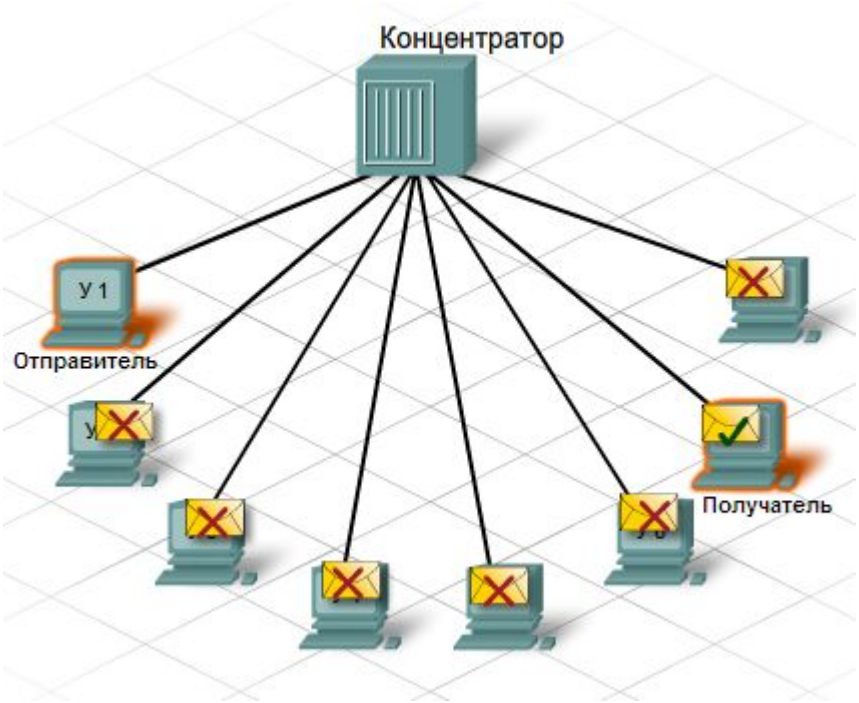


Коммуникационные устройства, используемые в сетях

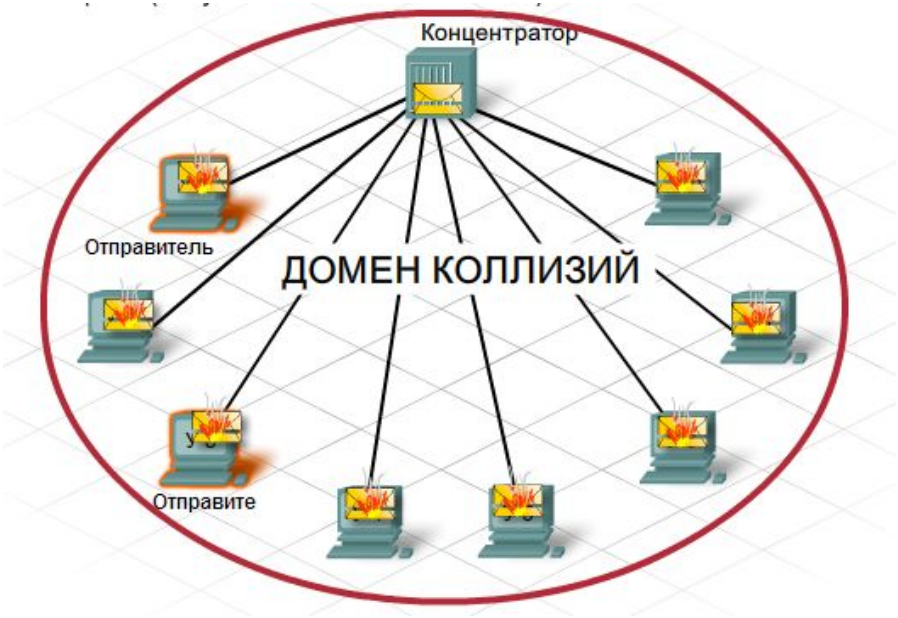
- **Повторители** — устройства, используемые для физического соединения сегментов кабеля с целью увеличения общей длины сети. Повторитель передает сигнал, приходящий из одного сегмента сети, в соседний сегмент.

- Повторители, которые имеют несколько портов (разъёмов) и соединяют более двух кабельных **сегментов** называются **концентраторами** или **хабами**.

  - Концентраторы - это простые устройства, не оборудованные необходимыми электронными компонентами для передачи сообщений между узлами в сети. Он просто принимает электронные сигнал одного порта и воспроизводит (или повторяет) то же сообщение для всех остальных портов.



Домен коллизий

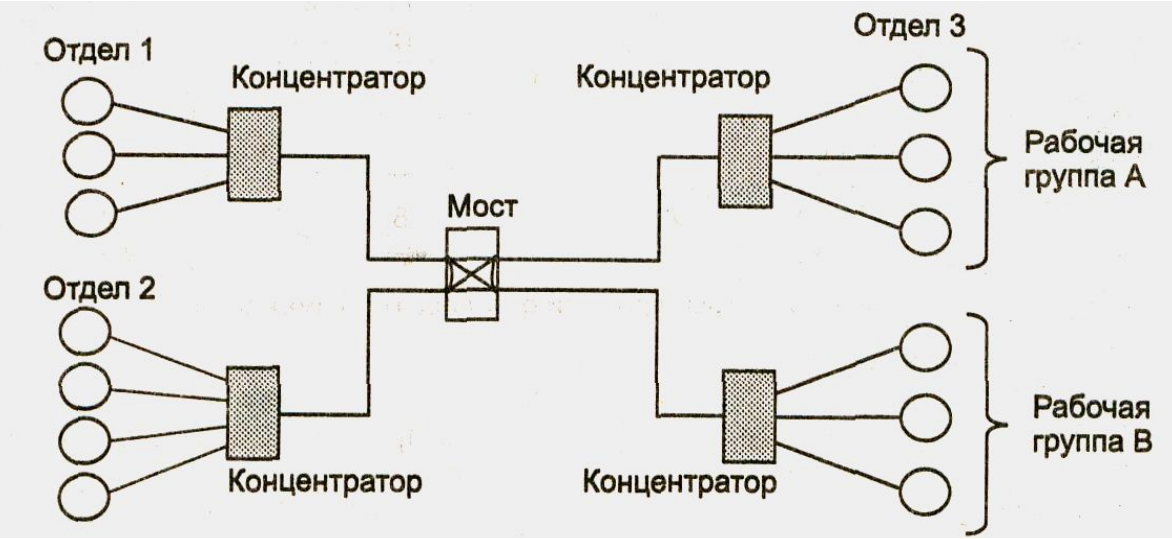


- Через концентратор можно одновременно отправлять только одно сообщение. Возможно, два или более узла, подключенные к одному концентратору, попытаются одновременно отправить сообщение. При этом происходит столкновение (**коллизия**) электронных сигналов, из которых состоит сообщение.

- Столкнувшиеся сообщения искажаются, в результате чего они не могут быть прочтены узлами. Поскольку концентратор не декодирует сообщение, он не обнаруживает, что оно искажено, и повторяет его всем портам. Область сети, в которой узел может получить искаженное при столкновении сообщение, называется **доменом коллизий**.

Коммуникационные устройства, используемые в сетях

- Для логической структуризации сети используются коммуникационные устройства: **мосты**, **коммутаторы**, **маршрутизаторы** и **шлюзы.**
- **Мост** делит сеть на части — логические сегменты, осуществляя передачу кадра из одного сегмента в другой только при явной адресации к узлу из другого сегмента.
- **Шлюзы** используются для объедения сетей с различными типами аппаратного и программного обеспечения.

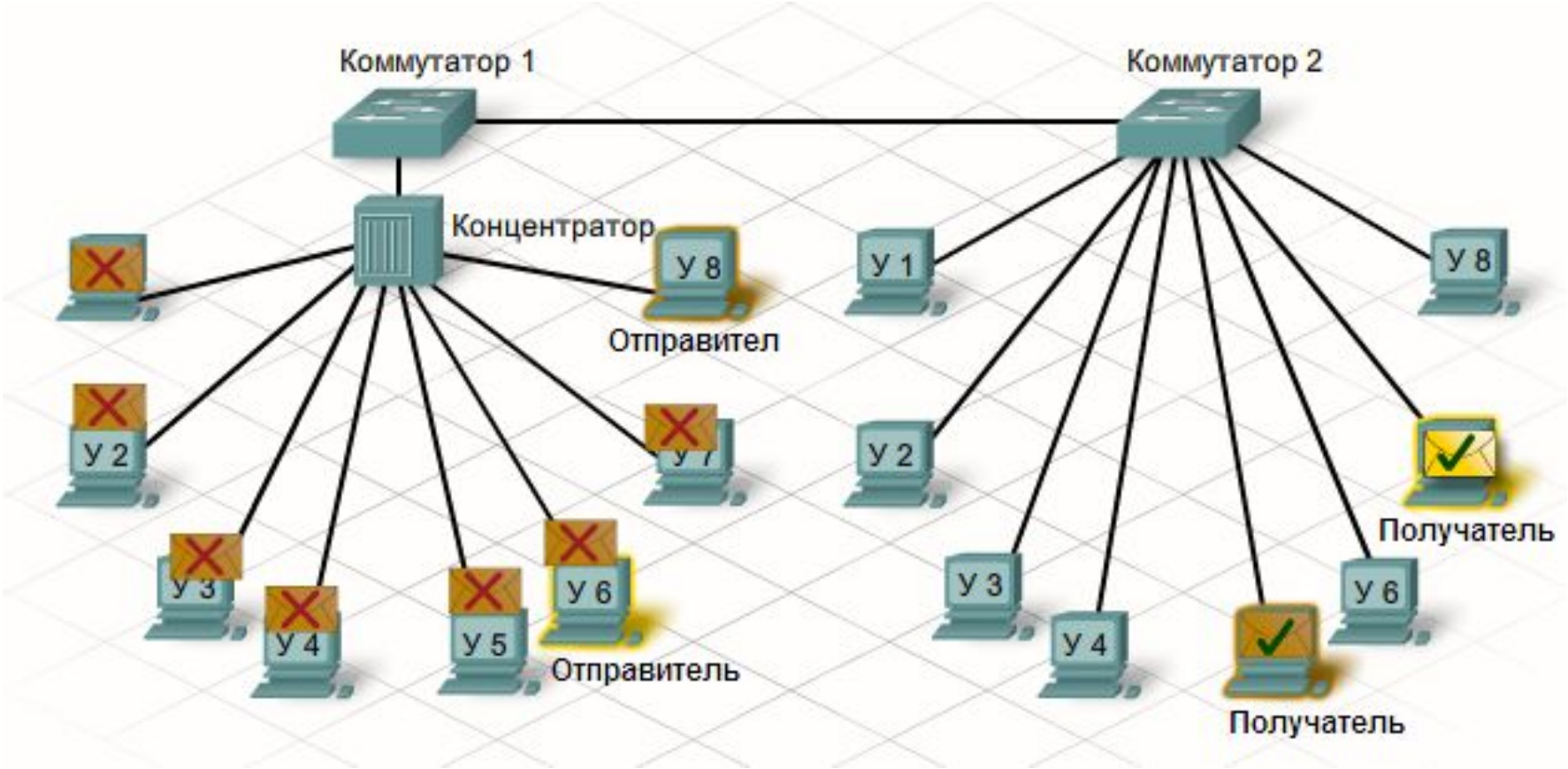


Коммутатор

- **Коммутаторы** отличается от моста тем, что он осуществляет обработку кадров, поступающих от разных узлов в параллельном режиме.
- Как и концентратор, **коммутатор** соединяет несколько узлов с сетью. В отличие от концентратора, коммутатор в состоянии передать сообщение конкретному узлу. Когда узел отправляет сообщение другому узлу через коммутатор, тот принимает и декодирует кадры и считывает физический (MAC) адрес сообщения.

Таблица MAC-адресов			
fa0/1	fa0/2	fa0/3	fa0/4
260.8c01.0000	260.8c01.1111	260.8c01.2222	260.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260.8c01.4444	260.8c01.5555	260.8c01.6666	260.8c01.7777

Коммутатор


Коммутатор 1
Коммутатор 2
Концентратор
У 8
Отправитель
У 1
У 8
У 2
У 2
Получатель
У 3
У 6
У 4
У 5
Отправитель
У 3
У 4
У 6
Получатель

Широковещательная рассылка

- Если узлы подключаются через коммутатор или концентратор, образуется **единая локальная сеть**. В локальной сети одному узлу часто приходится одновременно рассылать сообщения всем остальным узлам. Для этого используется так называемая **широковещательная рассылка** сообщений.

- Шестнадцатеричный MAC-адрес широковещательной рассылки выглядит как FFFF.FFFF.FFFF.

- Когда узел получает сообщение на адрес широковещательной рассылки, он его принимает и обрабатывает так же, как и те, что адресованы ему. Когда узел отправляет широковещательное сообщение, концентраторы и коммутаторы его передают всем подключенным к одной локальной сети узлам. Из-за этого локальная сеть иначе называется **домен широковещательной рассылки**.

Address Resolution Protocol

- В локальной сети узел принимает кадр только в том случае, если он отправлен на **MAC-адрес** широковещательной рассылки или **MAC-адрес** сетевого адаптера. При этом большинство сетевых приложений находят серверы и клиенты только по логическому IP-адресу.
- С помощью IP-протокола, который называется **Address Resolution Protocol** (ARP) можно определить MAC-адрес любого узла из той же локальной сети. При наличии IP-адреса узла ARP определяет и сохраняет MAC-адрес узла в локальной сети в три этапа.
  - Отправляющий узел создает и отправляет кадр по MAC-адресу широковещательной рассылки. В кадре находится сообщение с IP-адресом узла назначения.
  - Каждый сетевой узел получает этот кадр и сравнивает IP-адрес из сообщения со своим. Узел с соответствующим IP-адресом посылает отправителю свой MAC-адрес.
  - Отправитель получает сообщение и сохраняет MAC-адрес и IP-адрес в таблице ARP.
- Когда MAC-адрес получателя оказывается в таблице ARP отправителя, появляется возможность отправлять кадры напрямую, минуя запрос ARP.

Маршрутизаторы

- **Маршрутизаторы** образуют логические сегменты с помощью явно заданной иерархии адресов, в которых присутствуют номера подсетей.
- **Маршрутизатор** – это сетевое устройство, связывающее локальные сети. Они направляют трафик и выполняют другие важные для эффективной работы сети функции. Как и коммутаторы, маршрутизаторы могут декодировать и читать полученные сообщения. В отличие от коммутаторов, которые декодируют только кадры с MAC-адресом, маршрутизаторы декодируют пакеты, находящиеся внутри кадра.

Маршрутизатор

- Каждый порт, или интерфейс, маршрутизатора связан со своей локальной сетью. У каждого маршрутизатора есть **таблица** локально подключенных сетей и их интерфейсов. Кроме того, в этих **таблицах маршрутизации** бывает информация о маршрутах, или путях для подключения к другим локально подключенным удаленным сетям.

- Приняв кадр, маршрутизатор декодирует его и получает пакет с IP-адресом получателя. Этот адрес он сравнивает с данными всех сетей из таблицы маршрутизации. Если адрес сети получателя есть в таблице, маршрутизатор инкапсулирует пакет в новый кадр и отправляет. Этот новый кадр направляется в сеть получателя через интерфейс, относящийся к выбранному пути. Процесс перенаправления пакетов в сеть получателя называется **маршрутизацией**.

- Интерфейсы маршрутизатора не перенаправляют сообщения по MAC-адресу широковещательной рассылки. Поэтому рассылки локальной сети не попадают в другие сети через маршрутизатор.

Маршрутизатор

- Как узел-отправитель определяет MAC-адрес маршрутизатора? Узел получает IP-адрес маршрутизатора на основе адреса шлюза по умолчанию, выбранного в настройках TCP/IP. Адрес **шлюза по умолчанию** - это адрес интерфейса маршрутизатора, подключенного к той же локальной сети, что и узел-источник. Выяснив IP-адрес шлюза по умолчанию, узел сможет определить MAC-адрес, используя протокол ARP. Далее MAC-адрес маршрутизатора помещается в кадр, адресованный узлу из другой сети.

- Маршрутизаторы перемещают данные между локальной и удаленной сетью. Информация хранится в **таблицах ARP** и **таблицах маршрутизации**. В таблицах маршрутизации нет адресов отдельных узлов. В них хранятся адреса сетей и оптимальные пути к ним.

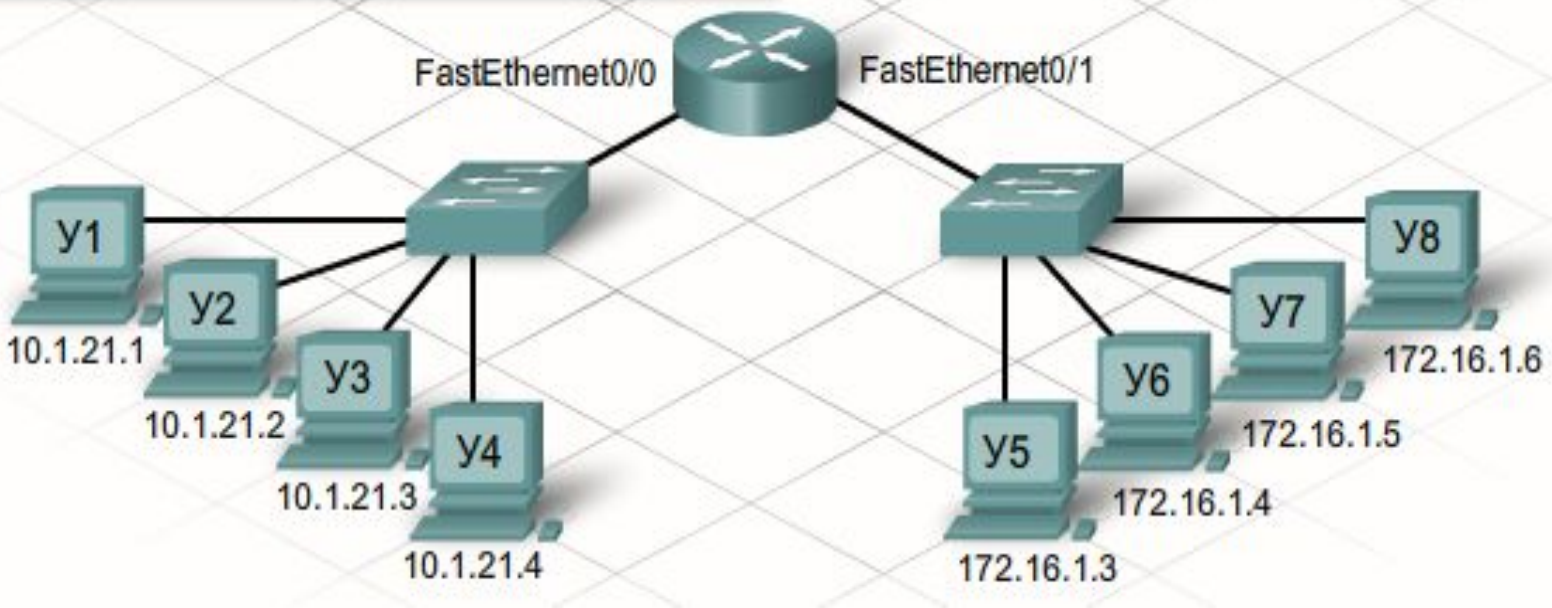
- Чтобы предотвратить сброс, вызванный отсутствием пути к адресату в таблице маршрутизации, сетевые администраторы вводят в таблицу маршрут по умолчанию. Он представляет собой интерфейс, через который маршрутизатор передает пакет с неизвестным IP-адресом сети получателя. Обычно он ведет к другому маршрутизатору, который может передать пакет в сеть получателя.

ARP-таблица

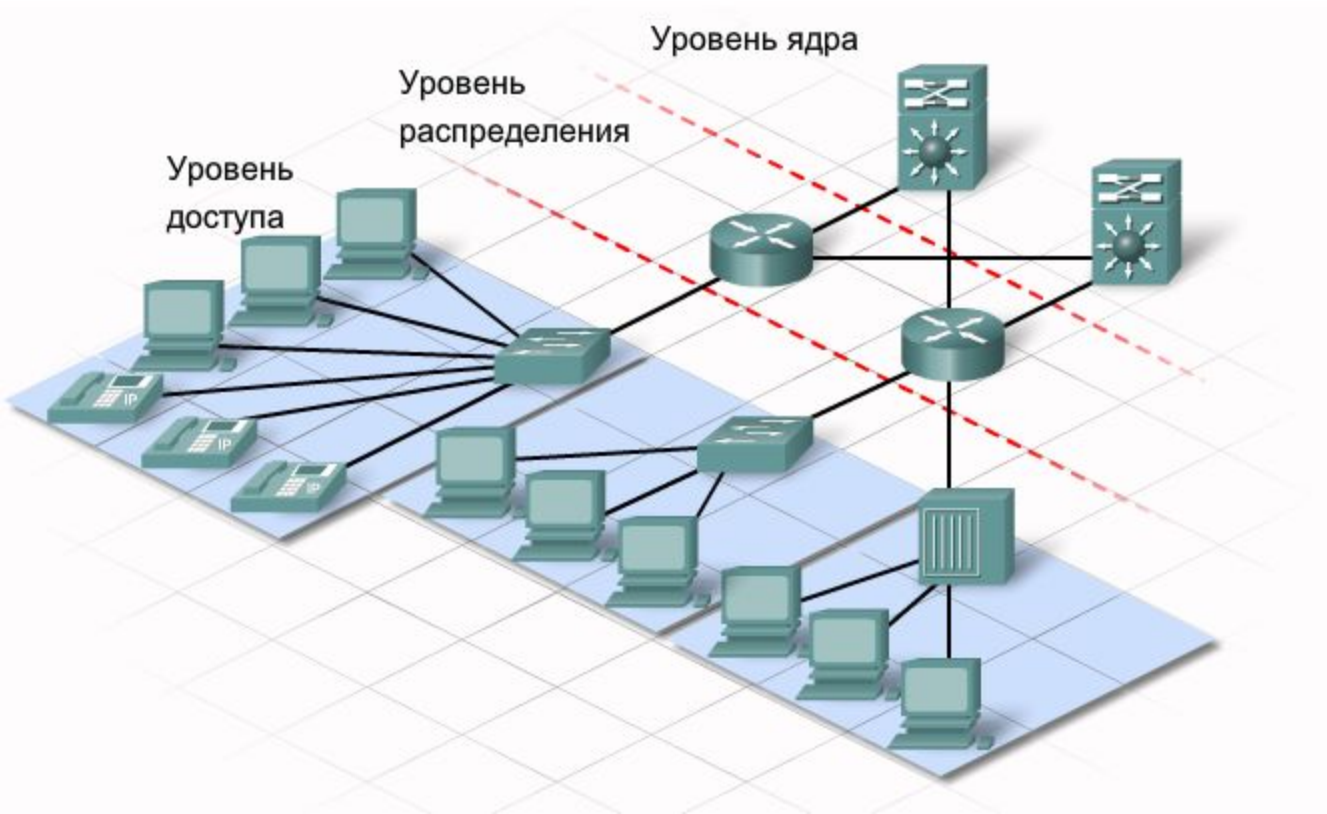
Адрес	Аппаратный адрес	Интерфейс
10.1.21.1	0002.a5ec.c7f9	FastEthernet0/0
10.1.21.2	0012.3fec.fb0d	FastEthernet0/0
10.1.21.3	0014.220e.dac5	FastEthernet0/0
10.1.21.4	00c0.9f4b.8b76	FastEthernet0/0
172.16.1.3	0ac3.a58c.d7f5	FastEthernet0/1
172.16.1.4	0a2f.4fed.dd0d	FastEthernet0/1
172.16.1.5	0b03.3002.ea2d	FastEthernet0/1
172.16.1.6	0d00.a94b.8caa	FastEthernet0/1

Таблица маршрутизации

Тип	Сеть	Порт
C	10.0.0.0/8	FastEthernet0/0
C	172.16.0.0/16	FastEthernet0/1

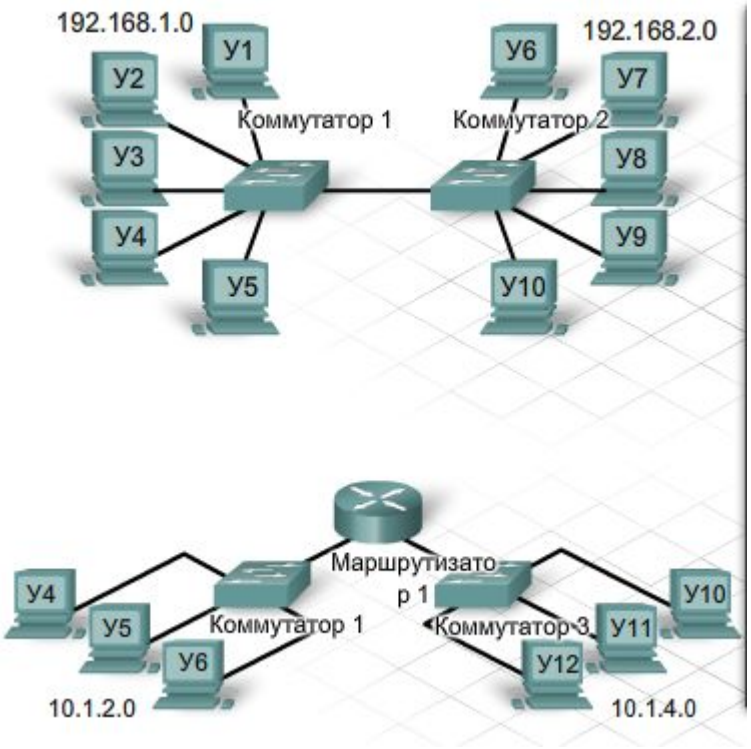


Иерархическая конструкция сети



- В иерархической конструкции есть три базовых уровня:
  - уровень доступа - соединяет узлы в локальной сети;
  - уровень распределения - соединяет небольшие локальные сети;
  - уровень ядра - высокоскоростное соединение между устройствами уровня распределения.

Сегментация локальной сети



- Размещение узлов в одном сегменте локальной сети

Преимущества:

- Подходит для простых сетей
- Простота, более низкая стоимость
- Устройства «видимы» для других устройств
- Высокая скорость передачи данных
- Простота доступа

Недостатки:

- Одна вещательная область – увеличение трафика и снижение скорости обмена данными

- Размещение узлов в удаленных сегментах локальной сети

Преимущества:

- Подходит для сложных сетей
- Сегментирует области вещания и уменьшает трафик
- Улучшение скорости обмена данными в сегменте
- Устройства в разных сегментах могут быть «невидимы» друг другу
- Дополнительная безопасность
- Лучшая организация сети

Недостатки:

- Необходимость маршрутизации
- Маршрутизатор может снизить трафик между сегментами
- Более высокая стоимость

Базовые сетевые технологии

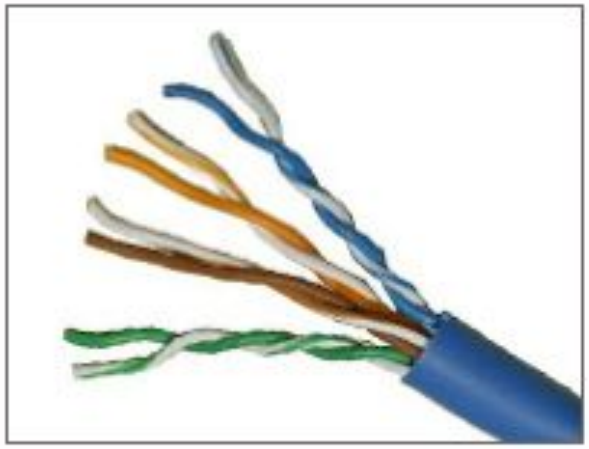
- **Сетевой технологией** называется согласованный набор стандартных соглашений и правил и реализующий их комплекс программно-аппаратных средств, достаточный для построения работоспособной сети.
- В настоящее время существуют следующие базовые сетевые технологии: Ethernet, Token Ring, FDDI, 100VG – Any LAN, Fast Ethernet, Gigabit Ethernet...
  - Token Ring разработан компанией IBM в 1984г. Топология – кольцо с пропускной способностью 16 Мбит/сек. Метод доступа маркерный. Максимальная длина кольца – 4 км, максимальное количество компьютеров – 260. Обладает свойствами повышенной отказоустойчивости по сравнению с Ethernet.
  - FDDI (Fiber Distributed Data Interface) разработан в 1986-1988г. Технология FDDI базируется на технологии Token Ring. Топология – кольцо с пропускной способностью 100 Мбит/сек по двойной волоконно-оптической линии длиной до 100 километров. Метод доступа – маркерный. Максимальное количество компьютеров – 500. Наиболее отказоустойчивая технология локальных сетей.
  - 100VG-Any LAN принят в 1995 году (стандарт IEEE 802.12). Топология – общая шина с пропускной способностью 100 Мбит/сек. Метод доступа Demand Priority, который является развитием случайного метода доступа. Поддерживает форматы кадров технологий Ethernet и Token Ring (отсюда Any LAN – любая локальная сеть).

Развитие стандарта Ethernet

Год	Стандарт	Описание
1973	Ethernet	Изобретена технология Ethernet Робертом Меткалфом (Robert Metcalfe)
1980	Стандарт DIX (DEC, Intel. Xerox)	Корпорации Digital Equipement Corp, Intel, Xerox выпустили стандарт для Ethernet со скоростью передачи данных 10 Мбит/с и передающей средой в виде коаксиального кабеля. Топология – общая шина. Доступ к шине через сетевые адаптеры. Каждый адаптер имеет уникальный аппаратный номер. Передача данных со скоростью 10 Мбит/сек по витой паре, тонкому или толстому коаксиальному или оптоволоконному кабелю. Случайный метод доступа (CSMA/CD) к разделяемой линии связи. Максимальная длина сети 2500 метров, количество компьютеров в сети не более 1024.
1983	IEEE 802.3	Сеть Ethernet, использующая толстый коаксиальный кабель с большей длиной сегмента для передачи данных со скоростью 10 Мбит/с
1985	IEEE 802.3a	Сеть Ethernet, использующая тонкий коаксиальный кабель меньшей длины сегмента для передачи данных со скоростью 10Мбит/с
1990	IEEE 802.3i	Использует витую пару для передачи данных со скоростью 10Мбит/с
1993	IEEE 802.3j	Используется оптоволокно для передачи данных со скоростью 10 Мбит/с
1995	IEEE 802.3u	Стандарт Fast Ethernet – используется витая пара и оптоволокно (или сдвоенная/счетверённая витая пара) для передачи данных со скоростью 100Мбит/с. Топология – общая шина. Случайный метод доступа (CSMA/CD) к разделяемой линии связи.
1998	IEEE 802.3z	Гигабитная сеть Ethernet, использующая оптоволокно
1999	IEEE 802.3ab	Гигабитная сеть Ethernet, использующая витую пару
2002	IEEE 802.3ae	10-гигабитная сеть Ethernet, использующая оптоволокно
2006	IEEE 802.3an	10-гигабитная сеть Ethernet, использующая витую пару

Типы кабелей в технологии Ethernet

- **Витая пара.** В современной технологии Ethernet для подключения устройств чаще всего используется тип кабеля с медными проводниками, который называется витой парой (ВП).
- **Коаксиальный кабель.** Обычно коаксиальные кабели изготавливают из меди или алюминия. Они применяются в кабельном телевидении. Кроме того, таким кабелем соединяются различные компоненты систем спутниковой связи.
- **Оптоволоконный кабель.** Оптоволоконные кабели изготавливаются из стекла или пластика. У них очень высокая пропускная способность, позволяющая передавать большие объемы данных. Оптоволоконные кабели используются в магистральных сетях, на крупных предприятиях и больших информационных центрах. Кроме того, их активно применяют телефонные компании.

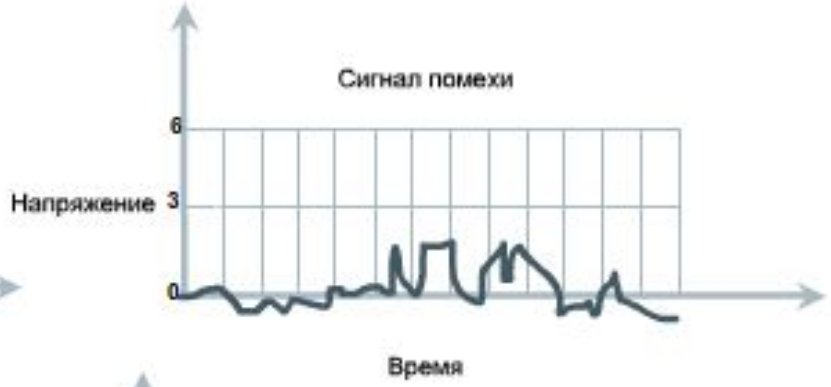


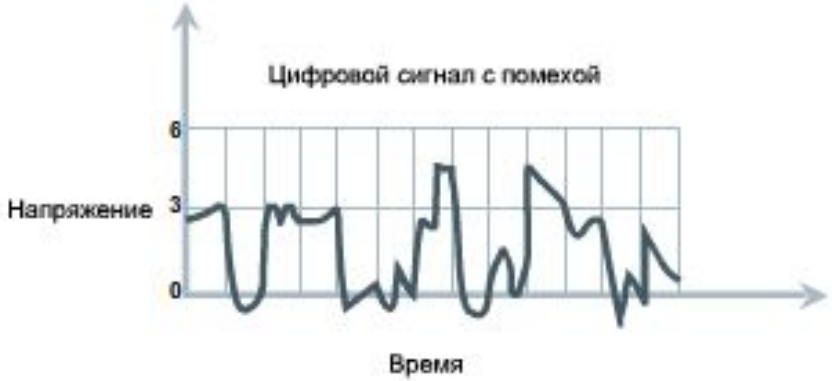
Витая пара

Коаксиальный кабель

Оптоволоконный кабель

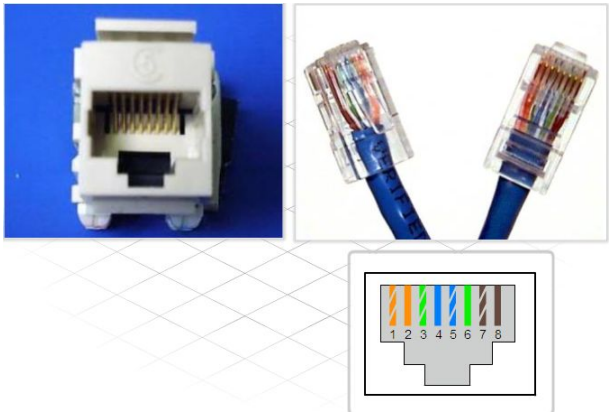
Сигнал, передаваемый по ВП

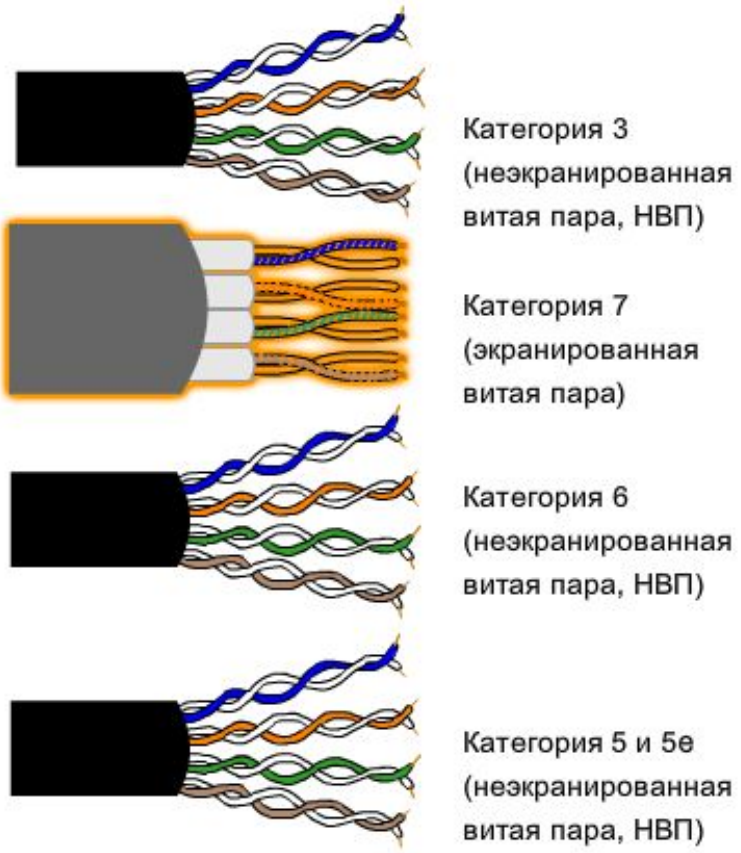




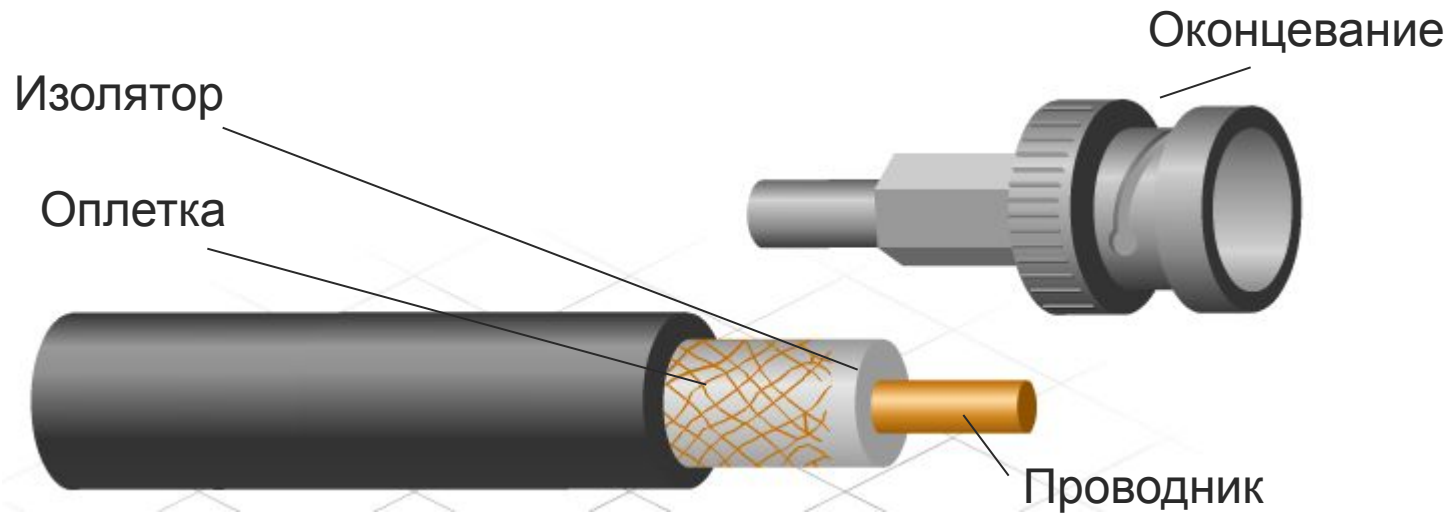
Типы ВП

- Существует <u>три типа витых пар</u>:
  - защищенная витая пара (STP – Shielded Twisted Pair)
  - незащищенная витая пара **(UTP –** Unshielded Twisted Pair**)**
  - экранированная витая пара (ScTP – Screened Twisted Pair)



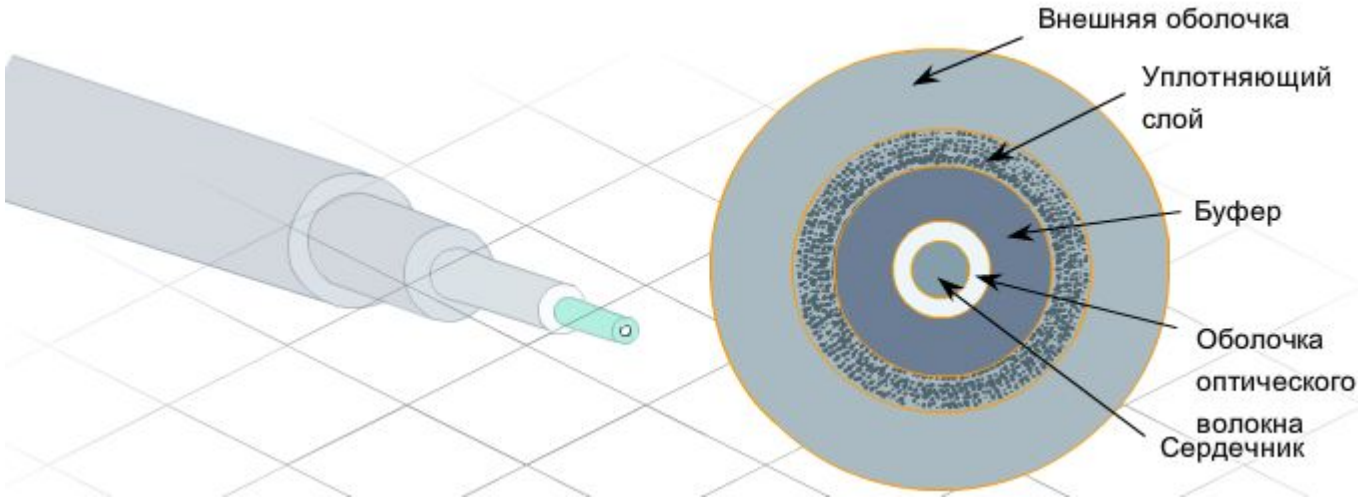


Коаксиальный кабель



- Состав коаксиального кабеля:
  - **Оконцевание**. Обычно оконцовывается разъемом BNC или F-series. BNC-разъем фиксируется поворотом замка на 90 градусов, поэтому считается более прочным соединителем. Разъем типа F-series имеет резьбу и привинчивается.
  - **Оплетка** – обычно изготавливается из алюминия для защиты от помех, вызываемых электромагнитным излучением.
  - **Изолятор** – плохо проводящий материал для защиты от ЭМП и для обеспечения дополнительной гибкости.
  - **Проводник** – центральный элемент кабеля. Материал, проводящий электрический ток, как правило, медь или алюминий.

Оптоволоконный кабель



- **Внешняя оболочка** – защитная, предназначена для защиты от механических повреждений и износа.
- **Уплотняющий слой** защищает кабель от растягивания (например, при вытаскивании).
- **Буфер** нужен в качестве защиты от повреждений.
- **Оболочка** оптоволокна выполняет роль зеркала, которое отражает свет в сердечник кабеля. Предотвращает рассеивание света при его прохождении по кабелю.
- **Сердечник** – светопередающая среда в кабеле. Как правило, выполняется из кварца или стекла.

Одномодовый

Создает прямую траекторию для света

- Небольшой сердечник
- Низкий уровень рассеивания
- Предназначено для использования на длинных дистанциях
- В качестве источников света используются лазеры
- Широко используется в качестве передающей среды высокоскоростных линий длиной несколько тысяч метров в пределах, например, территории учреждения образования

Многомодовый

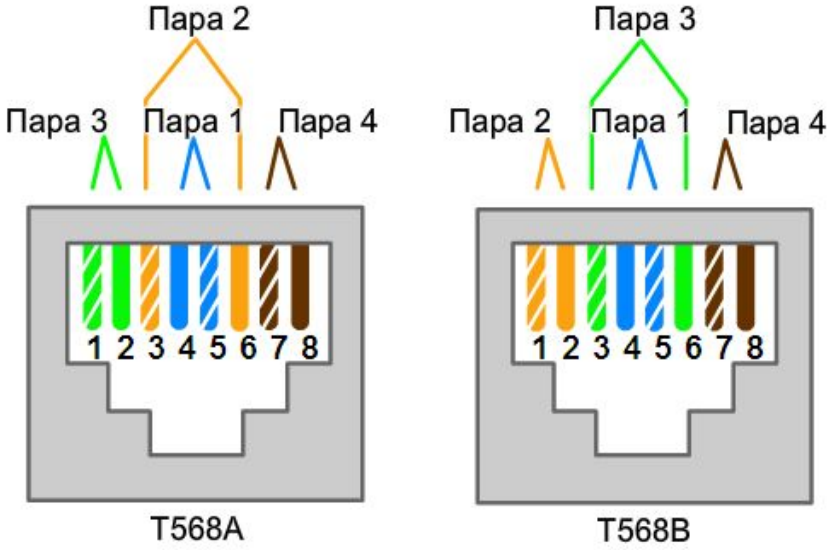
Позволяет свету проходить по нескольким траекториям

- Сердечник больше, чем у одномодовых кабелей
- Допускает более высокий коэффициент рассеивания, а следовательно, потерю сигнала
- Предназначено для использования на длинных дистанциях, но не таких длинных, как одномодовые кабели
- В качестве источников света используются светодиоды
- Широко используется в качестве передающей среды локальных сетей или линий длиной несколько сотен метров в пределах, например, территории учреждения образования

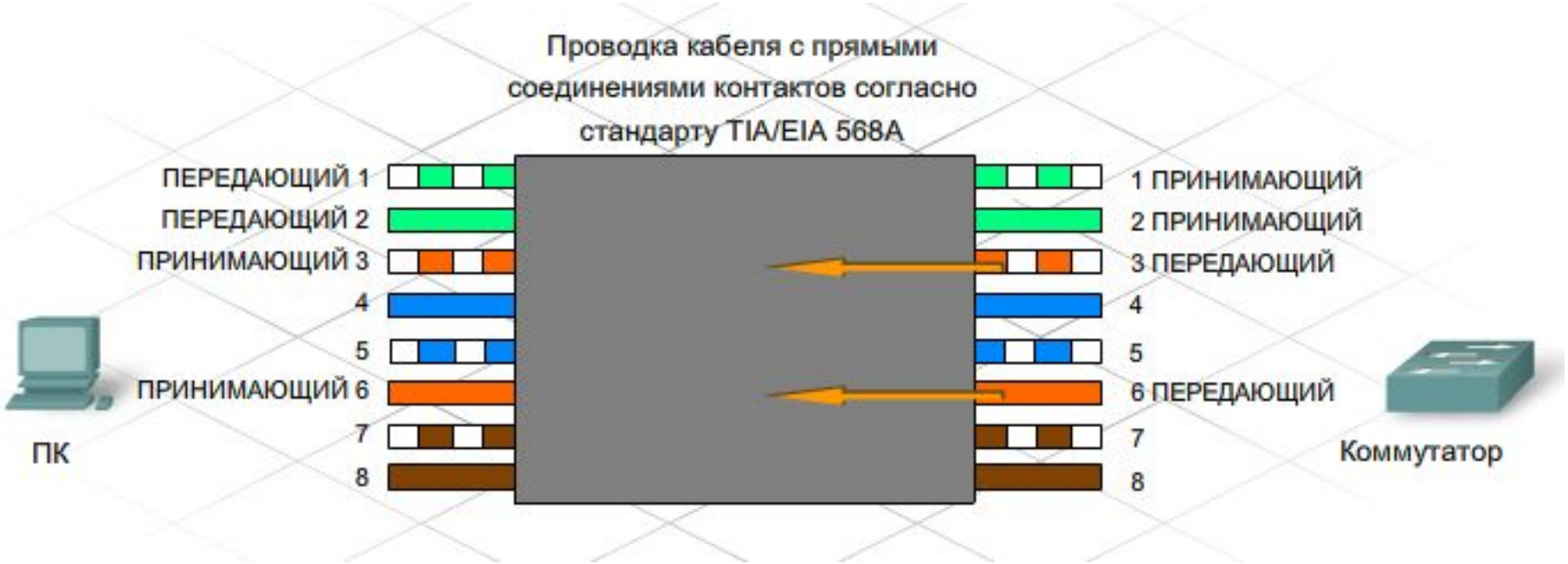
Схемы проводки ВП и типы кабелепроводов

- **Прямой кабель**. Его провод прикреплен к одним и тем же контактов на обоих концах кабеля. Другими словами, если на одном конце кабеля находится разъем T568A, то и на другом будет тот же разъем. Если на одном конце кабеля разъем T568B, на другом тоже разъем T568B. Это означает, что порядок подключения (схема выводов) проводов каждого цвета с обеих сторон совпадает. Схему проводки сети определяет тип прямого кабеля (T568A или T568B).

- **Перекрестный кабель.** В перекрестном кабеле используются обе схемы проводки. На одном конце кабеля находится разъем T568A, на другом - разъем T568B. Это означает, что порядок подключения концов кабелей не совпадает.

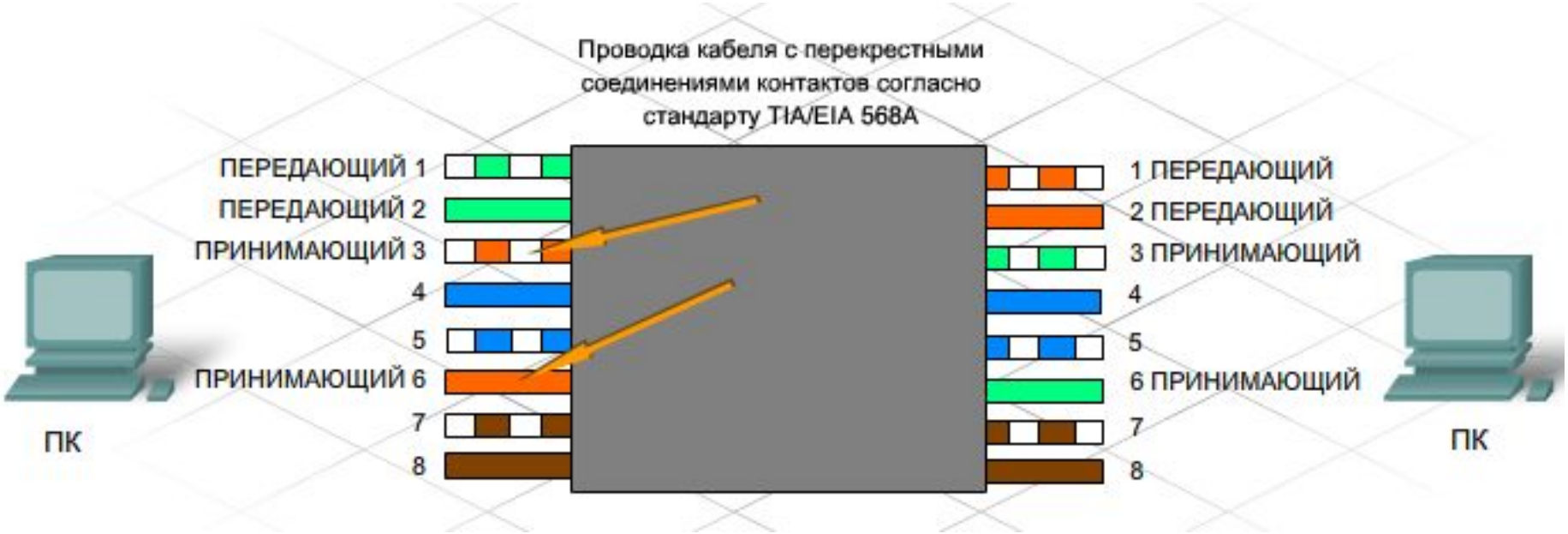


Разнородные устройства



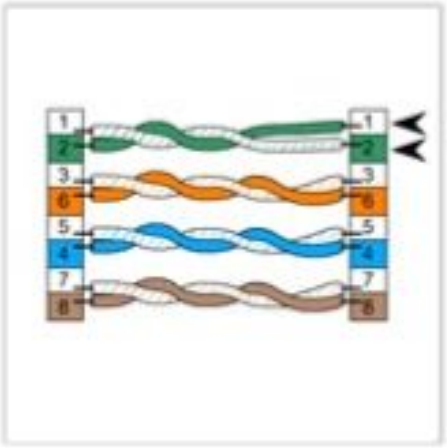
- В разъеме RJ-45 ПК контакты 1 и 2 работают на передачу данных, а контакт 3 и 6 - на прием. В разъеме коммутатора контакты 1 и 2 работают на прием, а контакты 3 и 6 - на передачу. Передающие контакты ПК соответствуют принимающим контактам коммутатора. Следовательно, необходим прямой кабель.
- Примеры разнородных устройств, для которых необходим прямой кабель:
  - порт коммутатора и порт маршрутизатора;
  - порт концентратора и ПК.

Однородные устройства

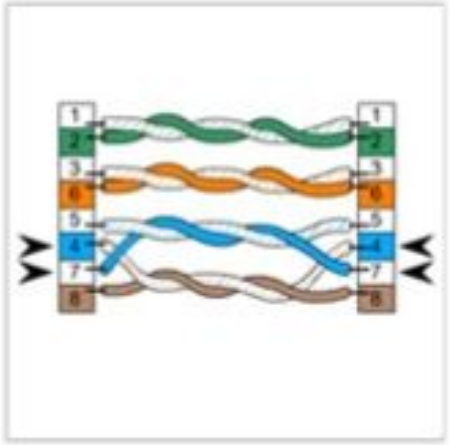


- Если ПК непосредственно подключается к другому ПК, контакты 1 и 2 обоих устройств являются передающими, а контакты 3 и 6 - принимающими. При использовании перекрестного кабеля зеленый провод, подходящий к контактам 1 и 2 (передающим) одного ПК соединяется с контактами 3 и 6 (принимающими) другого ПК.
- Примеры однородных устройств, для которых необходим перекрестный кабель:
  - порт коммутатора и порт коммутатора;
  - порт коммутатора и порт концентратора;
  - порт концентратора и порт концентратора;
  - порт маршрутизатора и порт маршрутизатора;
  - ПК и порт маршрутизатора;
  - ПК и ПК.

Диагностика кабеля

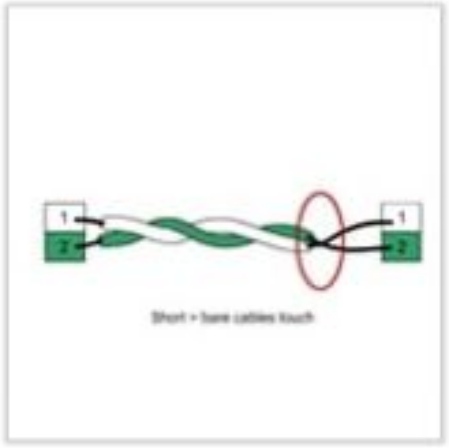


Реверсированная пара



Разделение пар

Обрыв



Короткое замыкание

Кабельный тестер

Кабельный сертификатор

Мультиметр

Рекомендации по подключению кабеля

- Типы кабелей и компонентов сети должны соответствовать обязательным стандартам.
- Необходимо учитывать ограничения по длине, относящиеся к установленным кабелям.
- UTP, как и любой другой кабель с медными проводниками, подвержен воздействию ЭМИ. Важно, чтобы он проходил вдали от источников помех, например, высоковольтных кабелей и флуоресцентных ламп. Возможными источниками помех являются телевизоры, компьютерные мониторы и микроволновые печи.
- Диагностика правильности подключения и работоспособности.
- В процессе монтажа необходимо помечать все кабели и вносить их положение в сетевую документацию.

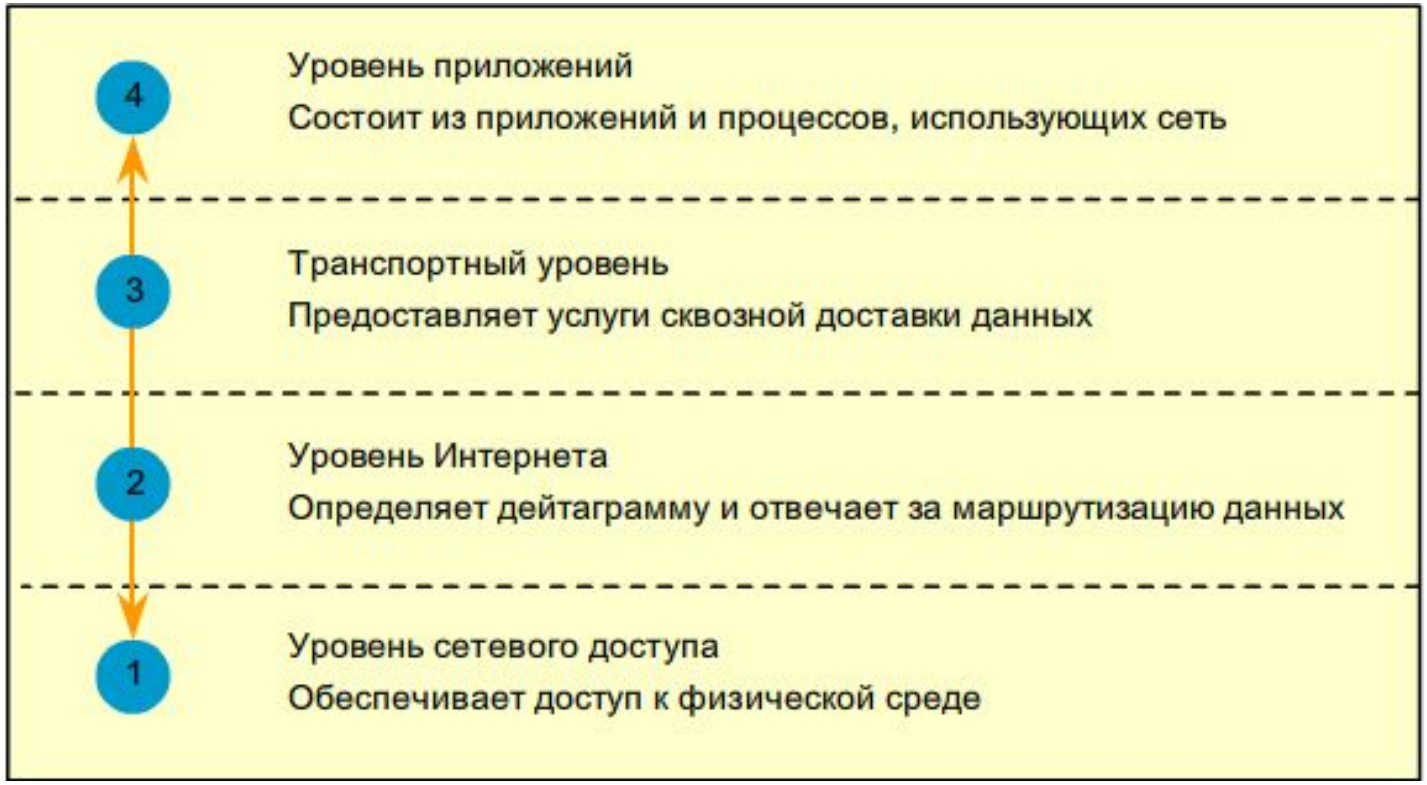
Многоуровневая модель взаимодействия открытых систем

- Организация взаимодействия различных узлов в сети является сложной задачей, для решения которой используется универсальный прием **декомпозиции**, когда решение сложной задачи разбивается на несколько более простых. В данном случае узел сети разбивается на несколько иерархических уровней, на каждом из которых сосредотачивается определенное количество функций. Такой способ организации работы узла называется **многоуровневым подходом**.

- **Базовые принципы многоуровневого подхода**
  - Модули, образующие уровень, формируются таким образом чтобы они обращались только к модулям нижележащих уровней, а результаты работы модулей могут передаваться только вышележащим уровням. На каждом уровне фиксируются его функции, а также межуровневый интерфейс. Эти соглашения обеспечивают относительную независимость уровня и возможность его замены без затрагивания остальных уровней.
  - В широком смысле открытая система это любая система с открытыми (опубликованными) стандартами, содержащими исчерпывающее формализованное описание какого-либо объекта. Под формализацией понимается записанное по определенным правилам, которые позволяют избежать неоднозначность их трактования.
  - Формализованная система правил, определяющих последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах называется **протоколом уровня**.
  - Модули, которые реализуют протоколы соседних уровней одного и того же узла также взаимодействуют друг с другом по чётко определённым правилам, которые образуют **интерфейс**.
  - Иерархически организованный набор протоколов, достаточный для взаимодействия узлов в сети называется **стеком коммуникационных протоколов.**

Модель TCP/IP

- Первая многоуровневая эталонная модель межсетевого взаимодействия была создана в начале 70-х годов и называется моделью сети Интернет. В ней определены четыре обязательных категории функций, необходимых для успешного взаимодействия. Архитектура протоколов TCP/IP построена на основе этой модели. Поэтому модель сети Интернет обычно называют моделью TCP/IP.



Модель взаимодействия открытых систем (OSI)

- Создана в качестве базовой архитектуры, которую разработчики использовали для создания протоколов сетевого взаимодействия.
- В модели OSI представлены все функции или задачи, ассоциированные с межсетевыми взаимодействиями.
- Модель OSI организует задачи на семь групп. Задача или группа задач присваивается каждому из семи уровней модели OSI.
- В модели **OSI** все средства сетевого взаимодействия организованы в семь уровней. Поэтому модель **OSI** часто называют семиуровневой моделью.

  Модель OSI содержит описания следующих уровней:
  - физический;
  - канальный;
  - сетевой;
  - транспортный;
  - сеансовый;
  - представительный;
  - прикладной.

Номер порта назначения	Аббревиатура	Назначение
20	Данные протокола	File Transfer Protocol (для передачи данных)

Сеансовый уровень OSI

Протоколы сеансового уровня обеспечивают фиксацию передающей и принимающей сторон, синхронизацию их взаимодействия, управление диалогом, выставление контрольных точек, позволяющих при сбое осуществлять возврат к контрольной точке, а не началу передачи. Сеансовый уровень часто объединяется с функциями более высоких уровней.

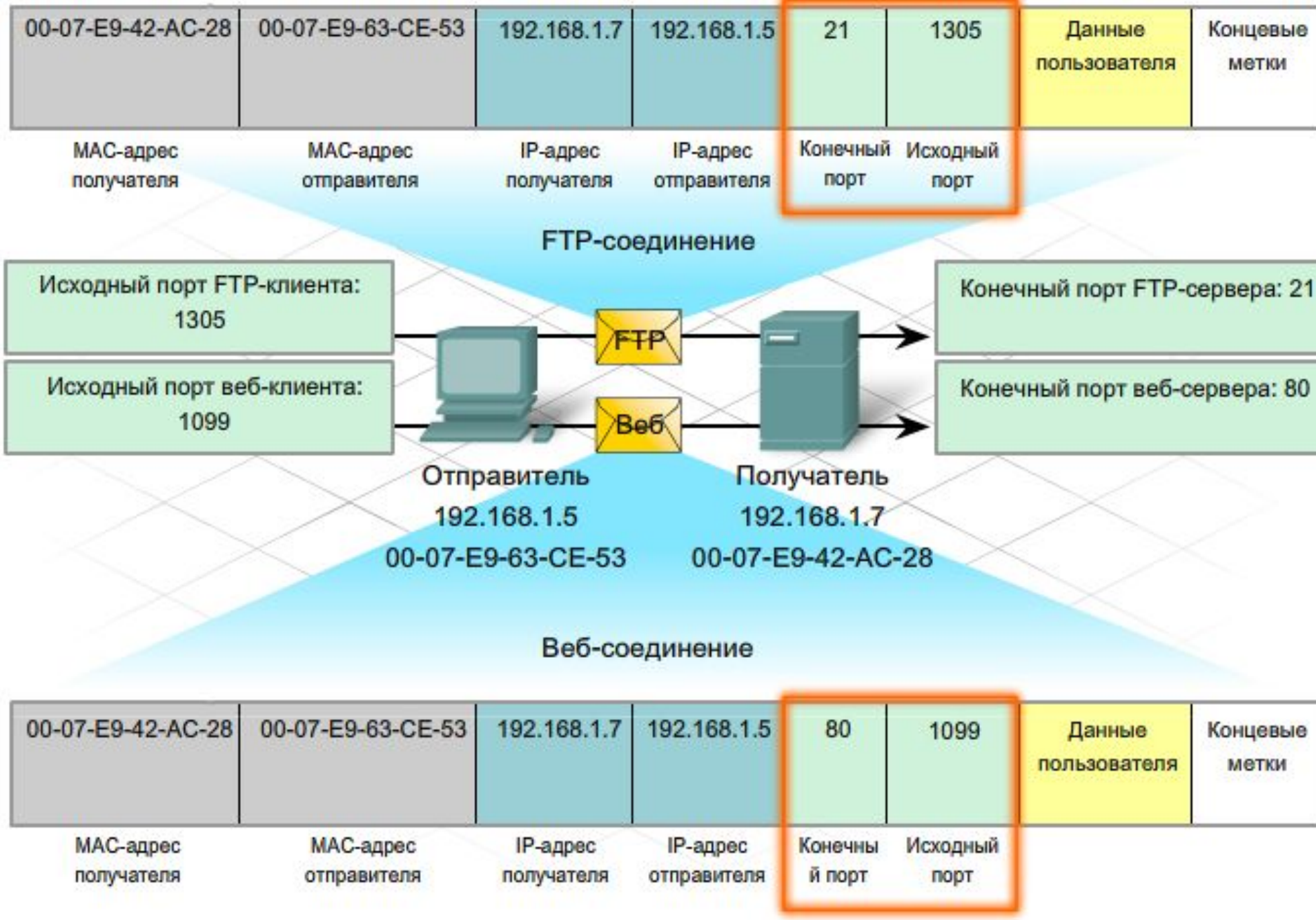
Представительный уровень OSI

Протоколы представительного уровня **OSI** описывают форму представления переданной по сети информации для её передачи на прикладной уровень или в приложение. Фактически эти протоколы определяют способы преобразования информации между различными системами кодировок, использованными при передаче информации по сети. Кроме того, эти протоколы обеспечивают необходимый уровень секретности.

Прикладной уровень OSI

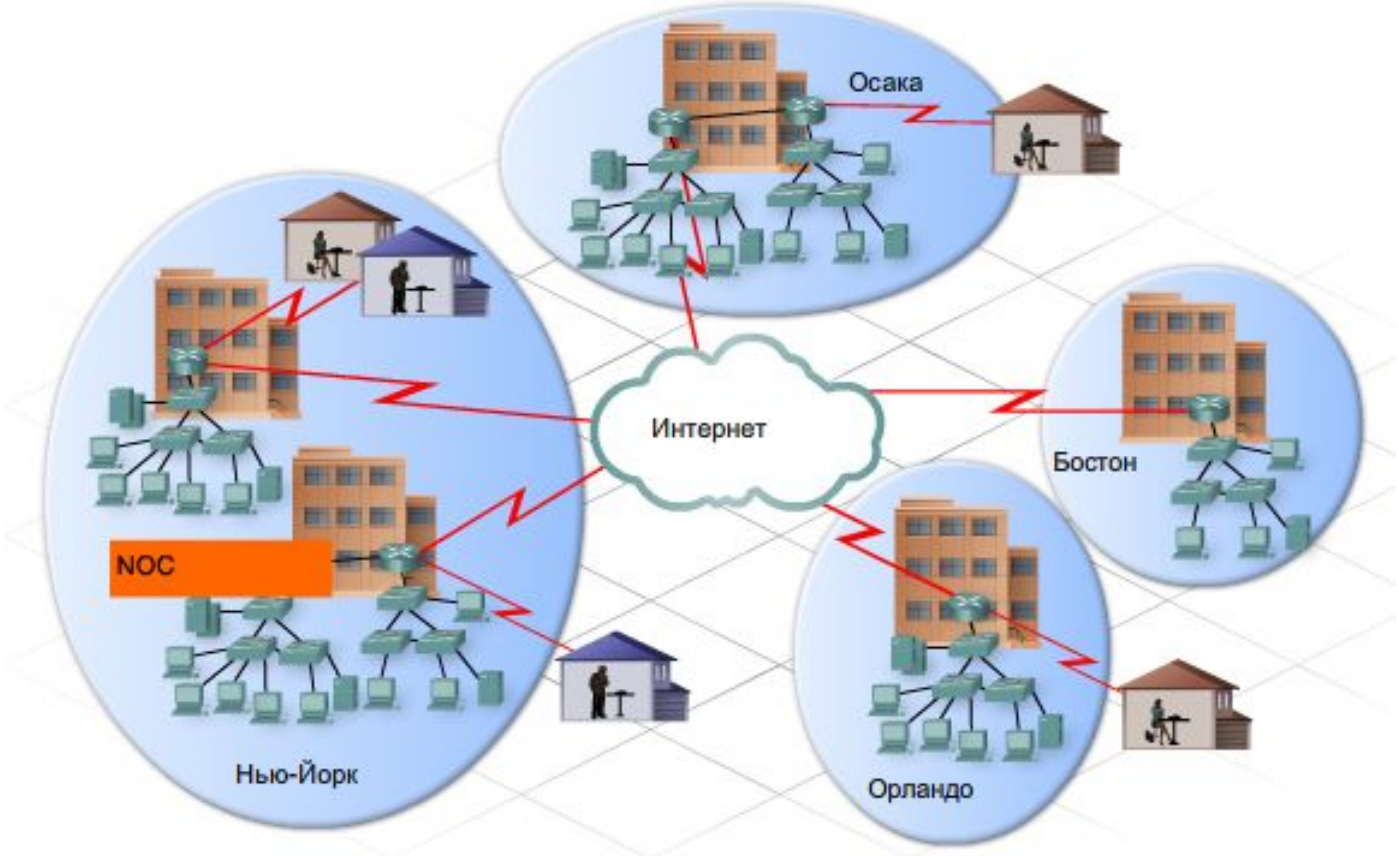
С помощью протоколов представительного уровня пользователь получает доступ к различным сетевым ресурсам. К этому уровню относятся такие протоколы, как FTP, HTTP, Telnet и т.д.

Примеры сетевых протоколов: **IP** и **IPX**.

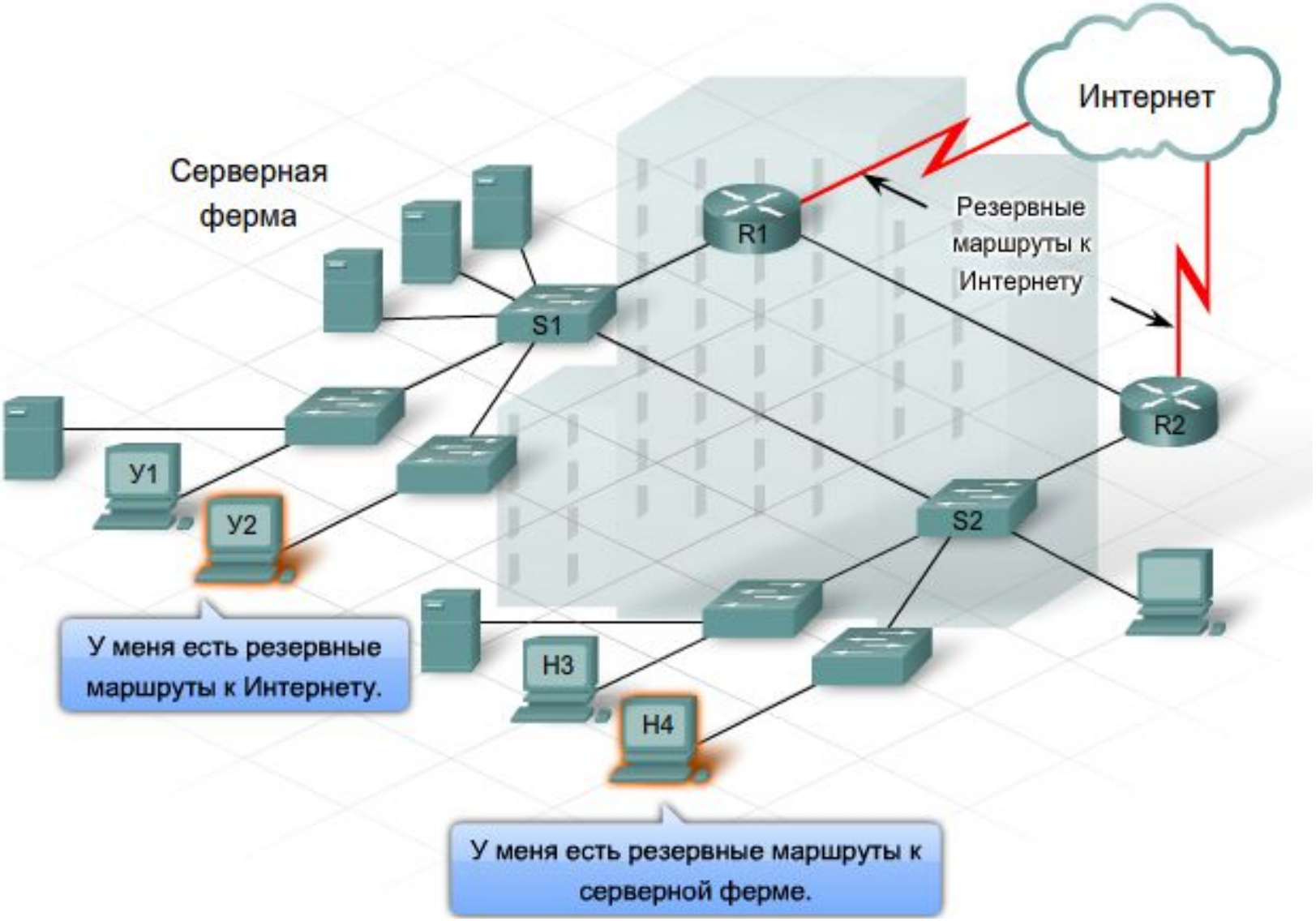

00-07-E9-42-AC-28
00-07-E9-63-CE-53
192.168.1.7
192.168.1.5
21
1305
Данные пользователя
Концевые метки
MAC-адрес получателя
MAC-адрес отправителя
IP-адрес получателя
IP-адрес отправителя
Конечный порт
Исходный порт
FTP-соединение
Исходный порт FTP-клиента: 1305
Исходный порт веб-клиента: 1099
FTP
Веб
Конечный порт FTP-сервера: 21
Конечный порт веб-сервера: 80
Отправитель
192.168.1.5
00-07-E9-63-CE-53
Получатель
192.168.1.7
00-07-E9-42-AC-28
Веб-соединение
00-07-E9-42-AC-28
00-07-E9-63-CE-53
192.168.1.7
192.168.1.5
80
1099
Данные пользователя
Концевые метки
MAC-адрес получателя
MAC-адрес отправителя
IP-адрес получателя
IP-адрес отправителя
Конечный порт
Исходный порт

Описание корпоративной сети

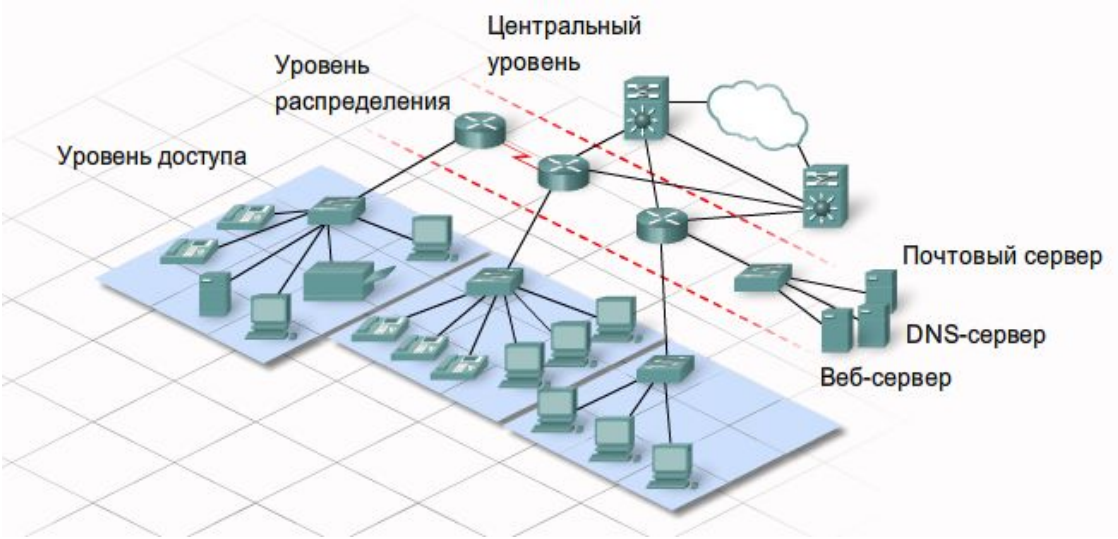
- Среда крупной организации с многочисленными пользователями, площадками и системами называется **предприятием**
- Сеть, используемая для поддержки корпорации, называется **корпоративной сетью**.
- Корпоративные сети имеют множество общих характеристик:
  - поддержка ключевых приложений;
  - поддержка конвергированного сетевого трафика;
  - потребность в централизованном управлении;
  - поддержка разнообразных потребностей бизнеса.



Описание корпоративной сети



Потоки трафика в корпоративной сети



- Уровень доступа:
  - Предоставляет точку для подключения конечных устройств к сети;
  - Позволяет нескольким узлам подключаться к одному сетевому устройству, например, к коммутатору;
  - Существует в одной логической сети;
  - Пересылает трафик другим узлам в той же логической сети;
  - Передает трафик на уровень распределения для доставки сообщения узлу в другой сети.

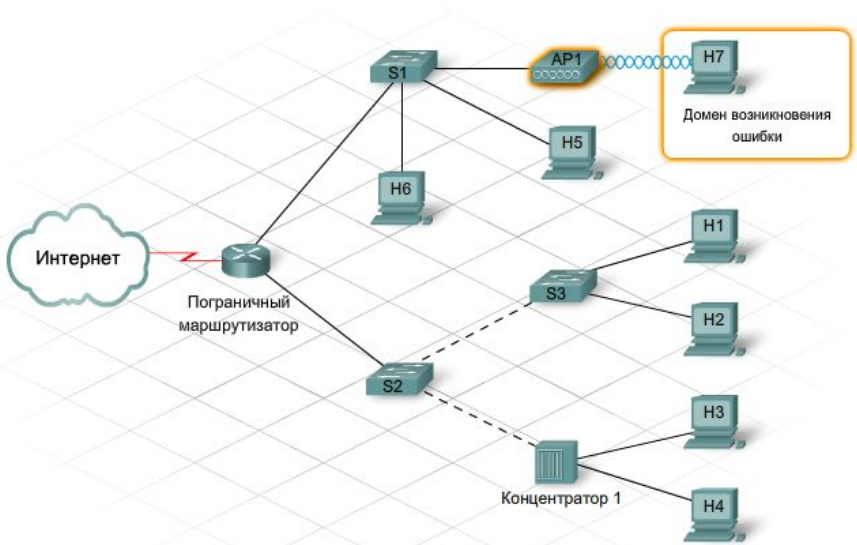
Потоки трафика в корпоративной сети

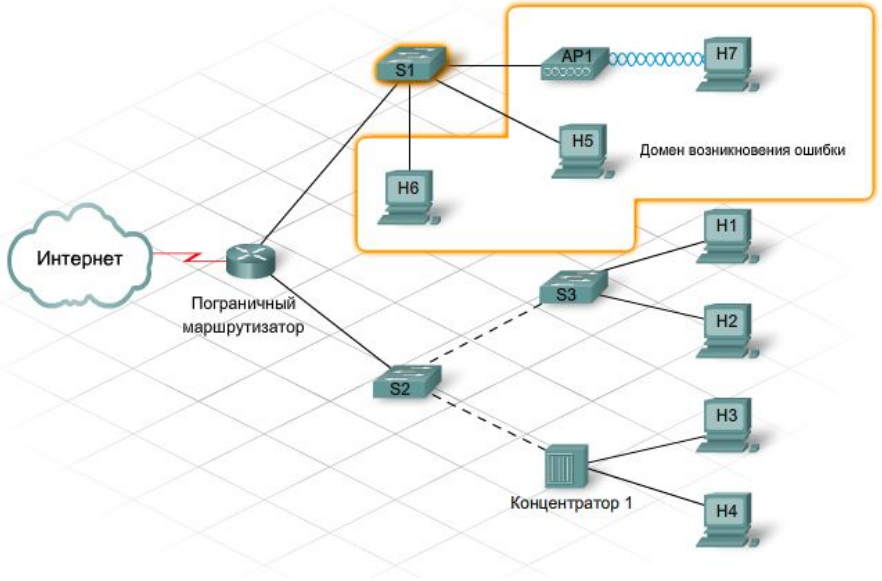
- Уровень распределения:
  - Предоставляет точку подключения для отдельных локальных сетей;
  - Контролирует поток информации между локальными сетями;
  - Гарантирует, что трафик между узлами в одной сети останется локальным;
  - Передает трафик, направленный в другие сети;
  - Фильтрует входящий и исходящий трафик для обеспечения безопасности и управления трафиком;
  - Включает более мощные коммутаторы и маршрутизаторы, чем уровень доступа;
  - Передает данные на центральный уровень для передачи в удаленную сеть.

- Центральный уровень:
  - Обеспечивает магистральный уровень с избыточными (резервными) подключениями;
  - Передает большие объемы данных между несколькими конечными сетями;
  - Включает мощные, высокоскоростные коммутаторы и маршрутизаторы.

- Функциональные компоненты:
  - **Комплекс зданий предприятия**: включает инфраструктуру комплекса зданий с серверными фермами и средствами управления сетью;
  - **Граница корпорации**: включает модули Интернета, VPN и WAN, которые соединяют корпорацию с сетью поставщика услуг;
  - **Граница поставщика услуг**: предоставляет услуги Интернета, телефонной сети общего пользования (ТСОП) и WAN.

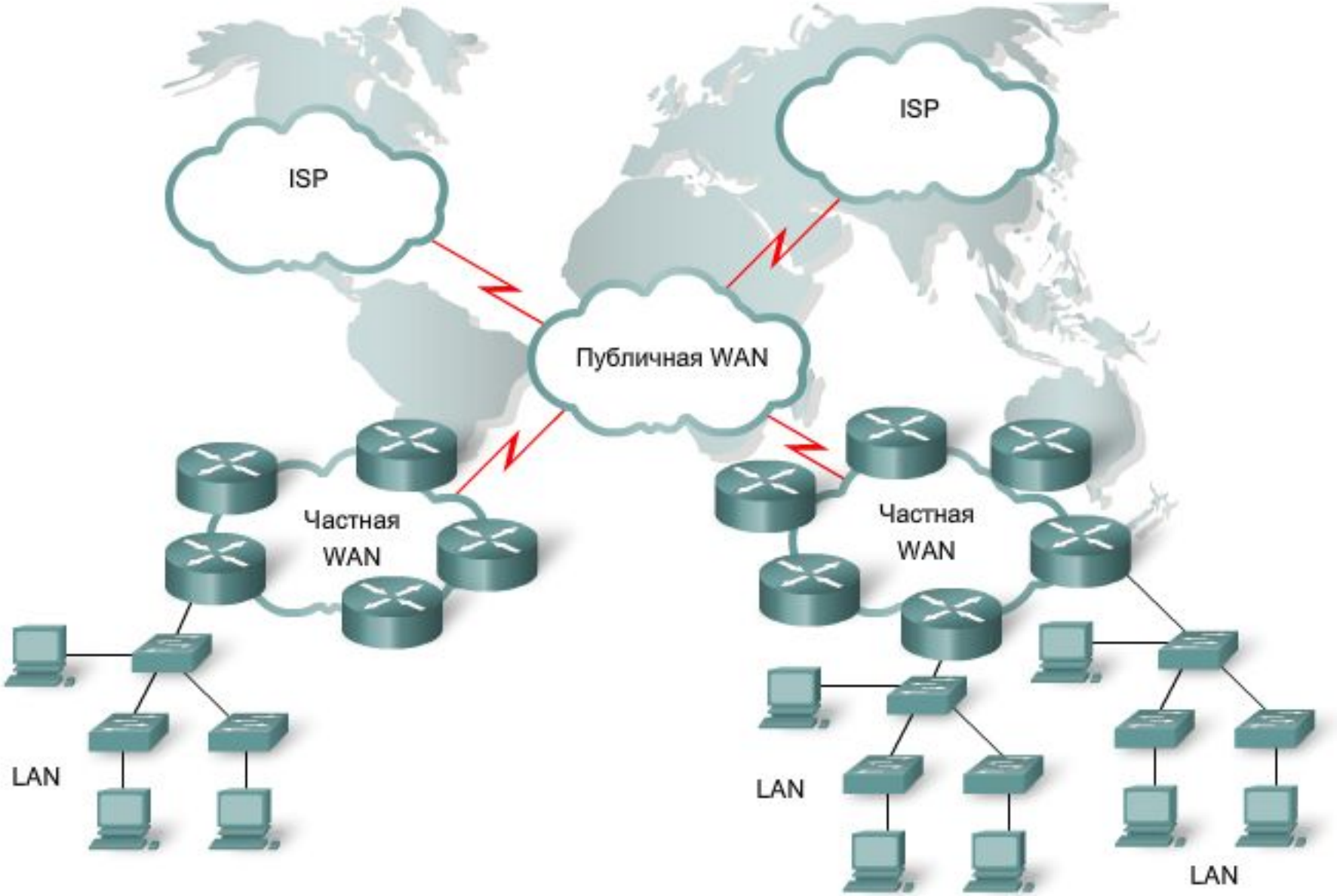
Потоки трафика в корпоративной сети





- **Домен возникновения сбоев** — это область сети, подверженная действию неполадок ключевого устройства или услуги.

Корпоративные LAN и WAN

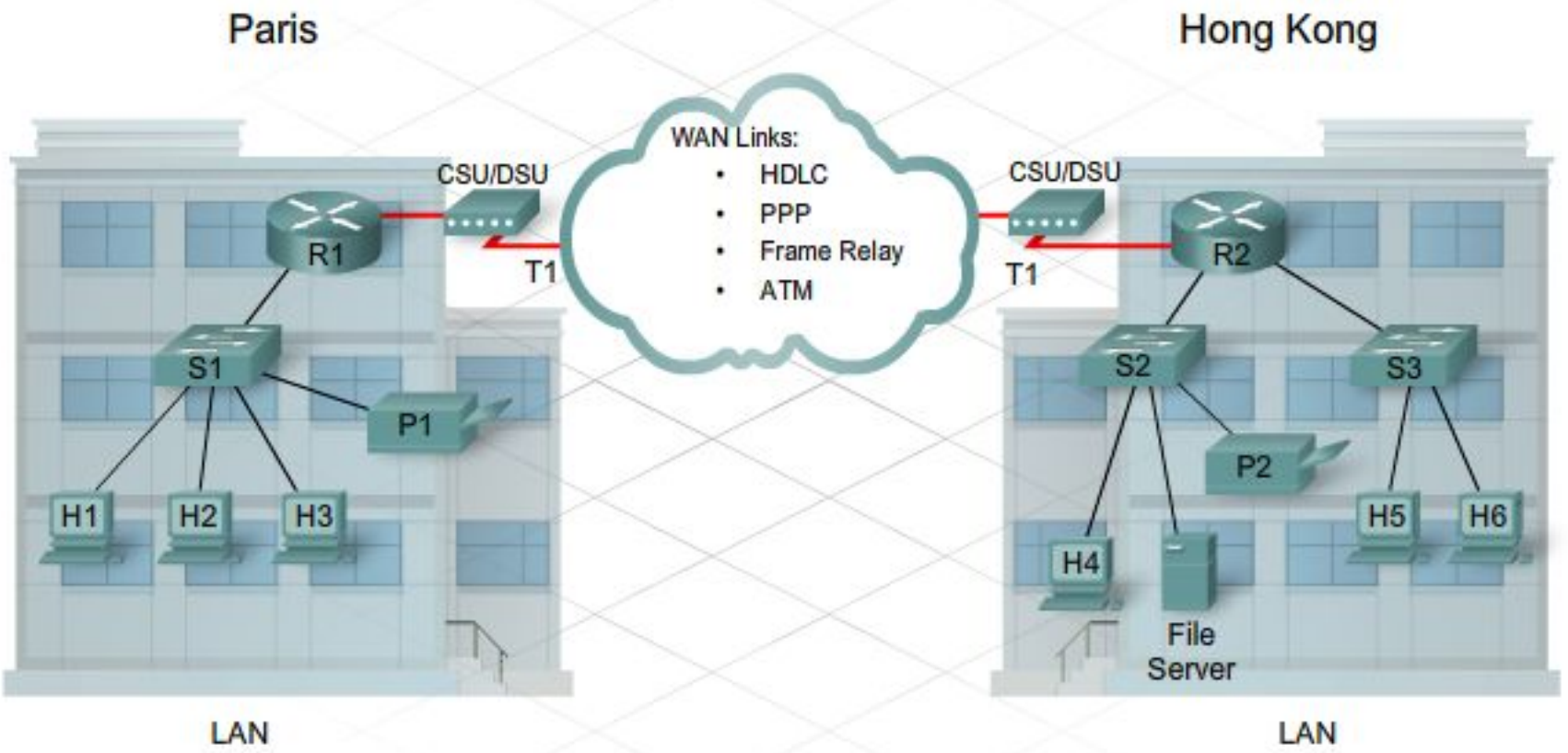


Корпоративные LAN и WAN

- Функции LAN:
  - организация несет ответственность за установку инфраструктуры и управление ею;
  - Ethernet — самая распространенная из используемых технологий;
  - она предназначена для уровней доступа и распределения;
  - LAN соединяет пользователей и предоставляет поддержку локализованных приложений и серверных ферм;
  - соединенные устройства, как правило, находятся в той же локальной области, например в здании или комплексе зданий.

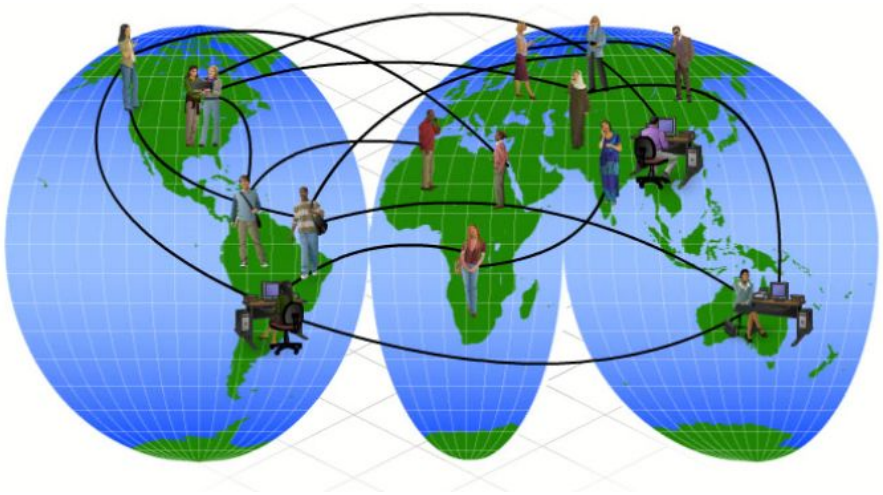
- Функции WAN:
  - соединение площадок, которые, как правило, находятся на значительном расстоянии друг от друга;
  - подключение к WAN требует устройства, преобразующего данные в форму, приемлемую для сети поставщика услуг, например модема или устройства CSU/DSU;
  - услуги предоставляются поставщиком услуг Интернета. Типы услуг WAN: T1/T3, E1/E3, DSL, кабельное соединение, Frame Relay и ATM;
  - ответственность за установку инфраструктуры и управление ею несет поставщик услуг Интернета;
  - пограничные устройства преобразуют инкапсуляцию Ethernet в последовательную инкапсуляцию WAN.

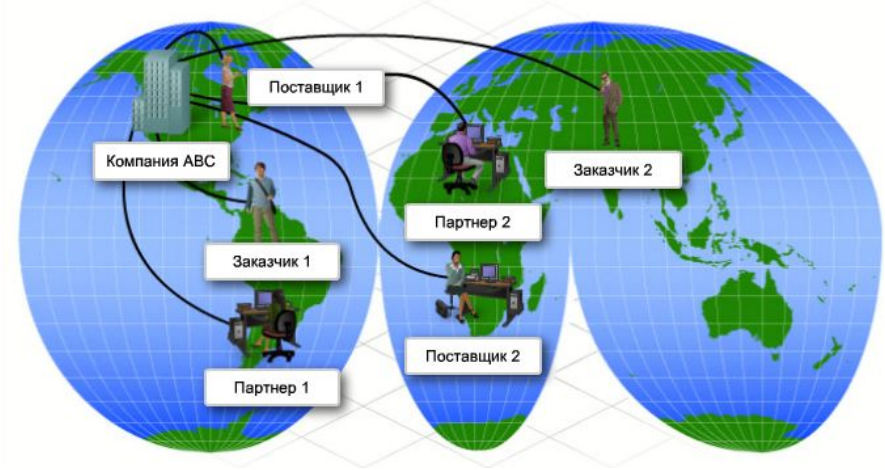
Корпоративные LAN и WAN



Интрасети и сети экстранет

- Многие компании используют частные сети или **интрасети** для предоставления доступа локальным и удаленным работникам с использованием технологий LAN и WAN.
- Интрасеть, поддерживающая подключение поставщиков и подрядчиков, называется сетью **экстранет**.
- Экстранет является частной сетью, использующей Интернет-протоколы и телекоммуникационные системы общего пользования для совместного использования внутренних ресурсов

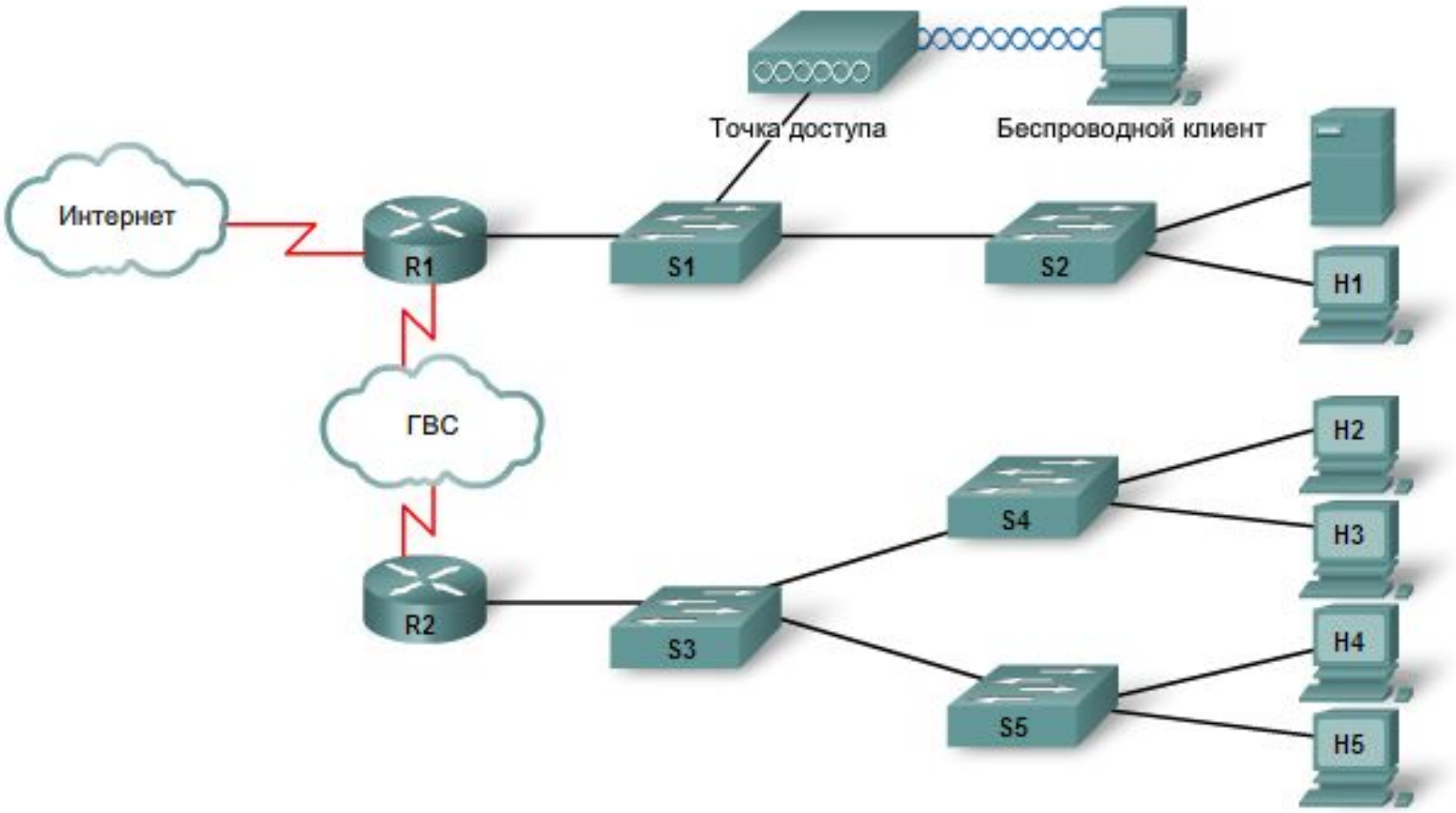




Режимы потоков трафика

- Сетевой трафик, который должен оставаться **локальным** для пользователей сети, включает:
  - общий доступ к файлам;
  - печать;
  - внутреннее резервное копирование и зеркалирование;
  - голосовые службы комплекса зданий.
- Типы трафика, которые чаще всего наблюдаются в **локальной** сети, но могут передаваться через **WAN**:
  - обновления системы;
  - корпоративная почта;
  - обработка транзакций.
- Помимо трафика WAN к **внешнему** трафику относятся данные, передаваемые в Интернет или полученные из него. Потоки трафика VPN и Интернета считаются **внешними**.

Режимы потоков трафика



Приложения и трафик в корпоративной сети

- Корпоративные сети должны поддерживать корпорации, обеспечивая передачу трафика из различных приложений:
  - обработка транзакций БД;
  - доступ к мэйнфреймам и ЦОД (центр обработки данных, он же центр управления сетью);
  - печать и совместный доступ к файлам;
  - аутентификация;
  - веб-сервисы;
  - электронная почта и другие коммуникации;
  - службы VPN;
  - голосовые вызовы и голосовая почта;
  - видео и видеоконференции;
  - процессы контроля и управления сетью, необходимые для ее эксплуатации.
- Для определения режимов потока трафика важно:
  - перехватить трафик в период пиковой загрузки, чтобы получить хорошее представление о различных типах трафика;
  - выполнить перехват в различных сегментах сети, так как некоторые типы трафика будут ограничены определенными сегментами.

Приоритизация сетевого трафика

- Трафик данных
  - для передачи трафика данных, как правило, используется протокол TCP. TCP использует квитирование, чтобы определить необходимость в повторной передаче потерянных пакетов и таким образом гарантирует доставку
- Голосовой и видеотрафик
  - Голосовые и видеоприложения требуют непрерывного потока данных для обеспечения высокого качества изображения и звука (UDP)
- **Задержка** (**запаздывание**) – вызывается сетевыми устройствами, которые обрабатывают трафик на пути от источника к месту назначения. Устройства 3-го уровня модели OSI вызывают более длительные задержки, чем устройства 2-го уровня, из-за большего числа заголовков, которые необходимо обработать.
- **Джиттер** — это колебания времени доставки пакетов по месту назначения
- **Качество обслуживания (QoS)** — это процесс, используемый для гарантированной доставки выбранного потока трафика. Механизмы службы QoS сортируют трафик в очереди на основе его приоритета

Виртуальные частные сети

- VPN (виртуальные частные сети) – обеспечивают шифрование всего трафика между удаленной площадкой и корпоративной сетью
- VPN часто описываются как туннели
- Все данные, передаваемые между источником и местом назначения, шифруются и инкапсулируются с использованием безопасного протокола
- VPN — это приложение типа "клиент-сервер"

Документация по корпоративной сети

- **Схемы сетевой инфраструктуры**, или **топологические схемы**, отслеживают положение, функцию и состояние устройств. Топологические схемы представляют физические или логические сети.
  - **Схема физической топологии** содержит значки, которые описывают положение узлов, сетевых устройств и носителей.
  - **Схема логической топологии** группирует узлы в соответствии с их использованием в сети, независимо от физического расположения. На такой схеме указываются имена и адреса узлов, а также сведения о группах и приложениях.

- Схемы корпоративной сети также могут включать **данные плана управления**. Данные контрольной плоскости описывают **домены возникновения сбоев** и определяют интерфейсы, в которых пересекаются различные сетевые технологии.

Документация по корпоративной сети

- Планирование непрерывности бизнеса.
  - План обеспечения непрерывности бизнеса (BCP) определяет действия, которые необходимо предпринять для продолжения работы организации в случае природной или антропогенной катастрофы.
- План обеспечения безопасности бизнеса.
  - План безопасности бизнеса (BSP) включает физические, системные и организационные меры контроля. Общий план безопасности должен включать раздел, посвященный ИТ, в котором описываются методы защиты сетевых и информационных активов организации.
- План технического обслуживания сети.
  - План обслуживания сети (NMP) гарантирует непрерывность бизнеса за счет поддержания эффективной и бесперебойной работы сети. Работы по обслуживанию сети должны выполняться по плану в течение определенных периодов, обычно по ночам и в выходные, чтобы свести к минимуму их влияние на работу организации.
- Соглашения об уровне обслуживания.
  - Соглашение об уровне обслуживания (SLA) — это соглашение между заказчиком и поставщиком услуг Интернета, описывающее такие параметры, как доступность сети и время отклика служб.

Центр управления сетью

- Большинство корпоративных сетей включают **центр управления сетью** (NOC), который обеспечивает центральное управление и мониторинг для всех сетевых ресурсов
- Как правило, центр управления сетью включает следующее:
  - фальшпол для прокладки проводов и силовых кабелей под устройствами;
  - высокопроизводительные системы бесперебойного питания и кондиционирования, обеспечивающие безопасное окружение для эксплуатации оборудования;
  - системы пожаротушения, встроенные в потолок;
  - станции мониторинга сети, серверы, системы резервного копирования и хранилища;
  - коммутаторы уровня доступа и маршрутизаторы уровня распределения, если они образуют главный узел распределения (MDF) здания или комплекса зданий, в котором располагаются.

Центр управления сетью

Серверная ферма

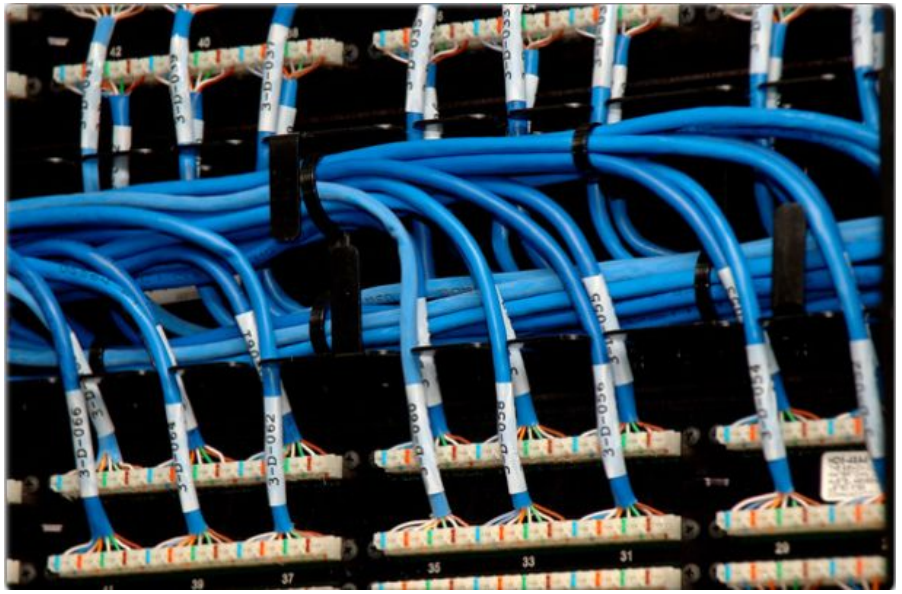
Сетевое хранилище (NAS)

- **Серверы** в центрах управления сетью, как правило, кластеризуются и образуют серверную ферму. Серверная ферма часто считается единым ресурсом, но на самом деле она выполняет две функции: резервирование и распределение нагрузки.

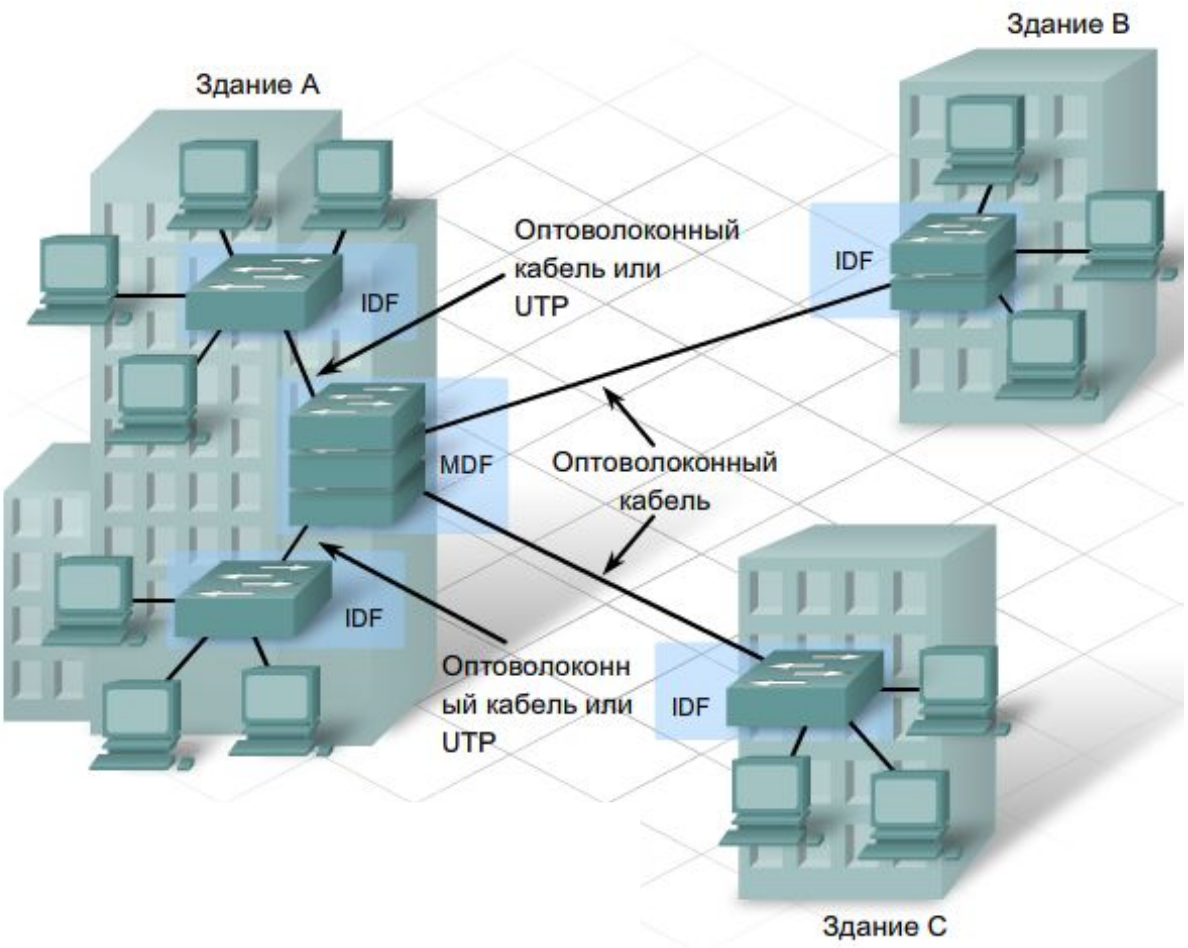
- Другой важный аспект центра управления сетью — высокоскоростное **хранилище данных** большой емкости. Хранилище данных, или хранилище с подключением по сети (NAS), объединяет большое количество дисков, которые подключаются непосредственно к сети и могут использоваться любым сервером. Устройство NAS, как правило, подключается к сети Ethernet и имеет собственный IP-адрес.

Центр управления сетью

- В корпоративных центрах управления сетью тысячи кабелей могут входить в объект и выходить из него.
- Для упрощения поиска и устранения неполадок:
  - оба конца кабеля должны отмечаться с использованием стандартных условных обозначений, указывающих на приемник и передатчик;
  - все кабельные пролеты должны быть задокументированы на схеме физической топологии сети;
  - все кабельные пролеты, как медные, так и оптоволоконные, должны пройти сквозные испытания путем отправки сигнала через кабель с последующим измерением потерь.



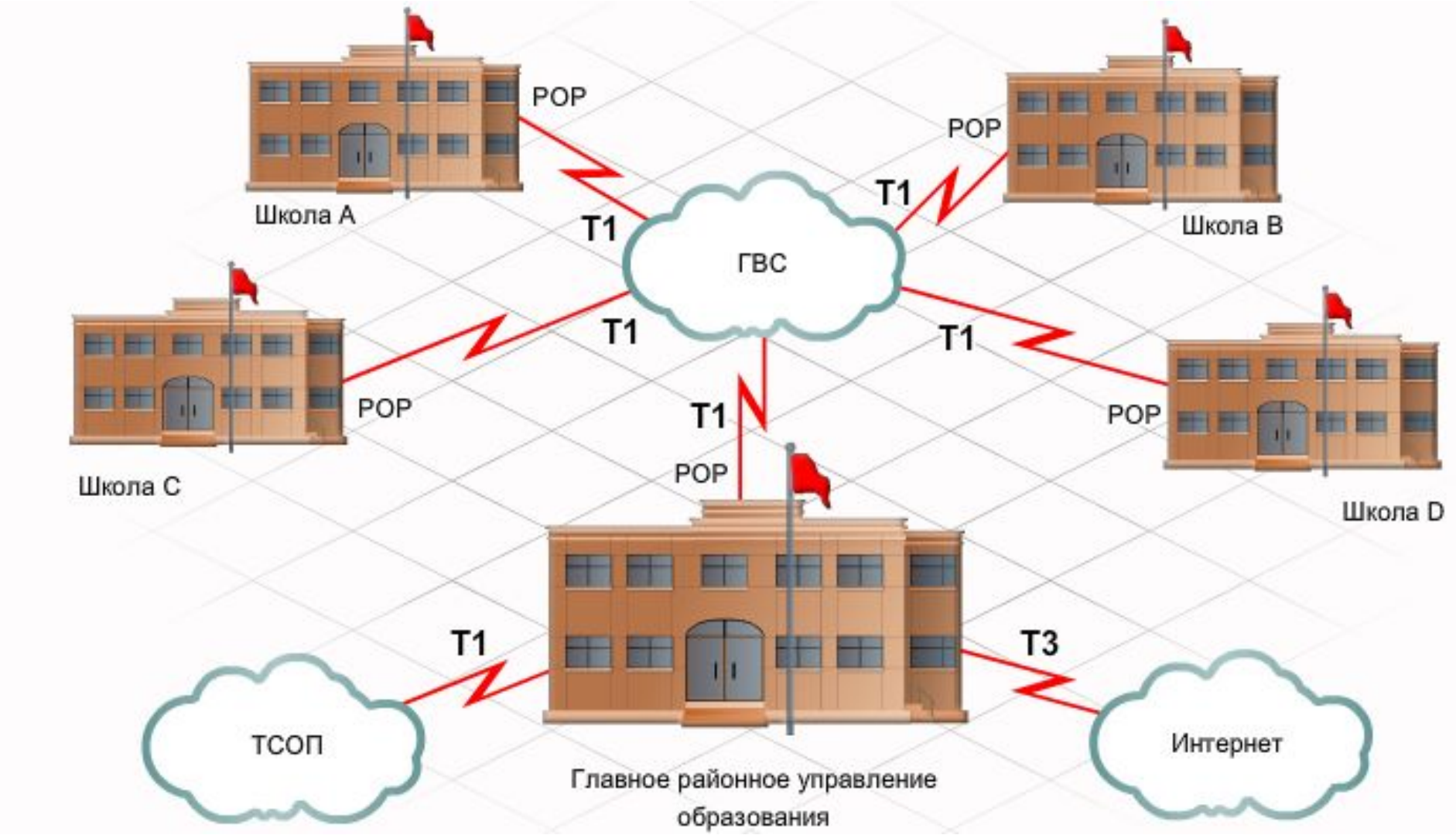
Проектирование и принципы телекоммуникационной комнаты



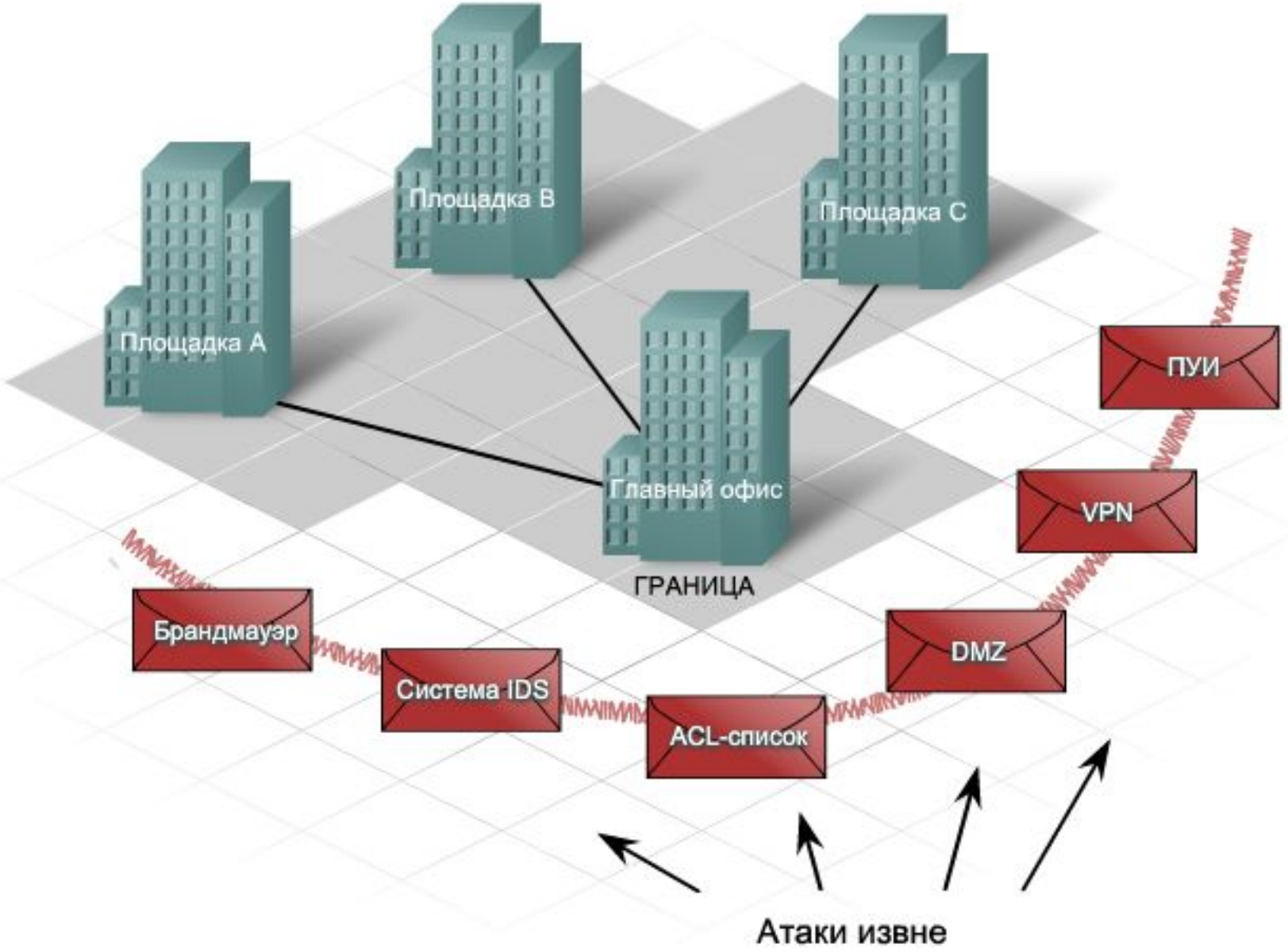
Телекоммуникационную комнату называют коммуникационным отсеком и промежуточным распределительным узлом (IDF)

Группа промежуточных узлов распределения подключается к главному распределительному отсеку (MDF) с использованием топологии расширенная звезда. MDF обычно располагается в центре управления сетью или в центральном помещении здания.

Предоставление услуг у точки присутствия



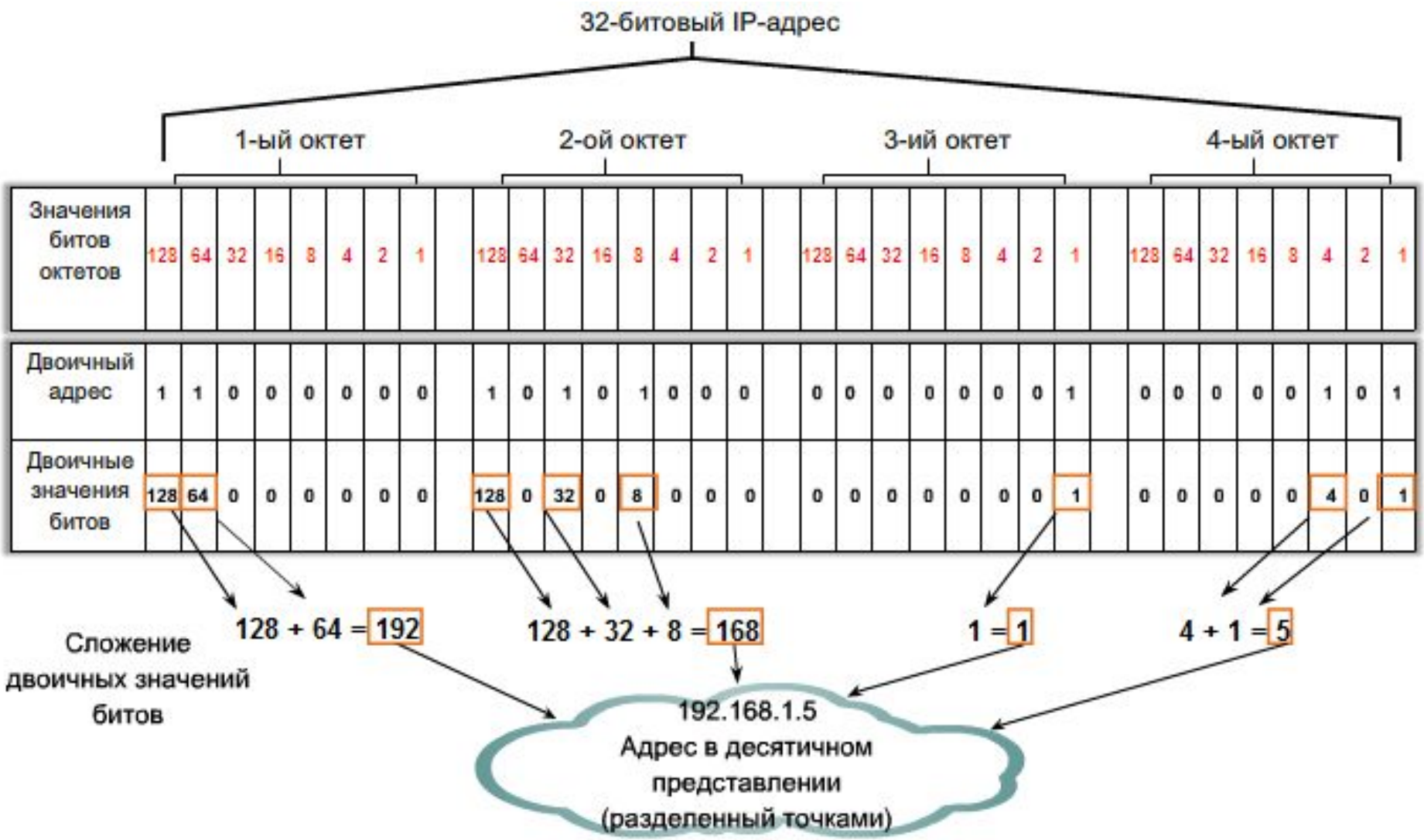
Безопасность на границе корпорации



IP-адресация

- IP-адрес присваивается сетевому интерфейсу узла. Обычно это сетевая интерфейсная плата (NIC), установленная в устройстве.
- IP-адрес представляет собой простую серию из 32 двоичных бит (единиц и нулей). Поэтому 32 бита группируются по четыре 8-битных байта – в октеты. Каждый октет IP-адреса представлен в виде своего десятичного значения. Октеты разделяются десятичной точкой: **195.209.66.3**
- Структура 32-битного IP-адреса определяется Интернет-протоколом версии 4 (IPv4). По 32-битной схеме адресации можно создать более 4 миллиардов IP-адресов.

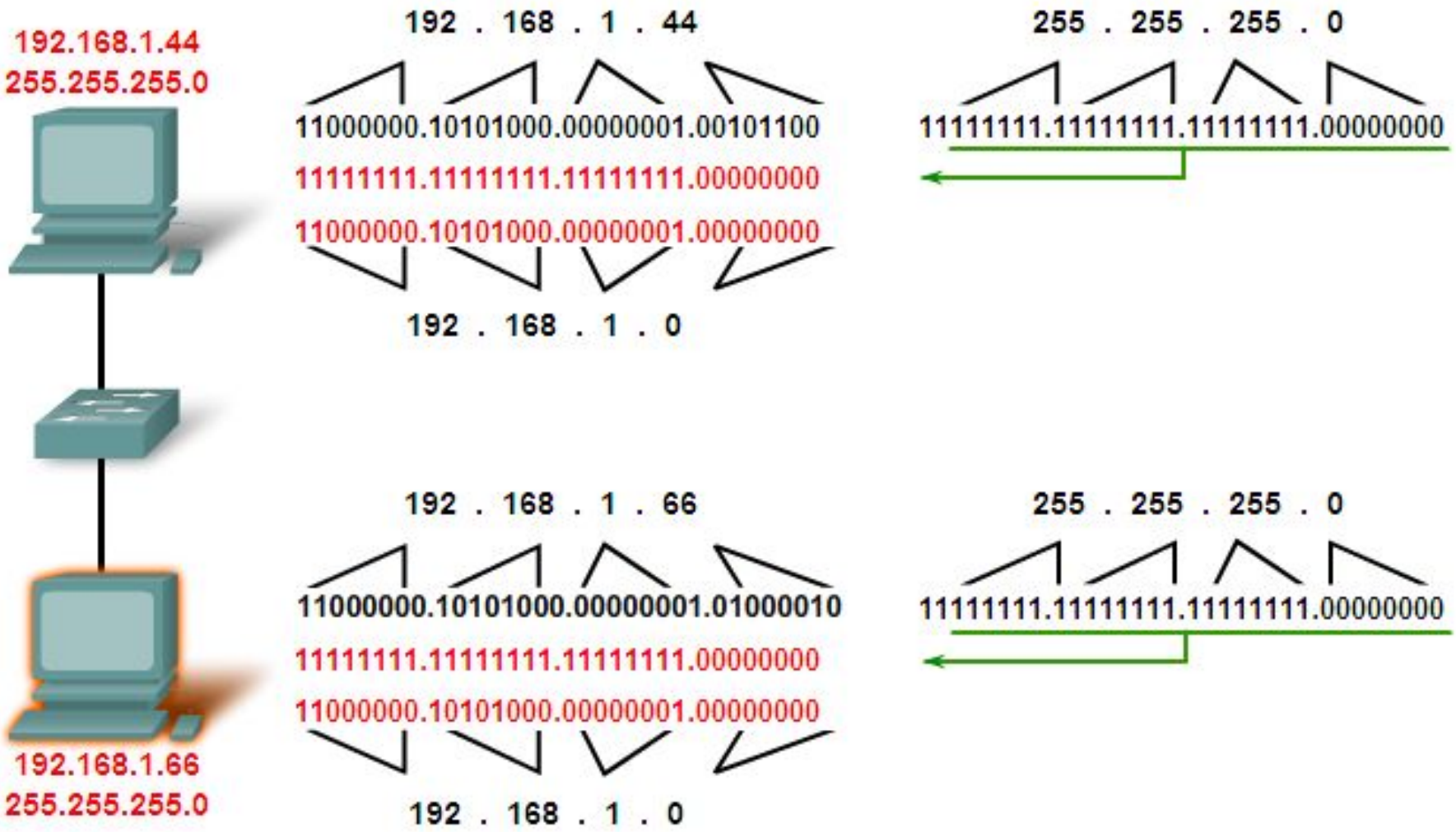
IP-адрес


32-битовый IP-адрес
1-ый октет
2-ой октет
3-ий октет
4-ый октет
Значения битов октетов
128 64 32 16 8 4 2 1 | 128 64 32 16 8 4 2 1 | 128 64 32 16 8 4 2 1 | 128 64 32 16 8 4 2 1
Двоичный адрес
1 1 0 0 0 0 0 0 | 1 0 1 0 1 0 0 0 | 0 0 0 0 0 0 0 1 | 0 0 0 0 0 1 0 1
Двоичные значения битов
128 64 0 0 0 0 0 0 | 128 0 32 0 8 0 0 0 | 0 0 0 0 0 0 0 1 | 0 0 0 0 0 4 0 1
Сложение двоичных значений битов
128 + 64 = 192
128 + 32 + 8 = 168
1 = 1
4 + 1 = 5
192.168.1.5
Адрес в десятичном представлении (разделенный точками)

Маска подсети

- Логический 32-битный IP-адрес представляет собой иерархическую систему и состоит из двух частей. Первая идентифицирует сеть, вторая - узел в сети. Обе части являются обязательными.
- Для определения части, идентифицирующей сеть, используется **маска подсети** – 32-битный набор.
- Маска сравнивается с IP-адресом побитно, слева направо. В маске подсети единицы соответствуют сетевой части, а нули - адресу узла.
- Отправляя пакет, узел сравнивает маску подсети со своим IP-адресом и адресом получателя. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если нет, отправляющий узел передает пакет на интерфейс локального маршрутизатора для отправки в другую сеть.

Маска подсети

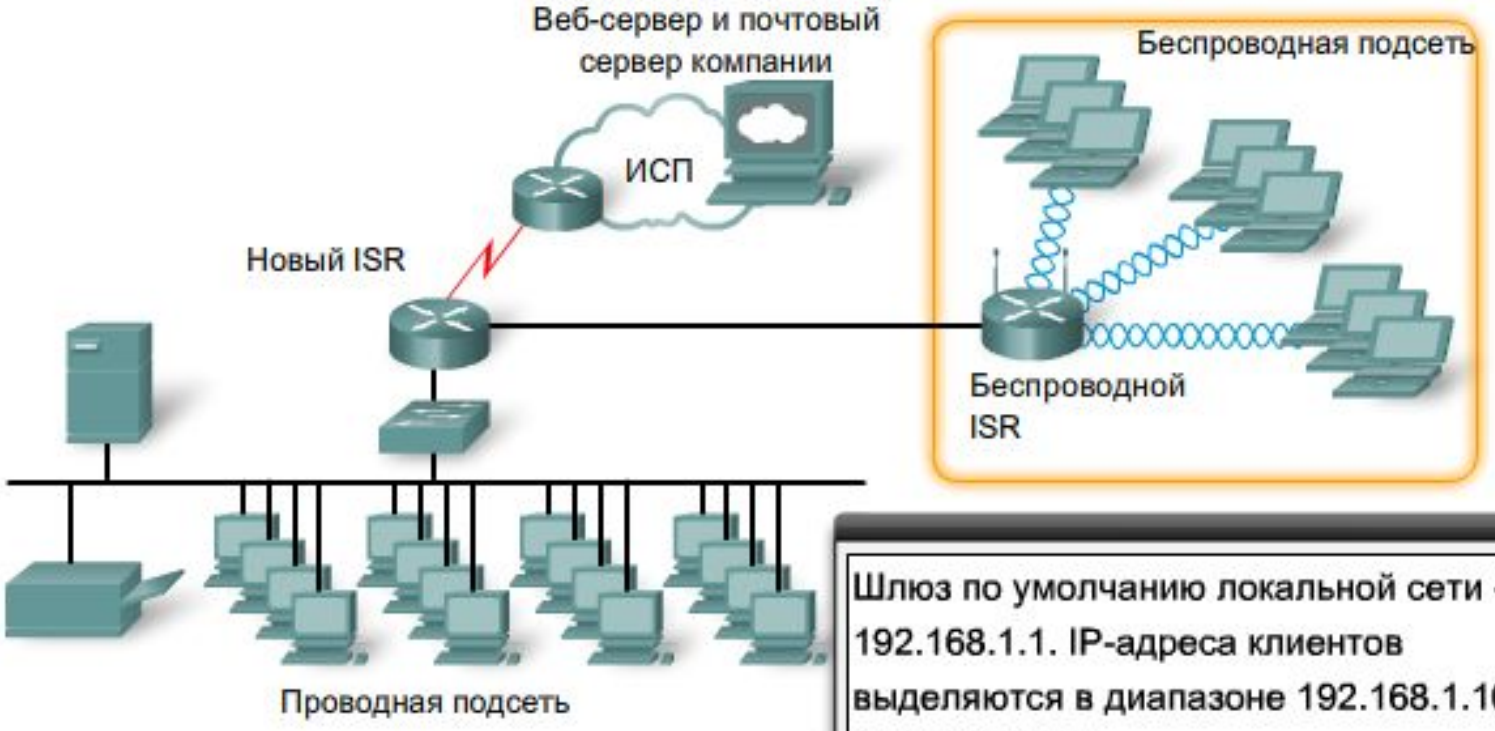


Классы IP-адресов

Классы IP-адресов					
Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в двоичном и десятичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей (2^7-2) 16 777 214 узлов для каждой сети (2^24-2)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей (2^14-2) 65 534 узла для каждой сети (2^16-2)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей (2^21-2) 254 узла для каждой сети (2^8-2)
D	224 - 239	11100000 - 11101111	В качестве узла не для коммерческого использования		
E	240 - 255	11110000 - 11111111	В качестве узла не для коммерческого использования		

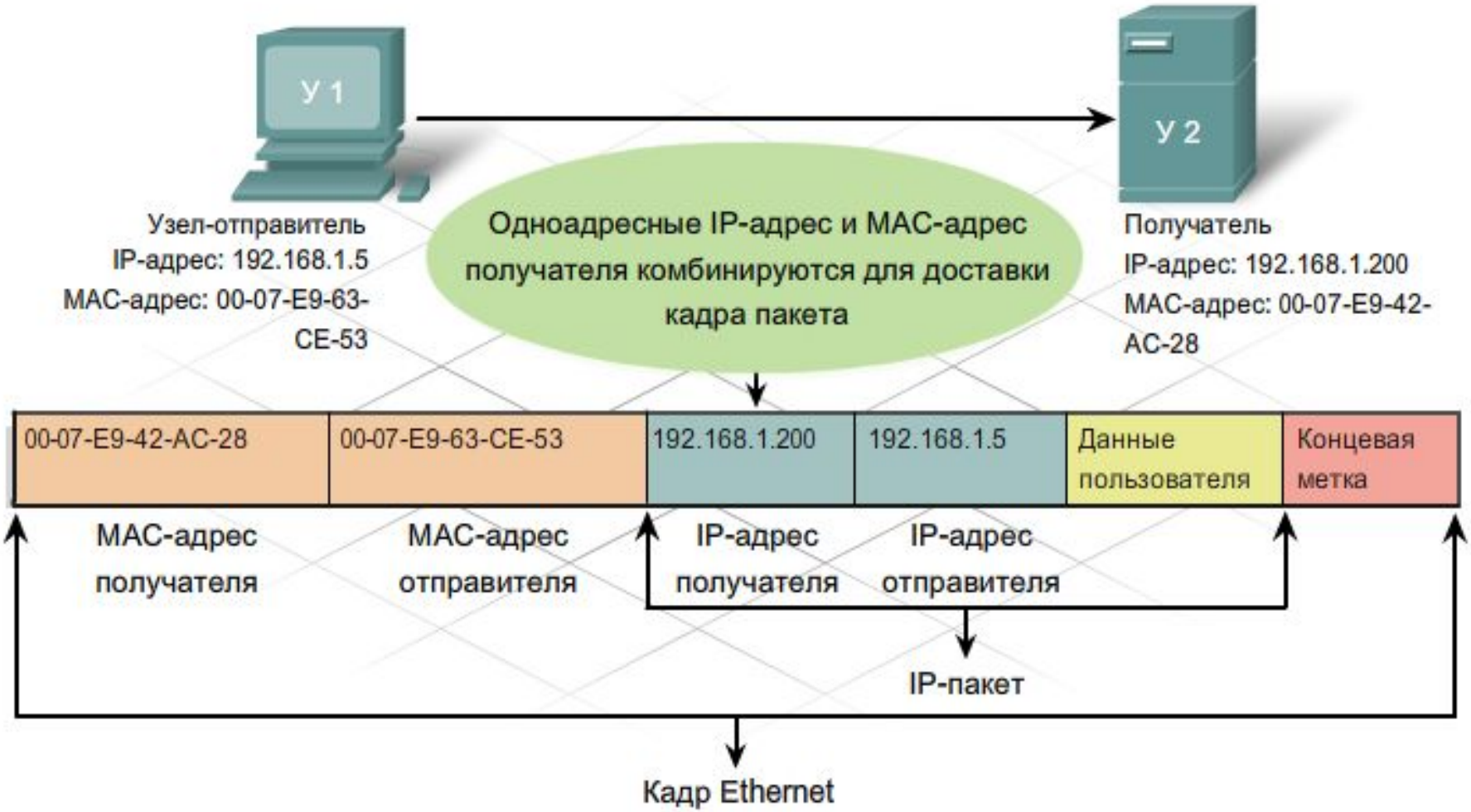
Частные IP-адреса

Класс	Частные IP-адреса(RFC 1918)	Маска подсети по умолчанию	Число сетей	Число узловв каждой сети	Общее число узлов
A	10.0.0.0 - 10.255.255.255	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 - 172.31.255.255	255.255.0.0	16	85,534	1,048,544
C	192.168.0.0 - 192.168.255.255	255.255.255.0	256	254	85,024

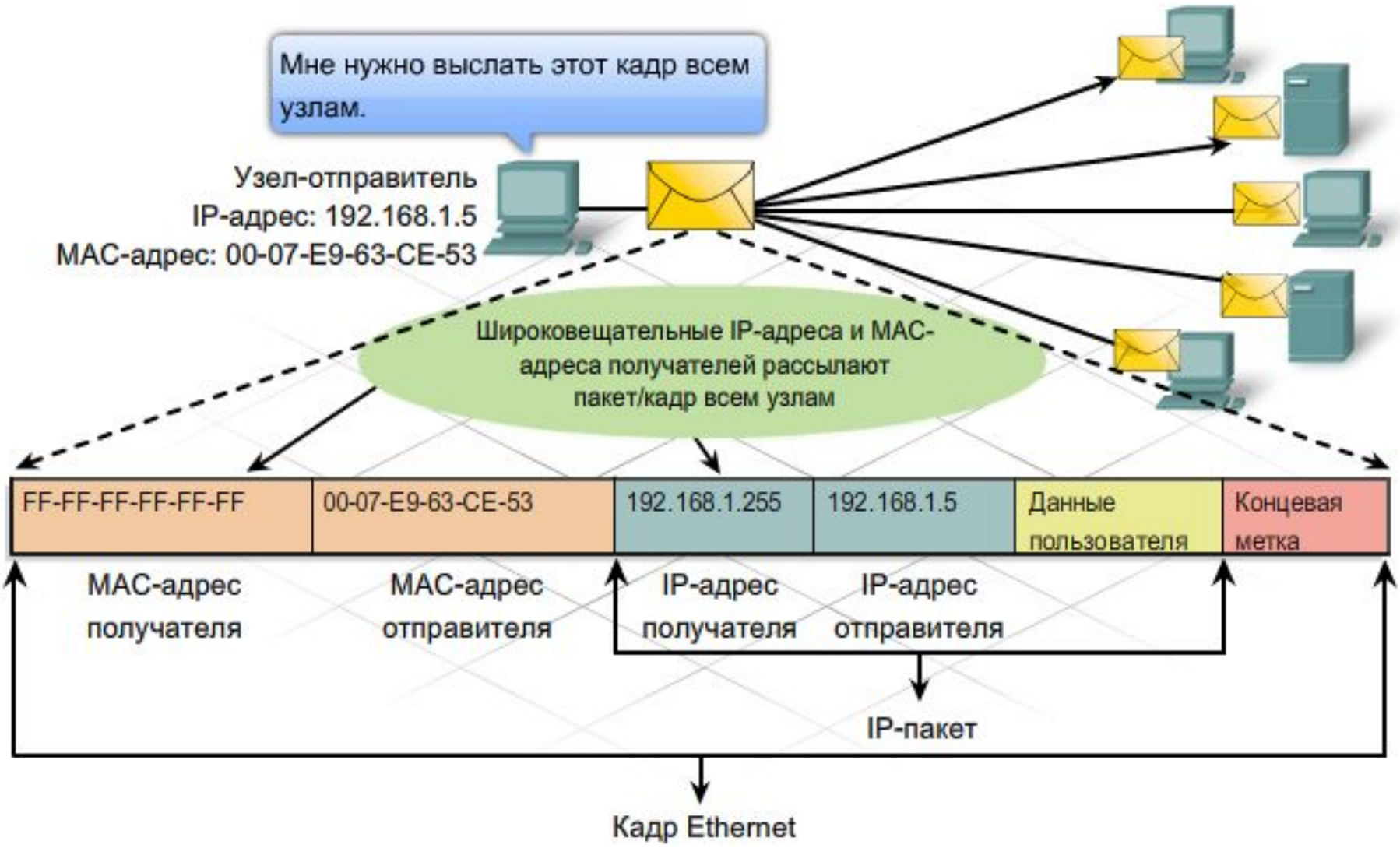


Шлюз по умолчанию локальной сети - 192.168.1.1. IP-адреса клиентов выделяются в диапазоне 192.168.1.101 - 192.168.1.150.

Одноадресная рассылка

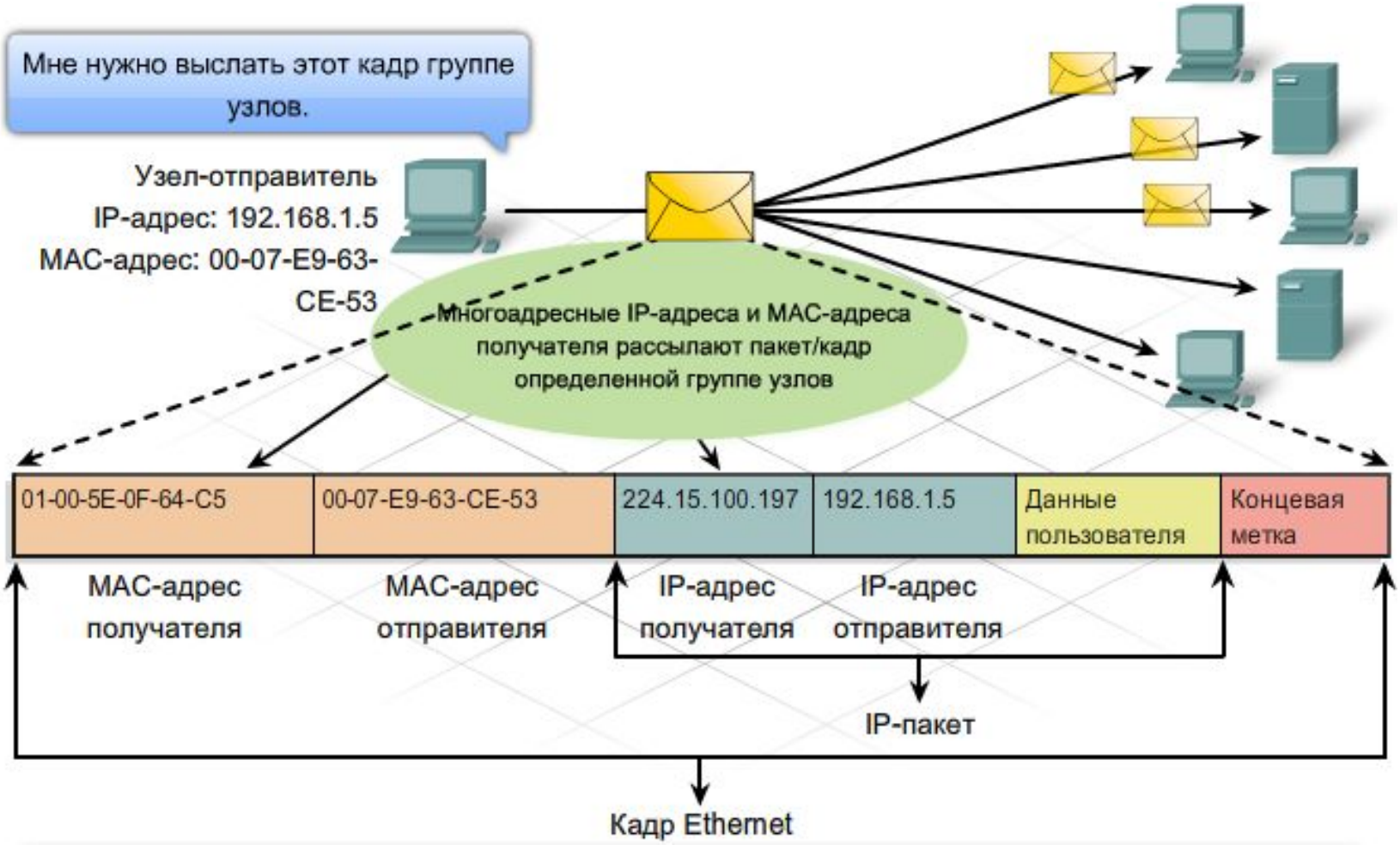


Широковещательная рассылка

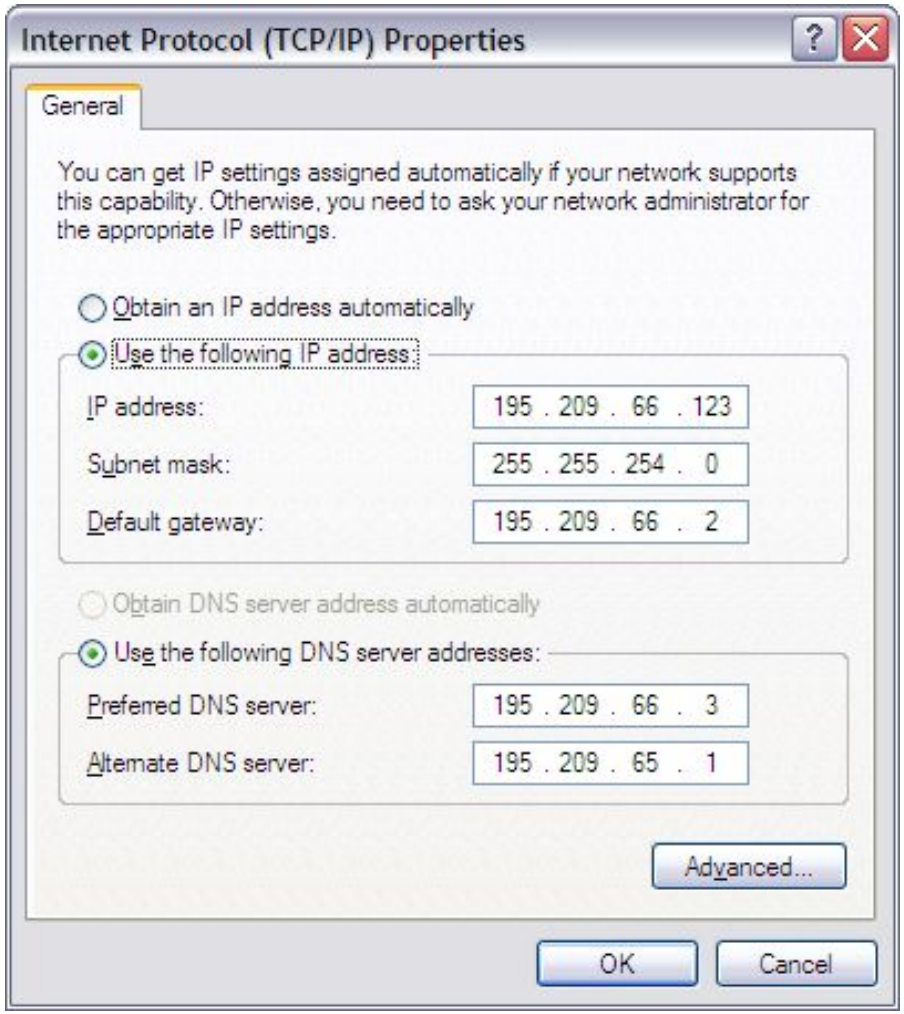


Многоадресная рассылка

- Диапазон адресов многоадресных рассылок - от 224.0.0.0 до 239.255.255.255.
- Многоадресный MAC-адрес - это особое значение, которое в шестнадцатеричном формате начинается с **01-00-5E**. Нижние 23 бита IP-адреса многоадресной группы преобразуются в остальные 6 шестнадцатеричных символов адреса Ethernet.



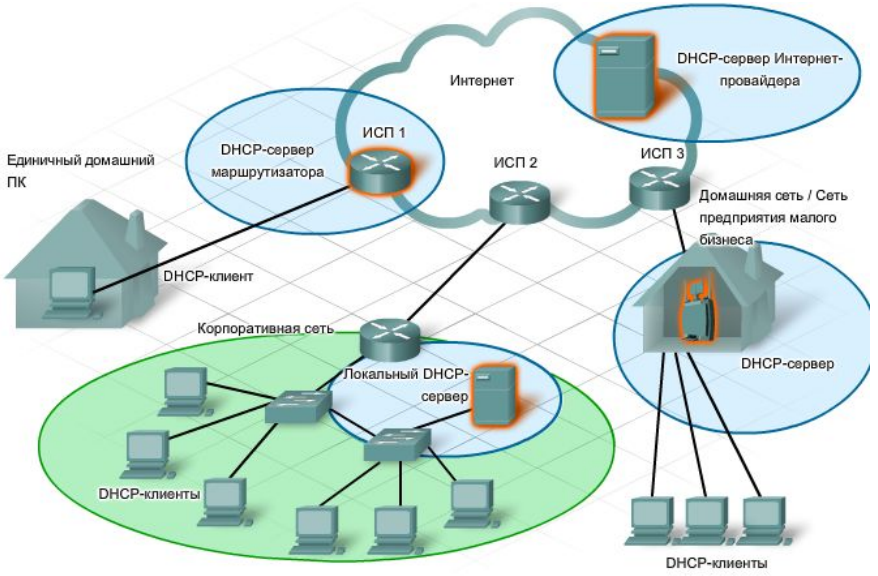
Статические и динамические адреса



- Dynamic Host Configuration Protocol (DHCP) предусматривает механизм автоматического присвоения информации об адресе, например, IP-адреса, маски подсети, шлюза по умолчанию и других настроек.
- Преимущества:
  - Облегчает работу специалистов
  - Снижает вероятность ошибки
  - Временное использование адресов узлами

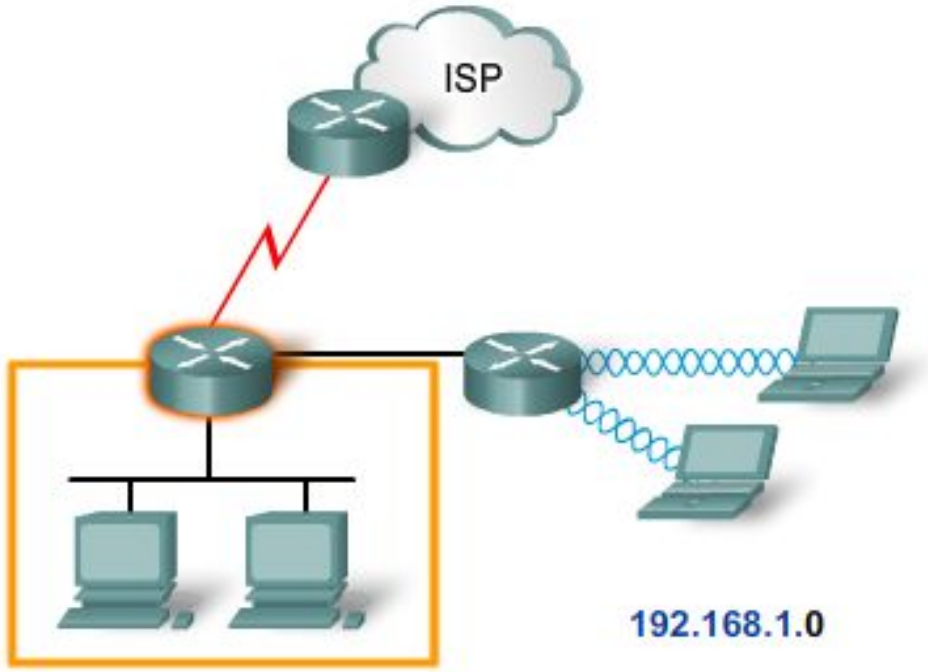
Динамическое получение IP-адреса

- Клиент, которому нужен IP-адрес, посылает сообщение о поиске DHCP в виде широковещательной рассылки с IP-адресом получателя 255.255.255.255 (32 единицы) и MAC-адресом получателя FF-FF-FF-FF-FF-FF (48 единиц). Кадр DHCP получат все узлы в сети, но ответит только сервер DHCP. Он отправляет источнику предложенный IP-адрес клиента. Узел в ответ посылает на указанный сервер запрос DHCP с подтверждением использования IP-адреса. Сервер присылает подтверждение.



Разбиение на подсети

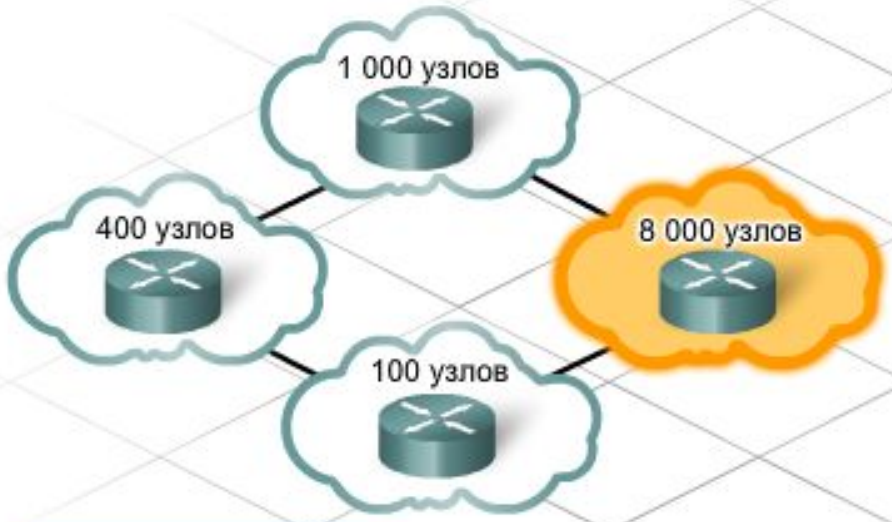
- Существует много причин разделить сеть на подсети, включая:
  - физическое местоположение;
  - логическую группировку;
  - безопасность;
  - требования приложений;
  - ограничение широковещательной рассылки;
  - модель иерархической сети.



Технология бесклассовой междоменной маршрутизации

- Для более эффективного использования IP-адресов была создана технология **бесклассовой междоменной маршрутизации** (CIDR – *C*lassless *I*nter*D*omain *R*outing). В режиме CIDR классы сетей не используются.
- Для создания подсетей в CIDR используются **маски подсетей меняющейся длины** (VLSM – *V*ariable *L*ength *S*ubnets *M*asks). Идентификатор сети не ограничивается рамками октета.
  - В сети с адресацией по классам сеть, представленная IP-адресом 192.168.5.0, относится к классу C. Идентификатор сети должен состоять минимум из 24 бит, узлов не может быть больше 254.
  - При использовании адресации CIDR, которую иногда называют бесклассовой, количество бит в идентификаторе сети не регулируется ее классом. Можно создавать сети с адресным пространством 192.168.0.0 и номером сети, занимающим меньше 24 бит.

Технология бесклассовой междоменной маршрутизации



Разбиение сети на подсети с классовой адресацией

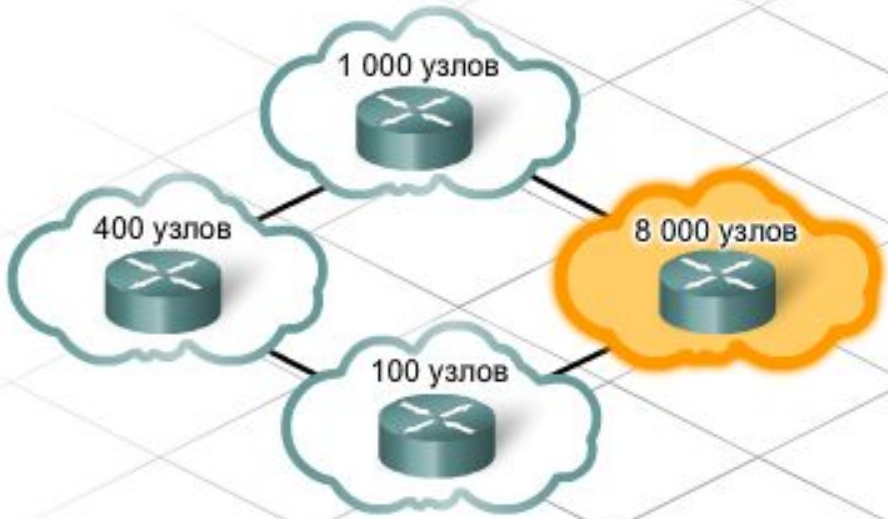
Разбиение на подсети с бесклассовой адресацией

При разбиении на подсети с классовой адресацией все подсети должны иметь одинаковую маску подсети. Если используются два бита, идентифицирующие узел, создаются четыре одинаковые подсети с 8 190 узлами.

Подсеть №1 имеет 8 000 узлов

Сетевой IP-адрес	172.16.0.0
Маска подсети	255.255.224.0
Общее число возможных узлов	8190 8000
Назначенные IP-адреса	190
Свободные IP-адреса	

Технология бесклассовой междоменной маршрутизации



Разбиение сети на подсети с классовой адресацией

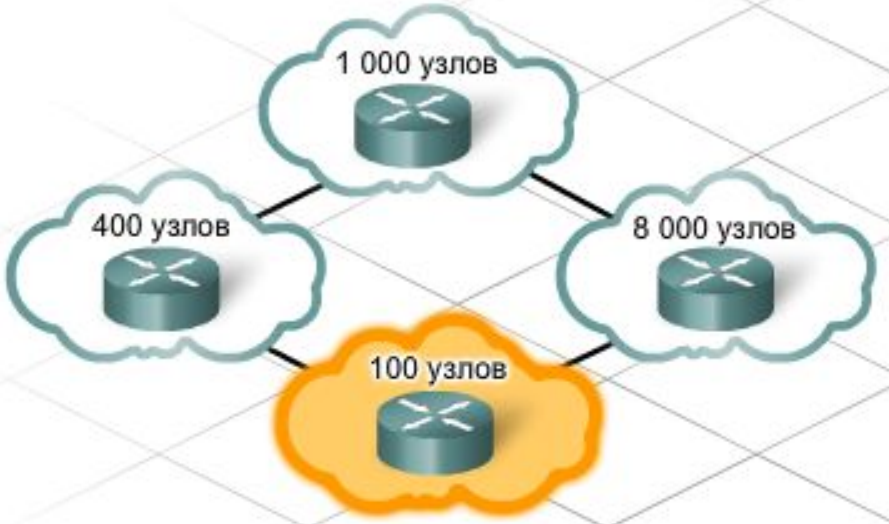
Разбиение на подсети с бесклассовой адресацией

Бесклассовая IP-адресация позволяет создавать подсети неодинакового размера. Подсети можно создавать, исходя из числа необходимых адресов узлов. Следует проявлять осторожность и не допускать пересечения диапазонов сетевых адресов.

Подсеть №1 имеет 8 000 узлов
Используя три бита, идентифицирующих узел, можно создать единственную подсеть с 8 190 узлами.

Сетевой IP-адрес	172.16.0.0
Маска подсети	255.255.224.0
Бесклассовое представление	172.16.0.0/19
Общее число возможных узлов	8 190
	8 000
Назначенные IP-адреса	190
Свободные IP-адреса	

Технология бесклассовой междоменной маршрутизации



Разбиение сети на подсети с классовой адресацией

Разбиение на подсети с бесклассовой адресацией

Бесклассовая IP-адресация позволяет создавать подсети неодинакового размера. Подсети можно создавать, исходя из числа необходимых адресов узлов. Следует проявлять осторожность и не допускать пересечения диапазонов сетевых адресов.

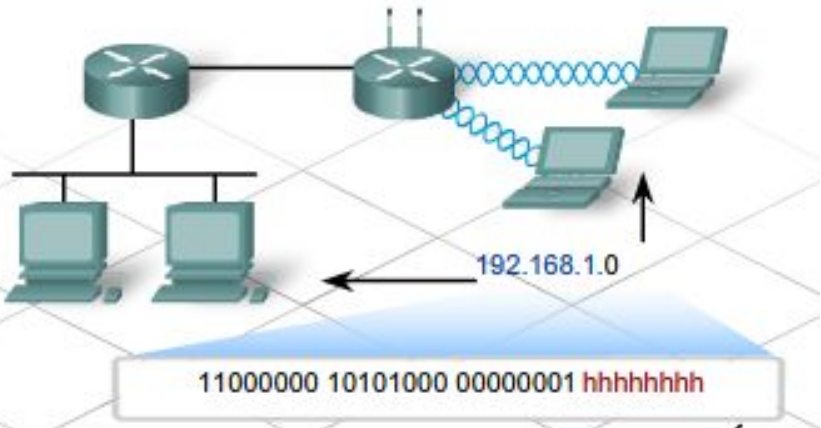
Подсеть №4 имеет 100 узлов
Используя девять битов, идентифицирующих узел, можно создать единственную подсеть со 126 адресами узлов.

Сетевой IP-адрес	172.16.38.0
Маска подсети	255.255.255.128
Бесклассовое представление	172.16.38.0/25
Общее число возможных	126
узлов	100
Назначенные IP-адреса	26
Свободные IP-адреса	

Технология бесклассовой междоменной маршрутизации

При планировании подсетей нужно учесть две вещи: количество узлов в каждой сети и количество локальных сетей.

Из таблицы возможных подсетей в сети 192.168.1.0 видно, как выбор количества бит в идентификаторе подсети влияет на количество возможных подсетей и количество узлов в каждой из них.



Идентификатор подсети (биты)	Идентификатор узла (биты)	Число подсетей	Число узлов	Значения битов
0	8	1	254	hhhhhhhh
1	7	2	126	shhhhhhh
2	6	4	62	sshhhhhh
3	5	8	30	sshhhhh
4	4	16	14	ssshhhh
5	3	32	6	sssshhh
6	2	64	2	ssssshh

Разбиение на подсети

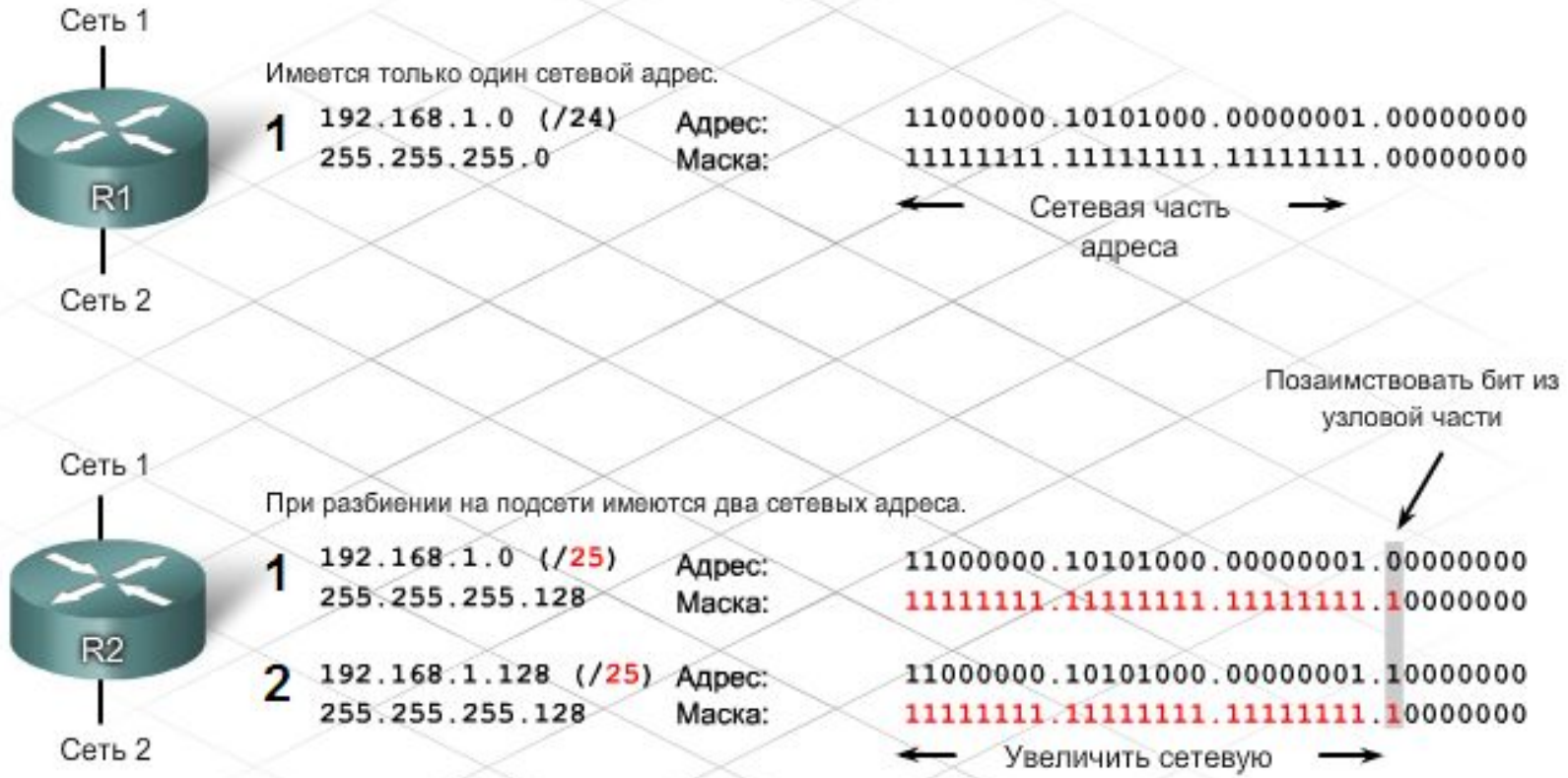
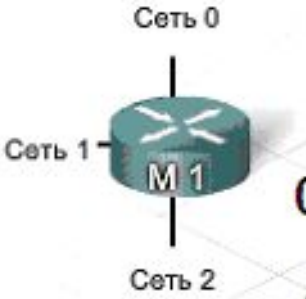


Схема адресации: Пример 2-х сетей

Подсеть	Сетевой адрес	Диапазон адресов узлов	Широковещательный адрес
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255



	192.168.1.0 (/24)	Адрес:	11000000.10101000.00000001.00000000
	255.255.255.0	Маска:	11111111.11111111.11111111.00000000
0	192.168.1.0 (/26)	Адрес:	11000000.10101000.00000001.00000000
	255.255.255.192	Маска:	11111111.11111111.11111111.11000000
1	192.168.1.64 (/26)	Адрес:	11000000.10101000.00000001.01000000
	255.255.255.192	Маска:	11111111.11111111.11111111.11000000
2	192.168.1.128 (/26)		11000000.10101000.00000001.10000000
	255.255.255.192		11111111.11111111.11111111.11000000
3	192.168.1.192 (/26)		11000000.10101000.00000001.11000000
	255.255.255.192		11111111.11111111.11111111.11000000

Позаимствованы 2 бита для обеспечения 4-х подсетей

Свободный адрес в данном примере.

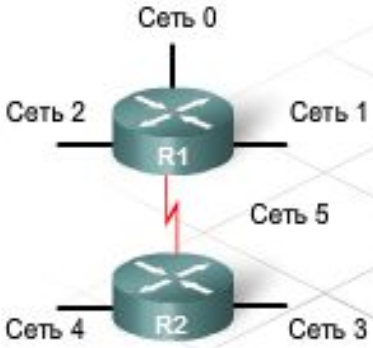
Цифра "1" в данных позициях в маске означает, что эти значения являются частью сетевого адреса.

Схема адресации: Пример 4-х сетей

Подсеть	Сетевой адрес	Диапазон узлов	Широковещательный адрес
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Возможно больше подсетей, но меньше адресов для каждой подсети.

Разбиение на подсети



	192.168.1.0 (/24)	Address:	11000000.10101000.00000001.00000000
	255.255.255.0	Mask:	11111111.11111111.11111111.00000000
0	192.168.1.0 (/27)	Address:	11000000.10101000.00000001.00000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
1	192.168.1.32 (/27)	Address:	11000000.10101000.00000001.00100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
2	192.168.1.64 (/27)	Address:	11000000.10101000.00000001.01000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
3	192.168.1.96 (/27)	Address:	11000000.10101000.00000001.01100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
4	192.168.1.128 (/27)	Address:	11000000.10101000.00000001.10000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
5	192.168.1.160 (/27)	Address:	11000000.10101000.00000001.10100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
6	192.168.1.192 (/27)	Address:	11000000.10101000.00000001.11000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
7	192.168.1.224 (/27)	Address:	11000000.10101000.00000001.11100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000

Позаимствованы 3 бита для обеспечения 8 подсетей

Разбиение на подсети | Схема адресации

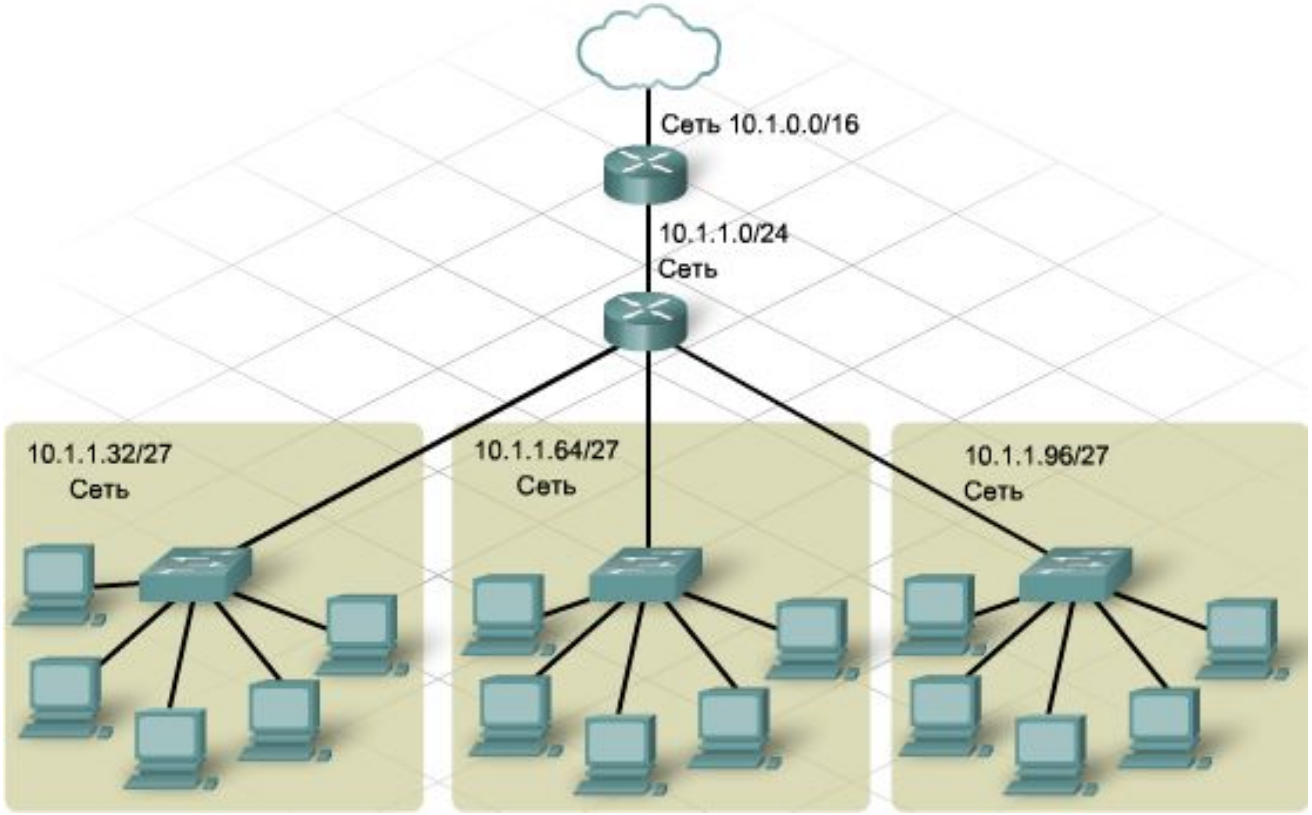
Схема адресации

Схема адресации: Пример 6-и сетей

Подсеть	Сетевой адрес	Диапазон узлов	Широковещательный адрес
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

- Если сеть класса С разделена на подсети, и из идентификатора узла взято для идентификатора подсети **три** бита, для адресов узлов остается **пять**. При этом в подсети может быть **30** узлов, или **2^5 - 2**.
- Количество подсетей определяется так же. Если адрес подсети состоит из **трех** бит, получится **2^3** подсетей.
- Определяя, сколько в каждой подсети необходимо узлов, следует учесть интерфейс маршрутизатора или шлюза и отдельные устройства. У каждого интерфейса маршрутизатора должен быть IP-адрес в подсети, к которой подключена сеть узла.

Эффективная иерархическая адресация



- **Эффективная** схема иерархической адресации состоит из адреса классовой сети на центральном уровне, который подразделяется на менее крупные подсети на уровнях распределения и доступа.
- Можно использовать иерархическую сеть без использования иерархической адресации. Хотя сеть продолжает функционировать, эффективность конструкции сети снижается, а определенные функции протокола маршрутизации (например, суммирование маршрутов) работают некорректно.

Информативность схемы иерархической адресации

- IP-адрес **192.168.1.75 /26** содержит следующие сведения:
  - *Десятичная маска подсети* – обозначение /26 означает маску подсети

    255.255.255.192.
  - *Число создаваемых подсетей* – предположим, что мы начали с маски подсети по умолчанию /24, то тогда 2 дополнительных бита узла заимствованы для сети. Это позволяет создать 4 подсети (2^2 = 4).
  - *Число узлов*, пригодных для использования в каждой подсети – шесть битов оставлены для узла, что дает 62 узла в каждой подсети (2^6 = 64 - 2 = 62).
  - *Сетевой адрес* – используя маску подсети для определения размещения сетевых битов, можно получить значение сетевого адреса. В этом примере это значение равно 192.168.1.64.
  - *Первый применимый адрес узла* – среди битов узла не могут содержаться все нули, поскольку они соответствуют сетевому адресу подсети. Следовательно, первым применимым адресом узла в подсети .64 будет .65.
  - *Широковещательный адрес* – среди битов узла не могут содержаться все единицы, поскольку они соответствуют широковещательному адресу подсети. В этом случае в качестве адреса широковещательной рассылки используется .127. Сетевой адрес следующей подсети начинается с .128.

Маски подсети переменной длины - VLSM

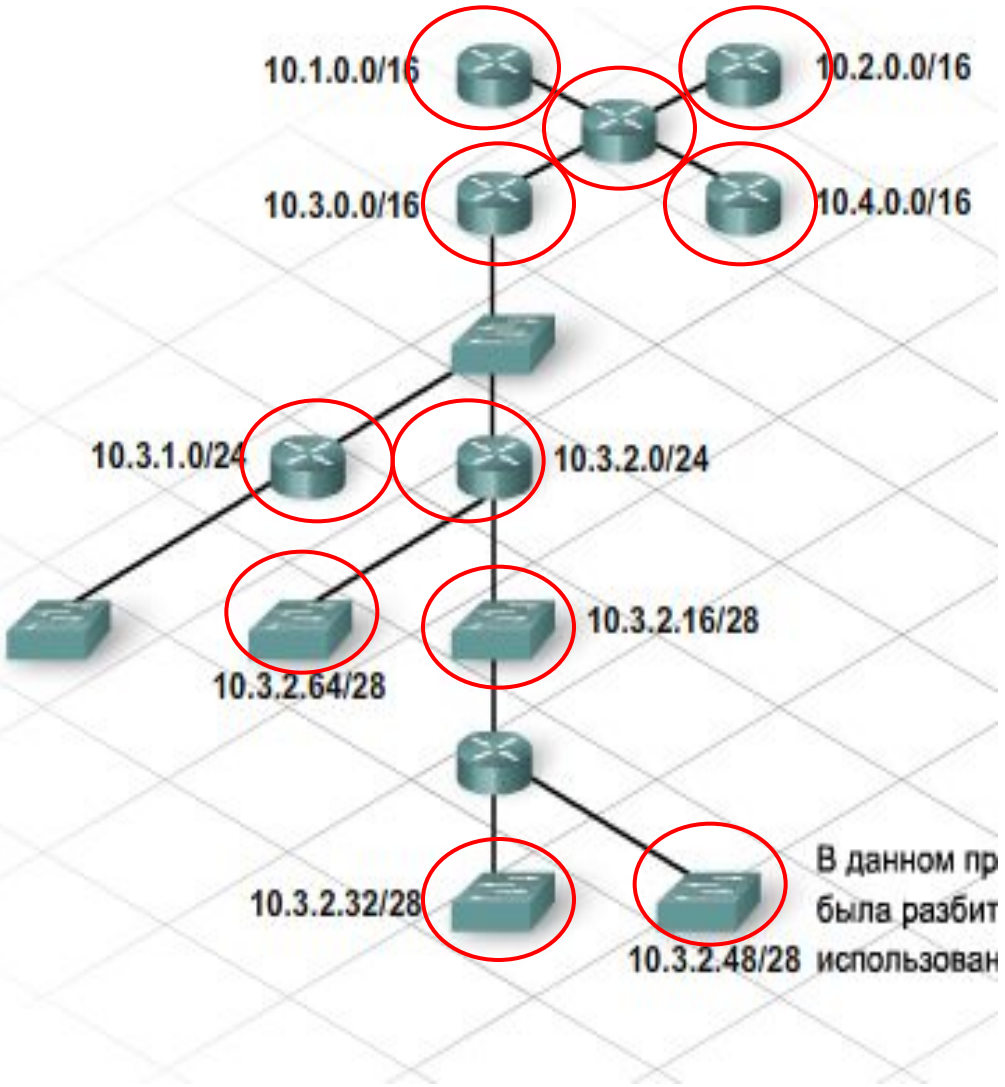
- **Маски подсети переменной длины (VLSM)** обеспечивают эффективное использование адресного пространства. Они также позволяют использовать иерархическую IP-адресацию, за счет которой маршрутизаторы могут эффективно применять суммирование маршрутов.

- **VLSM** - это концепция, используемая при разделении подсети на подсети. Они были изначально разработаны для повышения эффективности адресации. С внедрением частной адресации основное преимущество VLSM в настоящее время - организация и объединение.

- Преимущества VLSM:
  - позволяет эффективно использовать адресное пространство;
  - позволяет использовать маски подсети разной длины;
  - разбивает блок адресов на менее крупные блоки;
  - позволяет суммировать маршруты;
  - обеспечивает большую гибкость при конструировании сети;
  - поддерживает иерархические корпоративные сети.

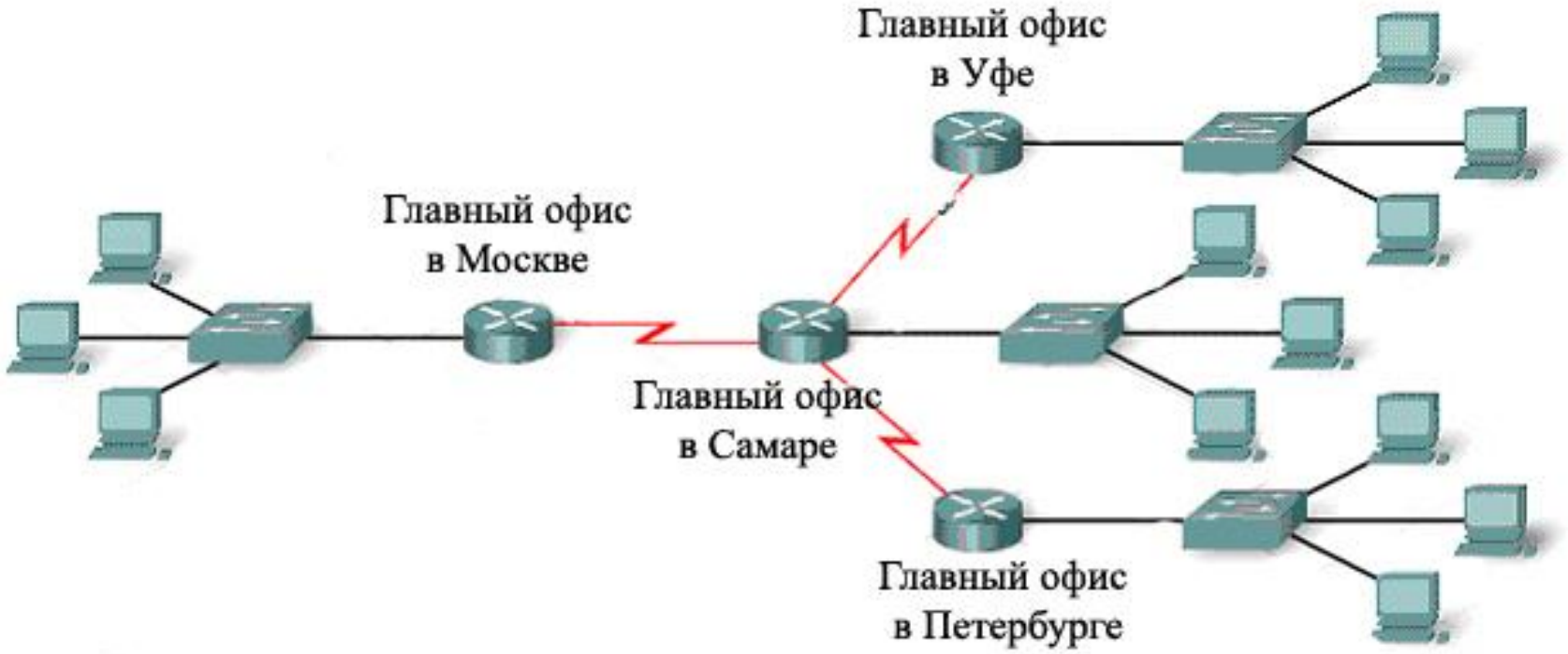
Маски подсети переменной длины - VLSM

- Сеть 10.0.0.0/8 с маской подсети /16 делится на 256 подсетей, каждая из которых может поддерживать 16382 узла:
  - 10.0.0.0/16
  - 10.1.0.0/16
  - 10.2.0.0/16 до 10.255.0.0/16
- Применив маску подсети /24 к любой из этих подсетей /16 (например, 10.1.0.0/16), можно получить разбиение на 256 подсетей. В каждой из этих новых подсетей можно поддерживать 254 узла:
  - 10.1.1.0/24
  - 10.1.2.0/24
  - 10.1.3.0/24 до 10.1.255.0/24
- Применив маску подсети /28 к любой из этих подсетей /24 (например, 10.1.3.0/28), можно получить разбиение на 16 подсетей. В каждой из этих новых подсетей можно поддерживать 14 узлов:
  - 10.1.3.0/28
  - 10.1.3.16/28
  - 10.1.3.32/28 до 10.1.3.240/28



Конструирование схемы IP-адресации с использованием VLSM

- Пусть к сети предъявляются следующие требования:
  - главный офис в Москве = 58 адресов узлов;
  - главный офис в Петербурге = 26 адресов узлов;
  - главный офис в Самаре = 10 адресов узлов;
  - главный офис в Уфе = 10 адресов узлов;
  - каналы связи через сети WAN = 2 адреса узлов (каждый).

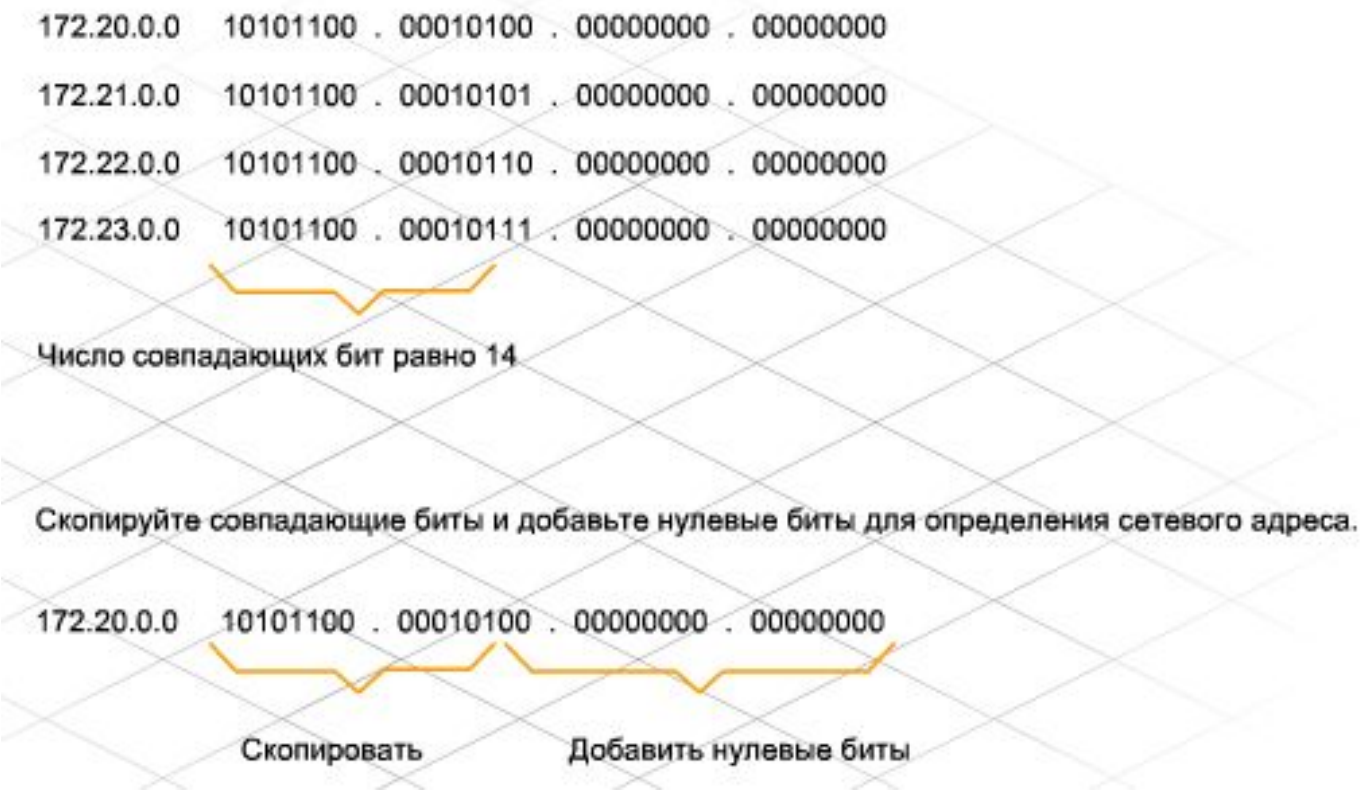


Конструирование схемы IP-адресации с использованием VLSM

Имя	Адрес подсети	Диапазон	Широковещат. адрес	Сеть/префикс
Главный офис в Москве – 58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
Главный офис в Петербурге – 28	192.168.15.64	.65 - .94	.95	192.168.15.64/27
Главный офис в Самаре – 10	192.168.15.96	.97 - .110	.111	192.168.15.96/28
Главный офис в Уфе – 10	192.168.15.112	.113 - .126	.127	192.168.15.112/28
WAN1 – 2	192.168.15.128	.129 - .130	.131	192.168.15.128/30
WAN2 – 2	192.168.15.132	.133 - .134	.135	192.168.15.132/30
WAN3 - 2	192.168.15.136	.137 - .138	.139	192.168.15.136/30

Расчет объединения маршрутов

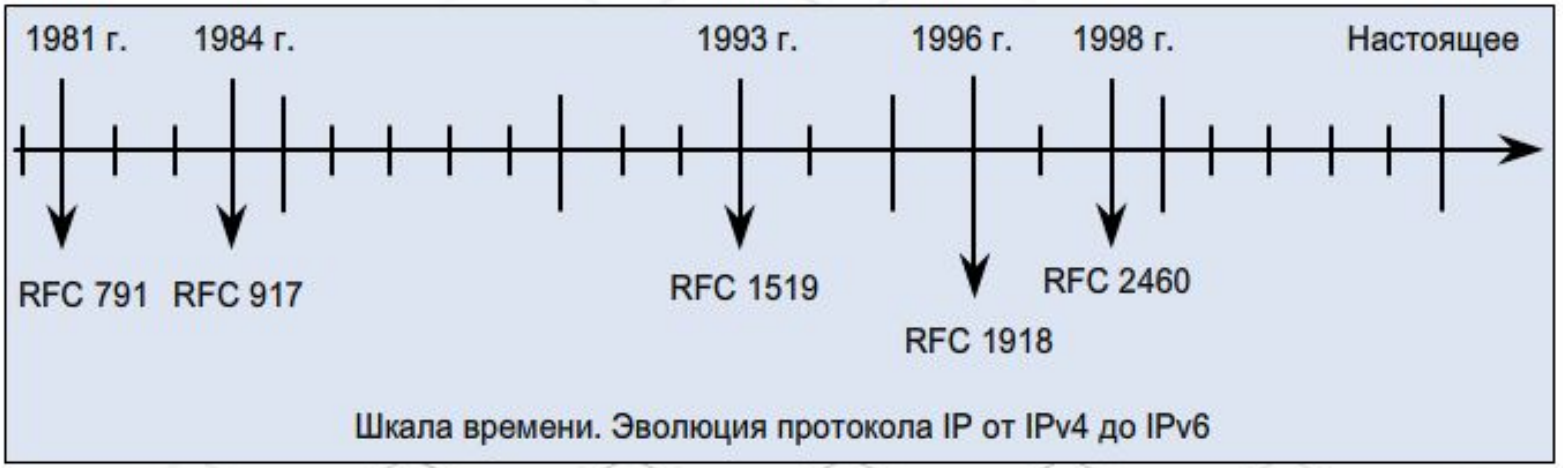
- Перечислите сети в двоичном формате
- Подсчитайте число самых левых совпадающих битов для определения маски для объединенного маршрута. Это число соответствует сетевому префиксу или маске подсети для объединенного маршрута.
- Определите адрес объединенной сети. Скопируйте совпадающие биты, а затем добавьте нулевые биты в конец.



Базовые рекомендации

- используйте более новые протоколы маршрутизации, поддерживающие VLSM и несмежные подсети;
- при необходимости отключите автоматическое объединение;
- используйте во всей сети один и тот же протокол маршрутизации;
- используйте современный маршрутизатор IOS, поддерживающий использование нулевой подсети;
- не смешивайте диапазоны частных сетевых адресов в одной и той же сети;
- по возможности избегайте возникновения несмежных подсетей;
- используйте VLSM, чтобы максимизировать эффективность адресации;
- назначайте диапазоны VLSM с учетом требований от самой крупной до самой мелкой подсети;
- предусматривайте объединение с использованием моделей иерархической сети и непрерывной адресации;
- выполняйте объединение на границах сетей;
- используйте диапазоны /30 для каналов связи через сети WAN;
- при планировании числа подсетей и поддерживаемых узлов учитывайте рост в будущем.

IPv6



Шкала времени. Эволюция протокола IP от IPv4 до IPv6

- Общий список улучшений, предложенных в IPv6:
  - расширение адресного пространства;
  - более совершенное управление адресным пространством;
  - упрощенное управление TCP/IP;
  - модернизация функций маршрутизации;
  - усовершенствованная поддержка многоадресных рассылок, безопасности и мобильности.

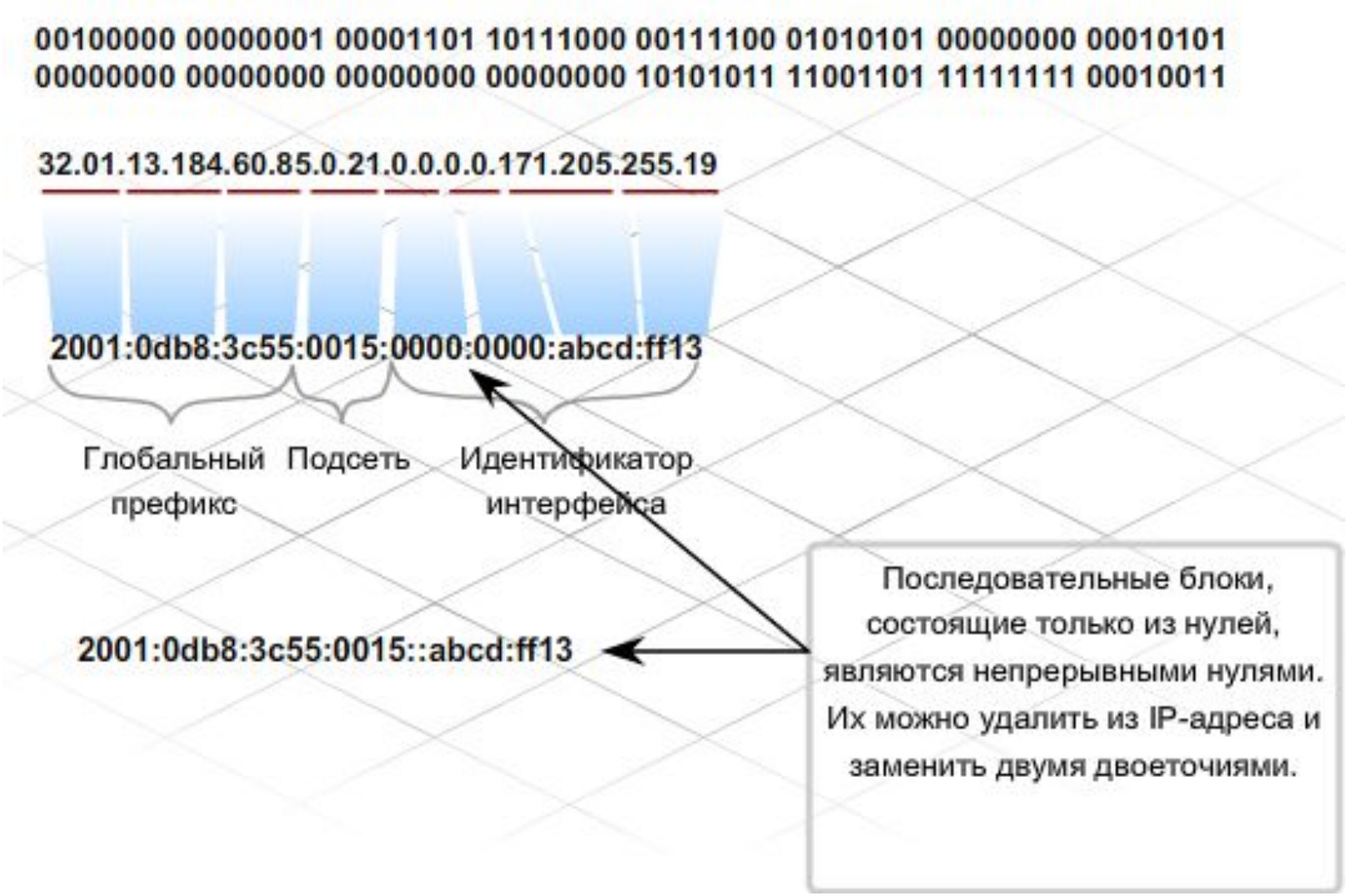
IPv6

- В IPv6 используются 128-битные IP-адреса, а возможный размер адресного пространства составляет 2^128. В десятичном выражении это, приблизительно, 3 с 38 нулями. *Если адресное пространство IPv4 представить в виде чайной ложки, то пространство IPv6 - это нечто размером с планету Сатурн.*

- В адресах IPv6 128 бит представлены в виде 32 шестнадцатеричных чисел, разделенных на восемь групп, в каждой группе 4 числа, и группы разделены между собой разделителем в виде двоеточия.

- Адреса IPv6 состоят из трех частей. Первые три блока адреса занимает глобальный префикс, присвоенный организации регистратором доменных имен в Интернете. Идентификатор подсети и интерфейса (ID) присваивает администратор сети.

IPv6


00100000 00000001 00001101 10111000 00111100 01010101 00000000 00010101
00000000 00000000 00000000 00000000 10101011 11001101 11111111 00010011
32.01.13.184.60.85.0.21.0.0.0.0.171.205.255.19
2001:0db8:3c55:0015:0000:0000:abcd:ff13
Глобальный префикс
Подсеть
Идентификатор интерфейса
2001:0db8:3c55:0015::abcd:ff13
Последовательные блоки, состоящие только из нулей, являются непрерывными нулями. Их можно удалить из IP-адреса и заменить двумя двоеточиями.

Преобразование частных адресов в публичные

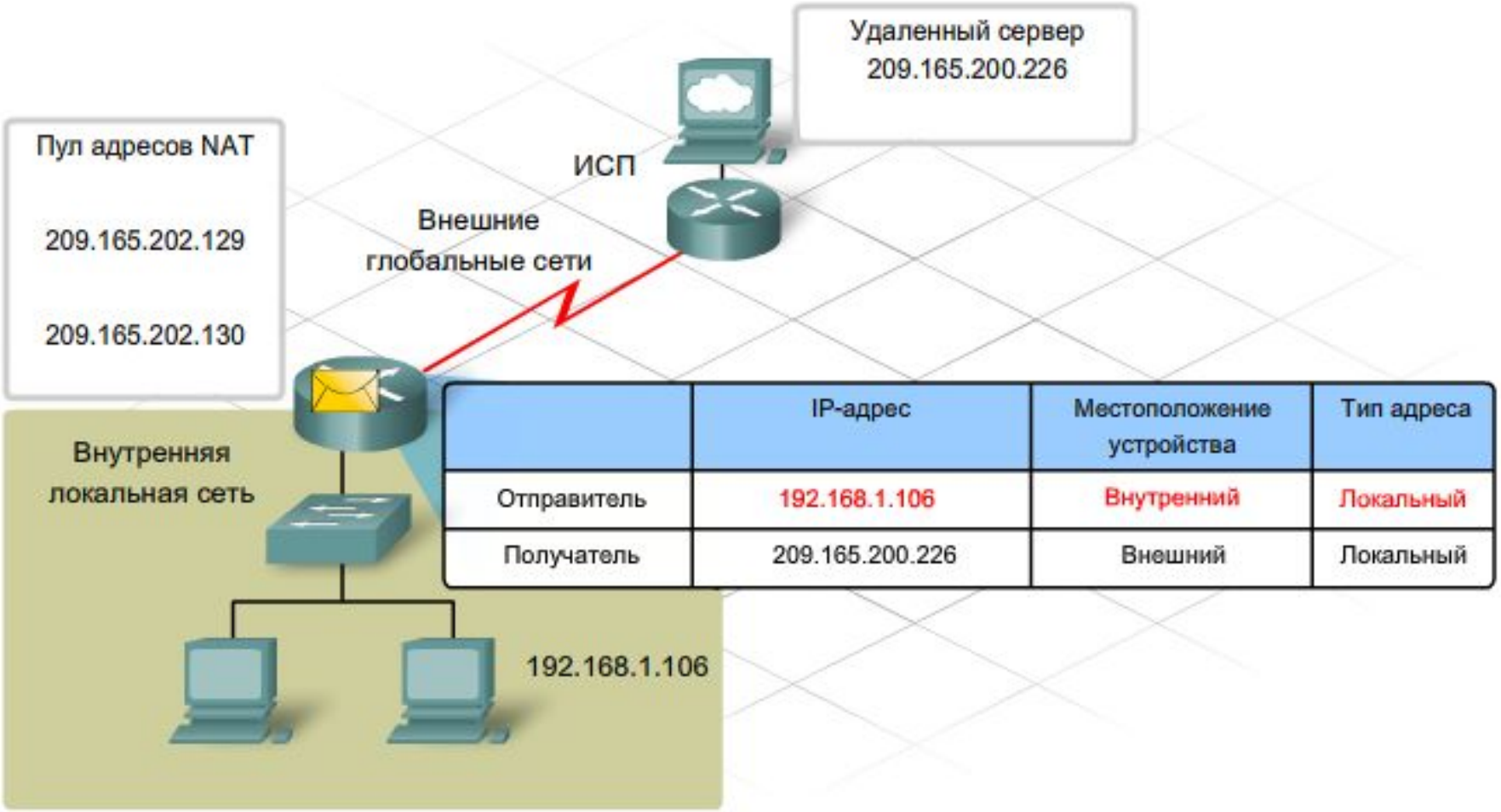
- Преобразование сетевых адресов (NAT – *N*etwork *A*ddress *T*ransformation) позволяет большой группе частных пользователей подключаться к Интернету через небольшой пул публичных IP-адресов.

Преимущества NAT	Недостатки NAT
• Совместное использование публичных IP-адресов; • Прозрачность для конечных пользователей; • Повышенная безопасность; • Расширяемость или масштабируемость локальной сети; • Локальное управление при подключении посредством Интернет-провайдера.	• Несовместимость с некоторыми приложениями; • Затруднение удаленного доступа; • Снижение производительности по причине увеличение обработки маршрутизатором.

Терминология NAT

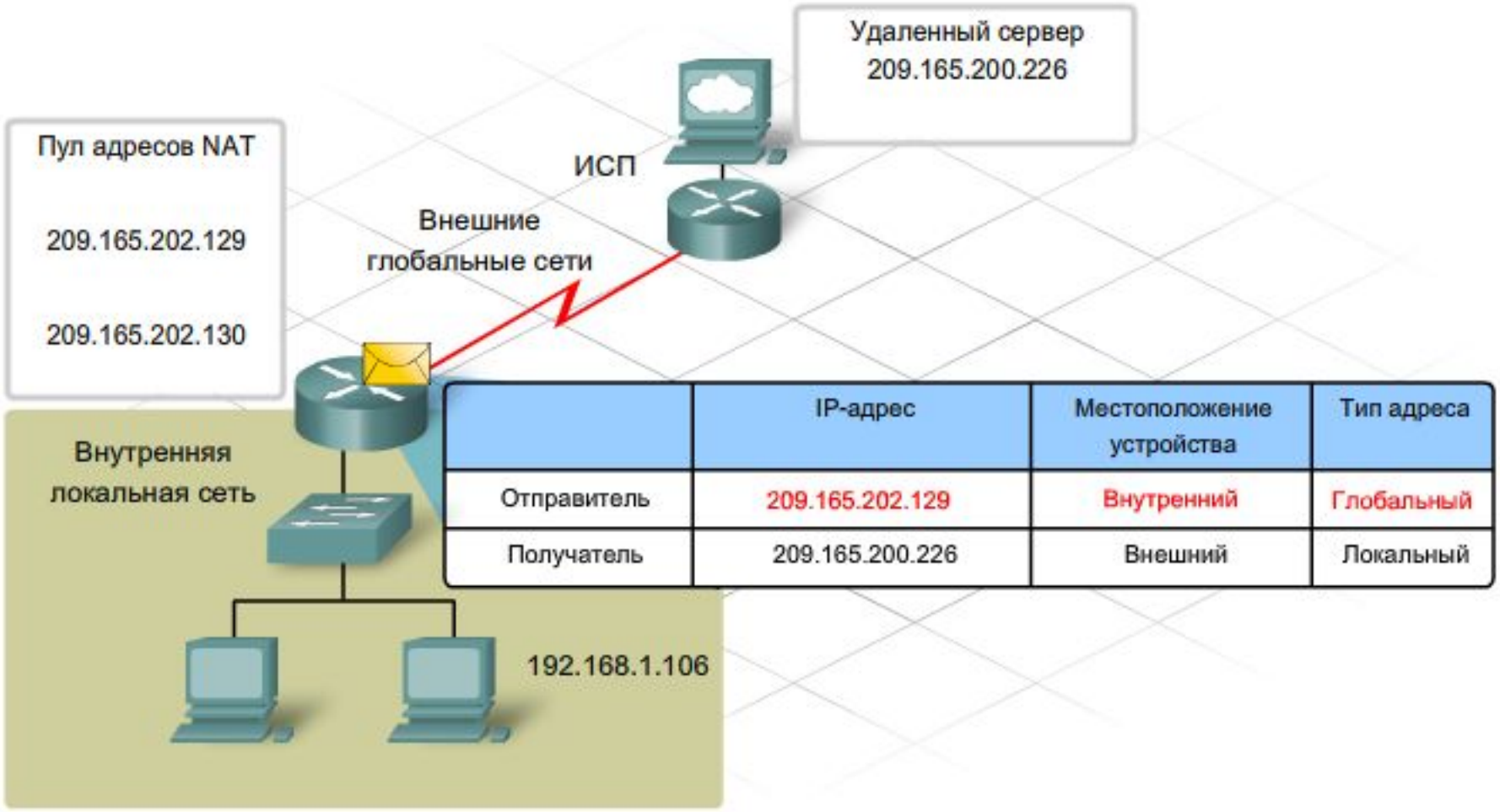
- **Внутренней локальной сетью** называется любая сеть, подключенная к интерфейсу маршрутизатора и входящая в ЛВС с частной адресацией. IP-адреса узлов во внутренних сетях преобразуются **до** передачи внешним адресатам.
- **Внешняя глобальная сеть** - это любая сеть, подключенная к внешнему по отношению к ЛВС маршрутизатору и не распознающая частные адреса узлов в ЛВС.
- **Внутренний локальный адрес** - это частный IP-адрес узла по внутренней сети. До передачи за пределы структуры адресации локальной сети его нужно преобразовать.
- **Внутренний глобальный адрес** - это IP-адрес внутреннего узла, который используется во внешней сети. Это преобразованный IP-адрес.
- **Внешний локальный адрес** - это адрес узла назначения пакета, находящегося в локальной сети. Обычно он совпадает с внешним глобальным адресом.
- **Внешний глобальный адрес** - это реальный частный IP-адрес внешнего узла. Адрес выделяется из пространства глобально маршрутизируемых адресов или сетевых адресов.

Преобразование NAT



	IP-адрес	Местоположение устройства	Тип адреса
Отправитель	192.168.1.106	Внутренний	Локальный
Получатель	209.165.200.226	Внешний	Локальный

Преобразование NAT



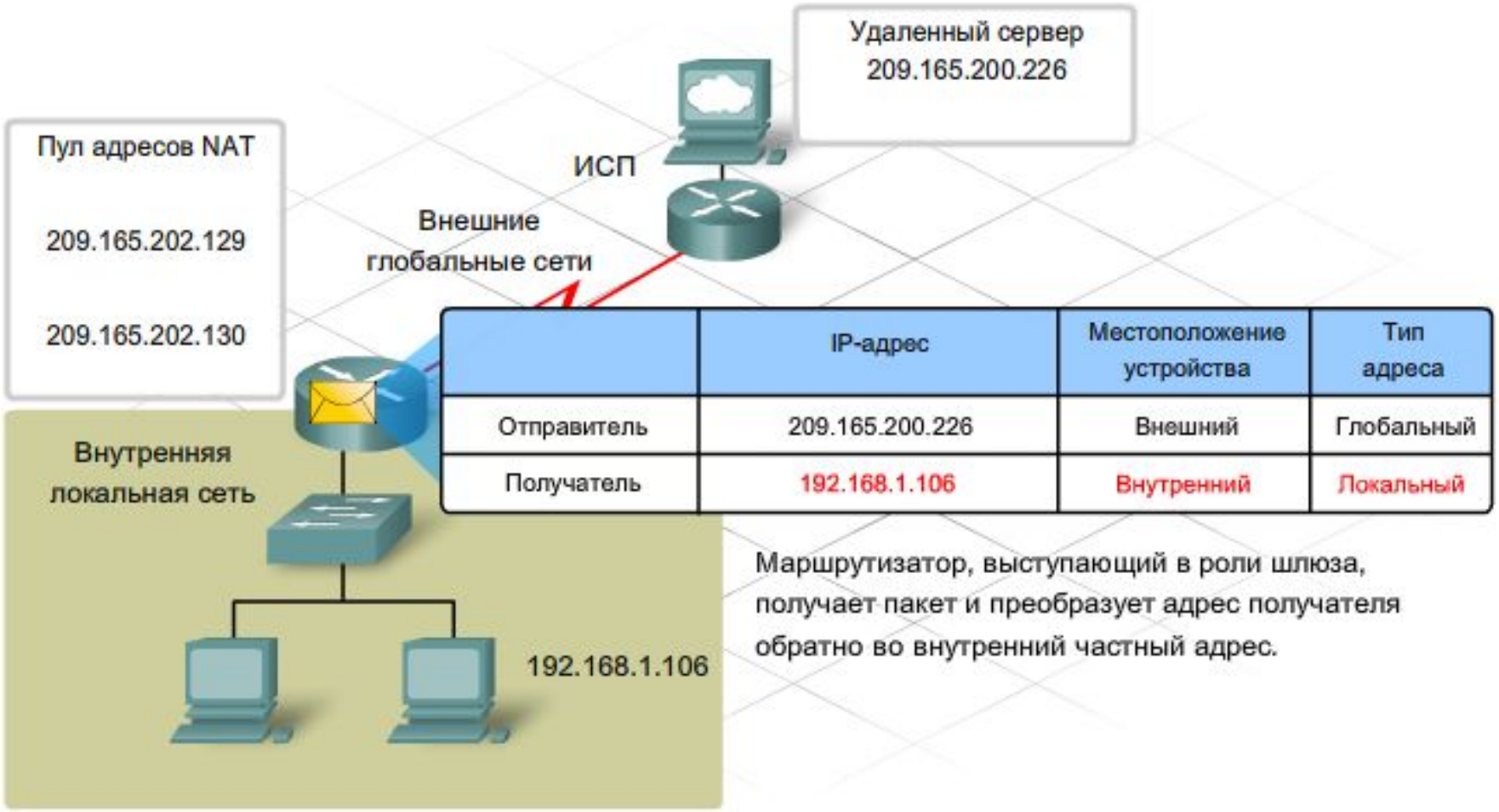
	IP-адрес	Местоположение устройства	Тип адреса
Отправитель	209.165.202.129	Внутренний	Глобальный
Получатель	209.165.200.226	Внешний	Локальный

Преобразование NAT

	IP-адрес	Местоположение устройства	Тип адреса
Отправитель	209.165.200.226	Внешний	Глобальный
Получатель	209.165.202.129	Внутренний	Глобальный

При ответе удаленный сервер использует преобразованный адрес в качестве адреса получателя пакета.

Преобразование NAT



	IP-адрес	Местоположение устройства	Тип адреса
Отправитель	209.165.200.226	Внешний	Глобальный
Получатель	192.168.1.106	Внутренний	Локальный

Маршрутизатор, выступающий в роли шлюза, получает пакет и преобразует адрес получателя обратно во внутренний частный адрес.

Статическое и динамическое преобразование NAT

- Статические преобразования гарантируют, что частный IP-адрес отдельного узла будет всегда преобразовываться в один и тот же зарегистрированный глобальный адрес. Кроме того, благодаря этому адрес никогда не получит другой локальный узел.

- Динамическое преобразование NAT происходит в том случае, если маршрутизатор присваивает IP-адреса из доступного пула внешних глобальных адресов. Пока сессия открыта, маршрутизатор отслеживает внутренние глобальные адреса и отправляет подтверждения внутренним устройствам. В конце сеанса он просто возвращает внутренний глобальный адрес в пул.

Преобразование сетевых адресов на основании портов (PAT)

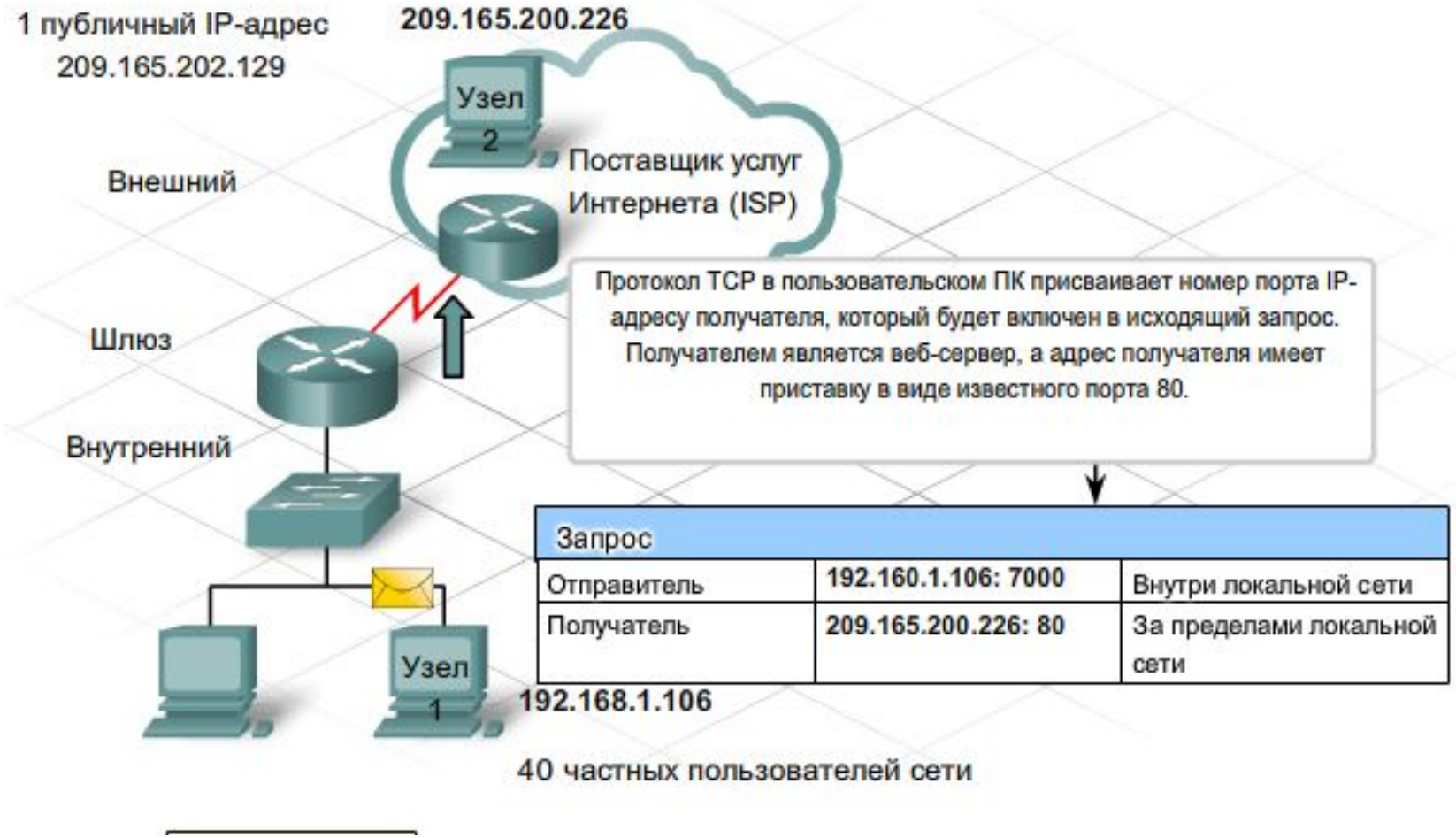
- Если зарегистрированный пул IP-адресов организации очень небольшой или если у нее есть всего один IP-адрес, к общедоступной сети все равно могут одновременно подключаться несколько пользователей, с использованием механизма, который называется перегрузкой NAT или преобразованием адресов портов (PAT).

- В режиме PAT шлюз преобразует адрес локального источника и номер порта из пакета в один глобальный IP-адрес и уникальный номер порта выше **1024**. Хотя каждый узел получает одинаковый глобальный IP-адрес, номер порта остается уникальным.

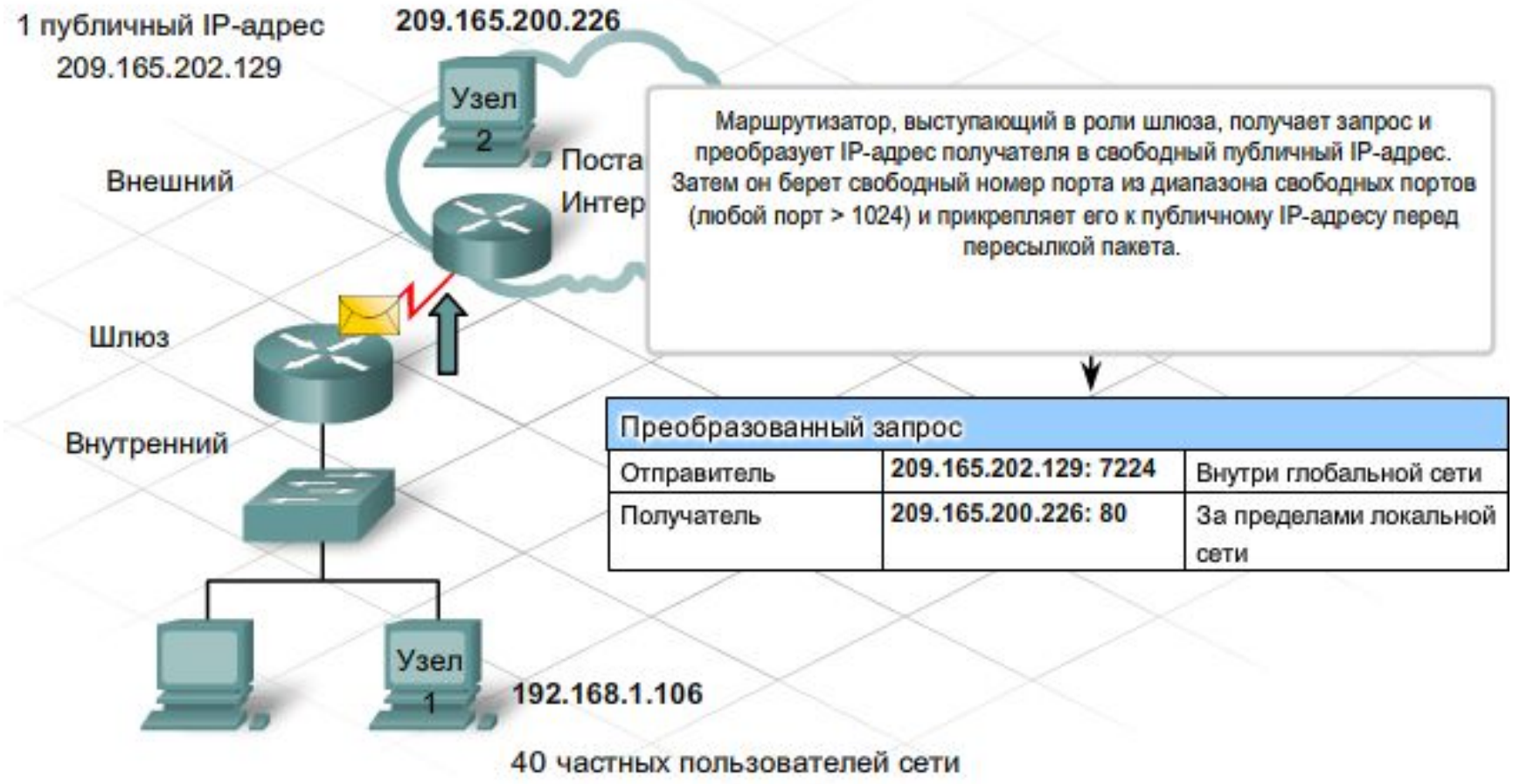
- Ответный трафик адресуется на преобразованный IP-адрес и номер порта узла. В таблице маршрутизатора находится список внутренних IP-адресов и номеров портов, которые преобразуются во внешние адреса. Ответный трафик направляется на соответствующий внутренний адрес и номер порта.

- Преобразование на основе локального адреса и локального порта выполняется отдельно для каждого соединения, при котором генерируется новый порт источника.

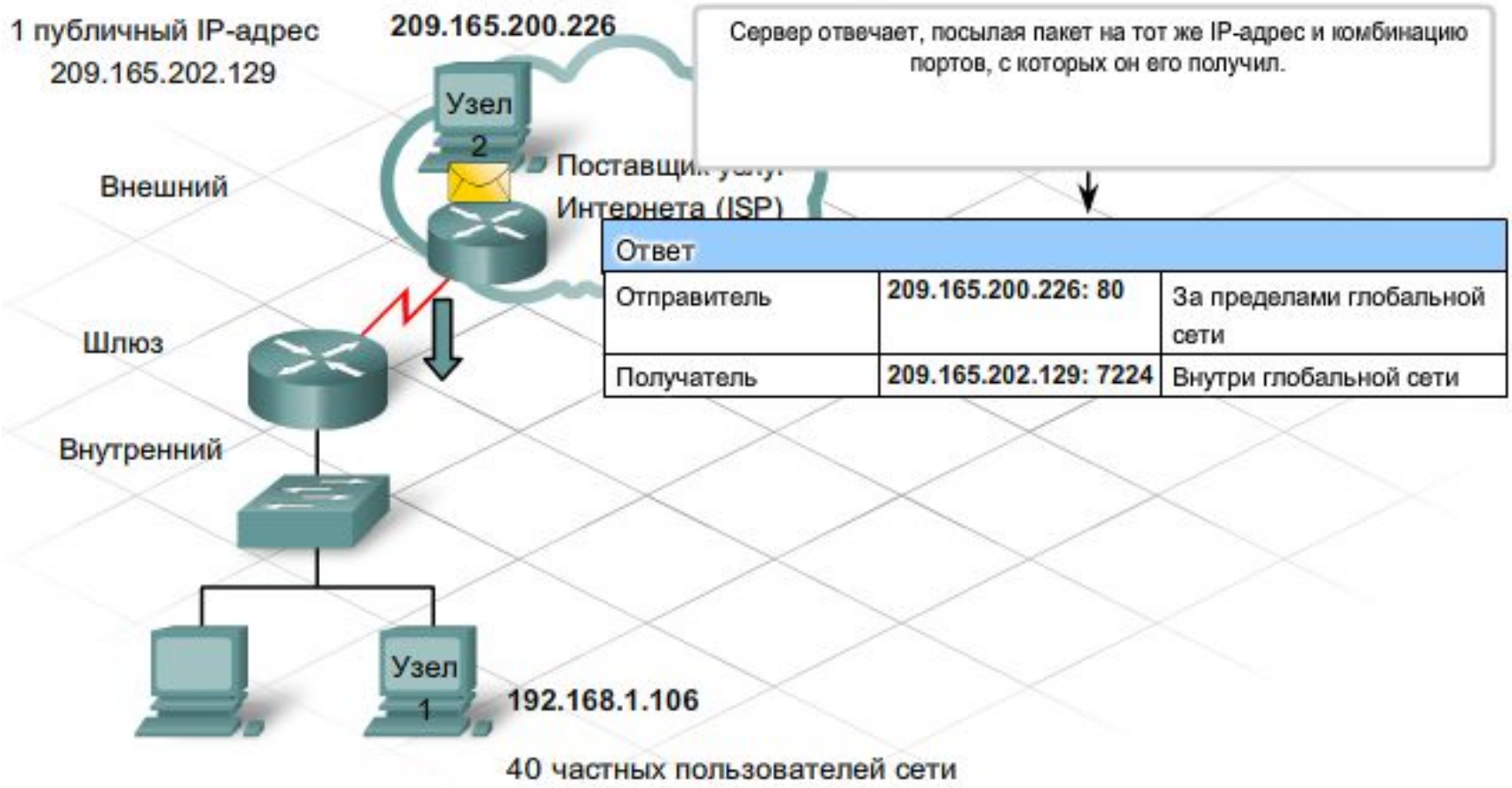
Преобразование сетевых адресов на основании портов (PAT)



Преобразование сетевых адресов на основании портов (PAT)



Преобразование сетевых адресов на основании портов (PAT)



Преобразование сетевых адресов на основании портов (PAT)

Настройка преобразования NAT

- При настройке статического или динамического преобразования NAT:
  - перечислите все серверы, для которых необходим постоянный внешний адрес;
  - определите, для каких внутренних узлов необходимо преобразование;
  - определите, какие интерфейсы являются источником внутреннего трафика (они станут внутренними интерфейсами);
  - определите, какой интерфейс передает трафик в Интернет (он станет внешним интерфейсом);
  - определите диапазон доступных публичных адресов.

- Настройка статического преобразования NAT
  - Определите публичный IP-адрес, который должны использовать внешние пользователи для получения доступа к внутреннему устройству/серверу. Администраторы обычно используют адреса, расположенные в начале или в конце диапазона статического NAT. Сопоставьте внутренний (частный) адрес с публичным адресом.
  - Настройте внутренний и внешний интерфейсы.

- Настройка динамического NAT
  - Укажите пул доступных публичных IP-адресов.
  - Создайте список контроля доступа (ACL-список) и укажите узлы, для которых требуется выполнять преобразование.
  - Назначьте интерфейсы как внутренние или внешние.
  - Свяжите список доступа и пул адресов.

Настройка преобразования PAT

- Для настройки PAT необходимо выполнить те же самые основные шаги и команды, что и при настройке NAT. Однако вместо преобразования в пул адресов PAT преобразует в один адрес. Для преобразования внутренних адресов в IP-адрес последовательного интерфейса используйте следующую команду:

  ip nat inside source list 1 interface serial 0/0/0 overload

- Для проверки функциональных возможностей NAT и PAT используйте следующие команды.

  show ip nat translations

  Эта команда отображает активные преобразования. Если преобразование не используется, его срок действия через некоторое время истечет. Записи статического преобразования NAT остаются в таблице постоянно. Записи динамического преобразования NAT требуют выполнения некоторого действия от узла в отношении внешней сети. При правильно выполненной настройке простой эхо-запрос или трассировка создают запись в таблице NAT.

  show ip nat statistics

- Эта команда отображает статистику по преобразованиям, включая число использованных адресов и число попаданий и пропусков. Выходные данные также содержат список доступа, указывающий внутренние адреса, пул глобальных адресов и диапазон указанных адресов.

Первоначальная настройка сетевых устройств

- Существуют два возможных метода подключения сетевого устройства к компьютеру для настройки и мониторинга: внутриполосное и внеполосное управление.

  - *Внеполосное управление* - необходим компьютер, непосредственно подключенный к порту консоли или вспомогательному порту (AUX) сетевого устройства. Подключение устройства к локальной сети при этом не требуется. Для работы в режиме внеполосного управления необходимо установить на ПК *эмулятор терминала*.

  - *Внутриполосное управление* - используется для удаленного мониторинга и изменения конфигурации сетевого устройства. Для подключения устройства Cisco в режиме внутриполосного управления используется два протокола TCP/IP: Telnet и HTTP.

Программы Cisco IOS

- *Интерфейс командной строки Cisco IOS (CLI)* - это текстовая программа, позволяющая вводить и исполнять команды Cisco IOS, и таким образом настраивать, отслеживать и обслуживать устройства Cisco.
- *Менеджер маршрутизации и устройств безопасности Cisco (SDM)* - это средство управления устройствами с графическим интерфейсом (GUI). В отличие от CLI, SDM поддерживает *только внутриполосное* управление. SDM Express упрощает первоначальную настройку маршрутизатора. Базовая конфигурация маршрутизатора создается быстро и легко, в пошаговом режиме. Более сложные задачи выполняются в полном пакете SDM: настройка дополнительных соединений LAN и WAN; создание межсетевых экранов; настройка соединений VPN; выполнение задач по обеспечению безопасности.

Файлы конфигурации устройств

- *Файл текущей конфигурации* - термин "текущая конфигурация" относится к наличной конфигурации устройства. В файле содержатся команды, определяющие принципы работы устройства в сети. Текущая конфигурация хранится в оперативной памяти устройства. Если не сохранить текущую конфигурацию устройства в файл начальной конфигурации, после отключения устройства она будет стерта.

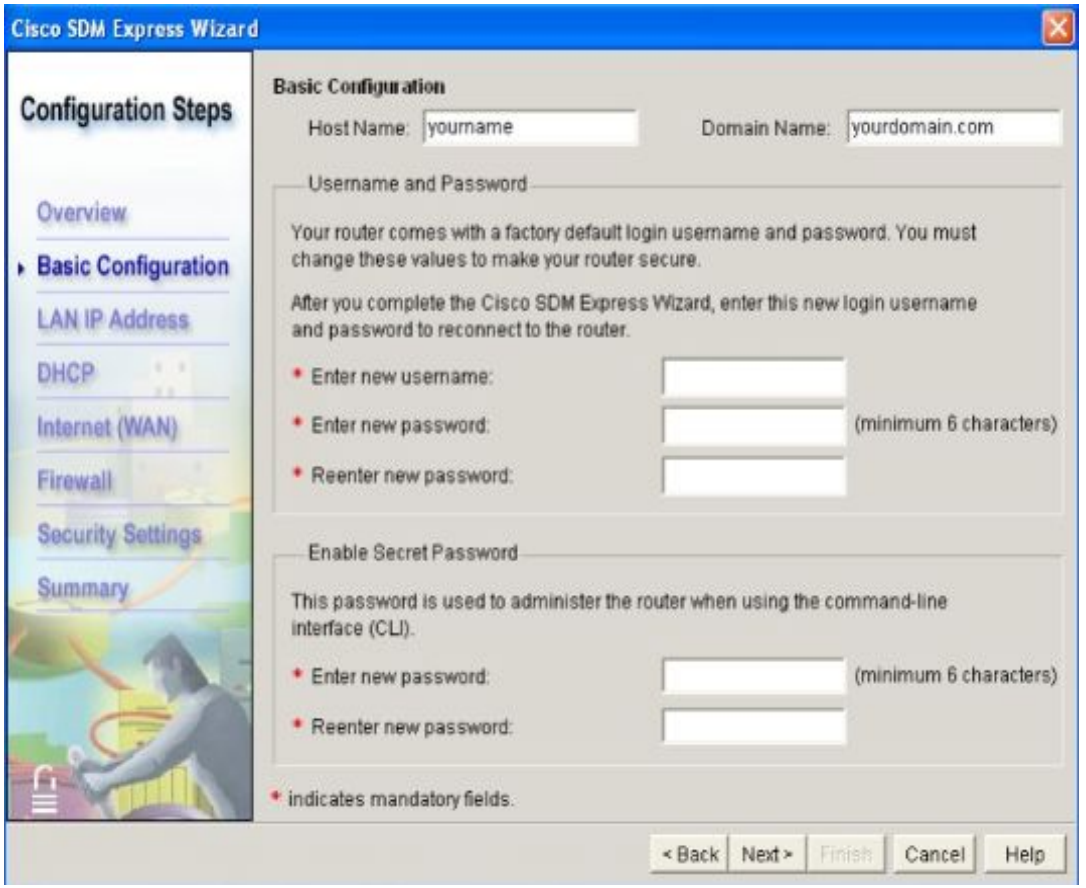
- *Файл начальной конфигурации* - это сохраненный файл конфигурации, устанавливающий при каждом включении устройства определенные характеристики конфигурации. Этот файл хранится в энергонезависимой памяти (NVRAM).

- Если изменения предполагается сохранить и после отключения питания, нужно *вручную скопировать текущую конфигурацию в файл начальной конфигурации*. В Cisco CLI для сохранения текущей конфигурации маршрутизатора в файл используется команда

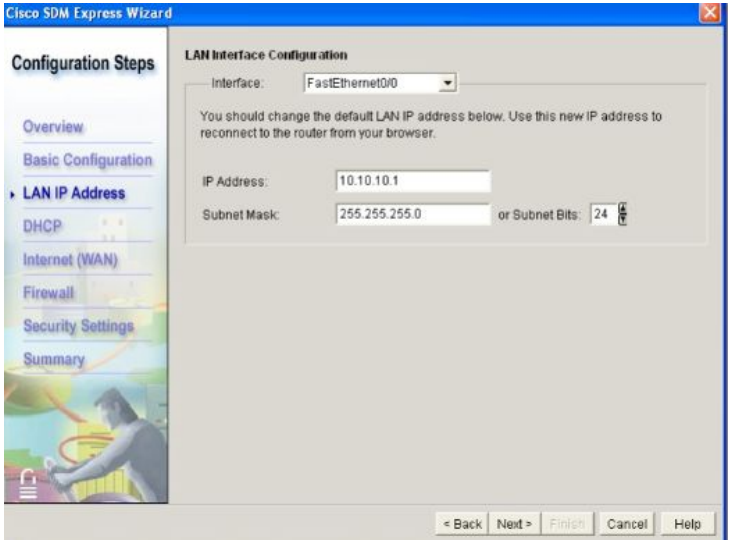
  copy running-config startup-config

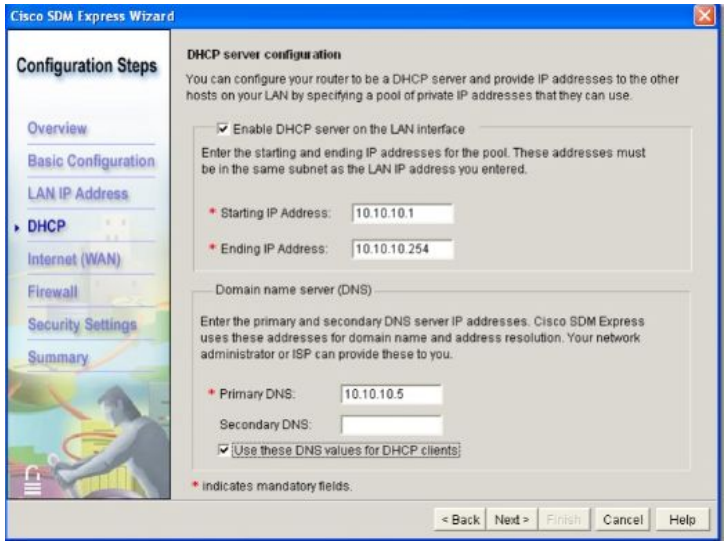
Настройка ISR в SDM

- В SDM Express предусмотрено восемь этапов создания базовой конфигурации:
  - обзор;
  - базовая конфигурация;
  - IP-адрес ЛВС;
  - DHCP;
  - Интернет (WAN);
  - межсетевой экран;
  - настройки безопасности;
  - сводка.



- Для настройки маршрутизатора необходимо указать:
  - IP-адрес интерфейса ЛВС;
  - Маску подсети (десятичное и битовое представления);
  - Параметры беспроводной связи.
- Настройка DHCP:
  - Отметить поле "Enable DHCP server on the LAN interface" ;
  - Указать начальный IP-адрес - наименьший адрес диапазона, выбранный на основе IP-адреса и маски подсети;
  - Указать конечный IP-адрес;
  - Настроить дополнительные параметры DHCP (доменное имя организации, IP-адрес основного сервера DNS, IP-адрес второстепенного сервера DNS)





Настройка последовательного соединения WAN

- *Настройка связи с сетью Интернет (WAN)* - маршрутизаторы можно подключать через последовательное соединение, подключая сети, находящиеся на большом расстоянии друг от друга. Для установления связи таких сетей WAN нужно последовательное подключение через поставщика телекоммуникационных услуг, или TSP.

  Обычно каналы последовательной связи медленнее каналов Ethernet и требуют дополнительной настройки. До установки соединения обязательно выберите тип связи и инкапсуляцию протокола.

- *Последовательная инкапсуляция* - на обоих концах последовательного соединения используется одна и та же инкапсуляция. Для некоторых типов инкапсуляции нужно настроить параметры проверки подлинности, например, имя пользователя и пароль.

Типы инкапсуляции

- *High-Level Data Link Control (HDLC)* – протокол высокоуровневого управления каналом передачи данных, разработанный Международной организацией по стандартам;

- *Frame Relay* – высокоскоростная технология передачи кадров, включающая деление данных передающим устройством на кадры переменной длины, передачу кадров цифровым устройством с использованием собственного виртуального канала и сбор на приемном конце. Каждый виртуальный канал может использовать инкапсуляцию HDLC между связанными устройствами. Идентификатор канала связи (Data Link Connection Identifier - DCLI) – уникальный номер, который присваивается пункту назначения поставщиком услуг связи;

- *Point-to-Point Protocol (PPP)* – как правило, используется для связи между двумя устройствами на последовательных линиях связи – будь это прямая последовательная связь, связь поверх Ethernet, модемная связь по телефонным линиям, мобильная связь, радиоканалы или оптоволоконные линии связи. Большинство провайдеров Интернет-услуг используют PPP для предоставления доступа к сети Интернет по коммутируемым телефонным линиям. Некоторые особенности PPP позволяют выполнить аутентификацию до создания соединения. Имена пользователей и пароли PPP можно настроить с помощью SDM.

Список типов адресов

В зависимости от выбранного типа инкапсуляции, существуют различные методы получения IP-адреса через последовательный интерфейс.

- *Статический IP-адрес*: используется для инкапсуляции типов Frame Relay, PPP и HDLC; для настройки статического IP-адреса нужно ввести IP-адрес и маску подсети.

- *Ненумерованный IP*: используется для инкапсуляции типов Frame Relay, PPP и HDLC; устанавливает адрес последовательного интерфейса, соответствующий IP-адресу одного из работающих интерфейсов маршрутизатора.

- *Согласованный IP*: маршрутизатор автоматически получает IP-адрес через PPP; выберите Easy IP (IP Negotiated); маршрутизатор будет автоматически получать IP-адрес через PPP.

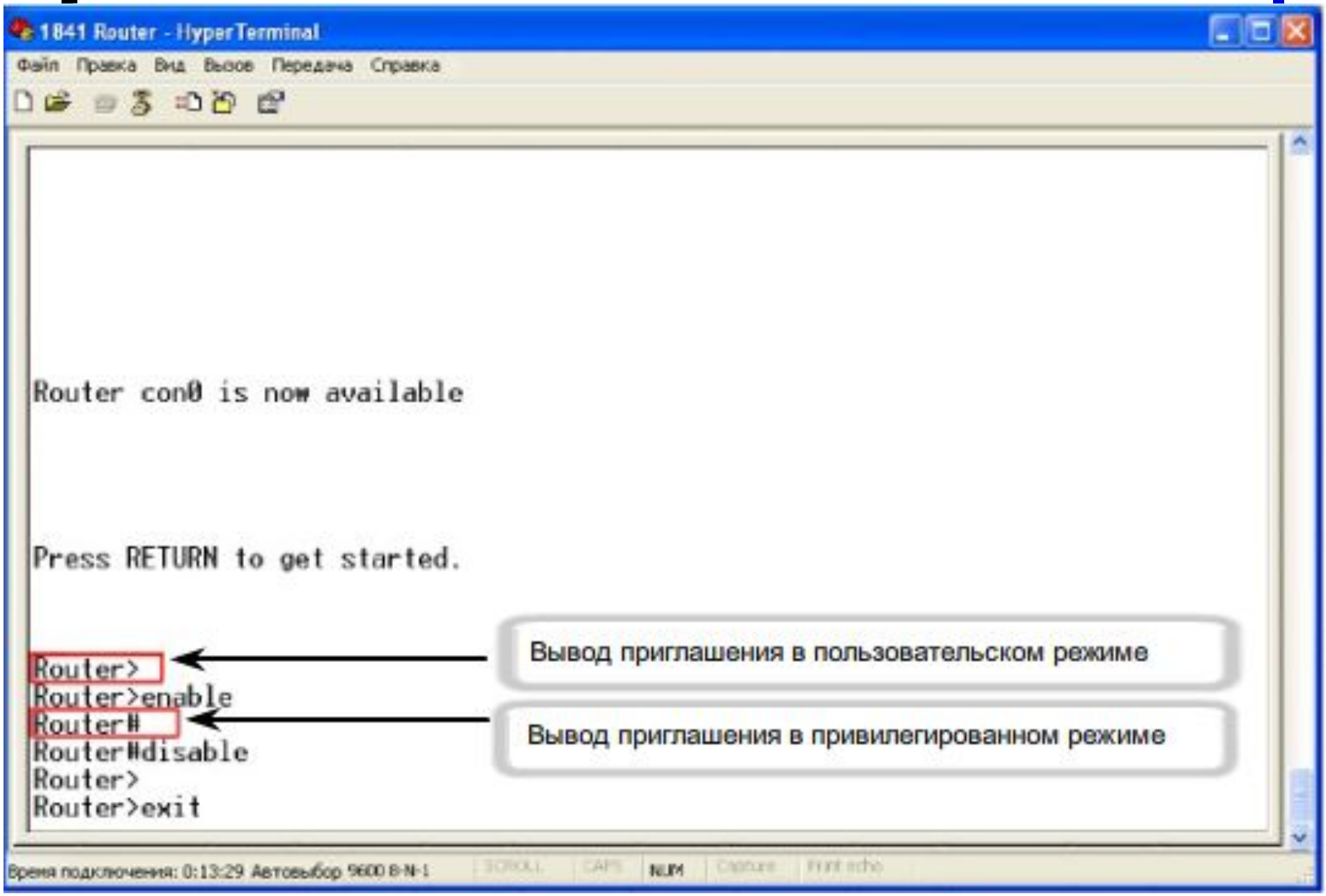
Интерфейс командной строки и режимы

- Cisco IOS поддерживает два уровня доступа к интерфейсу командной строки: *пользовательский* доступ EXEC и *привилегированный* доступ EXEC.

- В *пользовательском* режиме EXEC можно только получать информацию о работе устройств и устранять неполадки с помощью команд **ping** или **traceroute**. В пользовательском режиме в командной строке отображается следующее: **Router>**

- Для ввода команд, меняющих режим работы устройства, нужен привилегированный доступ. Чтобы переключиться в привилегированный режим EXEC, нужно ввести в командную строку **enable** и нажать **Enter**. Командная строка соответственно изменится. Отобразится **Router#**. Чтобы вернуться в пользовательский режим, введите **disable** или **exit**.

- Оба режима можно защитить *паролем* или *именем пользователя и паролем*.


1841 Router - HyperTerminal
Файл Правка Вид Вызов Передача Справка
Router con0 is now available
Press RETURN to get started.
Router>
Router>enable
Router#
Router#disable
Router>
Router>exit
Вывод приглашения в пользовательском режиме
Вывод приглашения в привилегированном режиме
Время подключения: 0:13:29 Автовыбор 9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Режимы командной строки

- Для получения доступа к командам настройки нужно, прежде всего, войти в соответствующий режим. В большинстве случаев *результат записывается с терминала в файл текущей конфигурации*. Чтобы открыть эти команды, пользователю нужно войти в режим глобальной конфигурации. Для этого введите команду:

  configure terminal

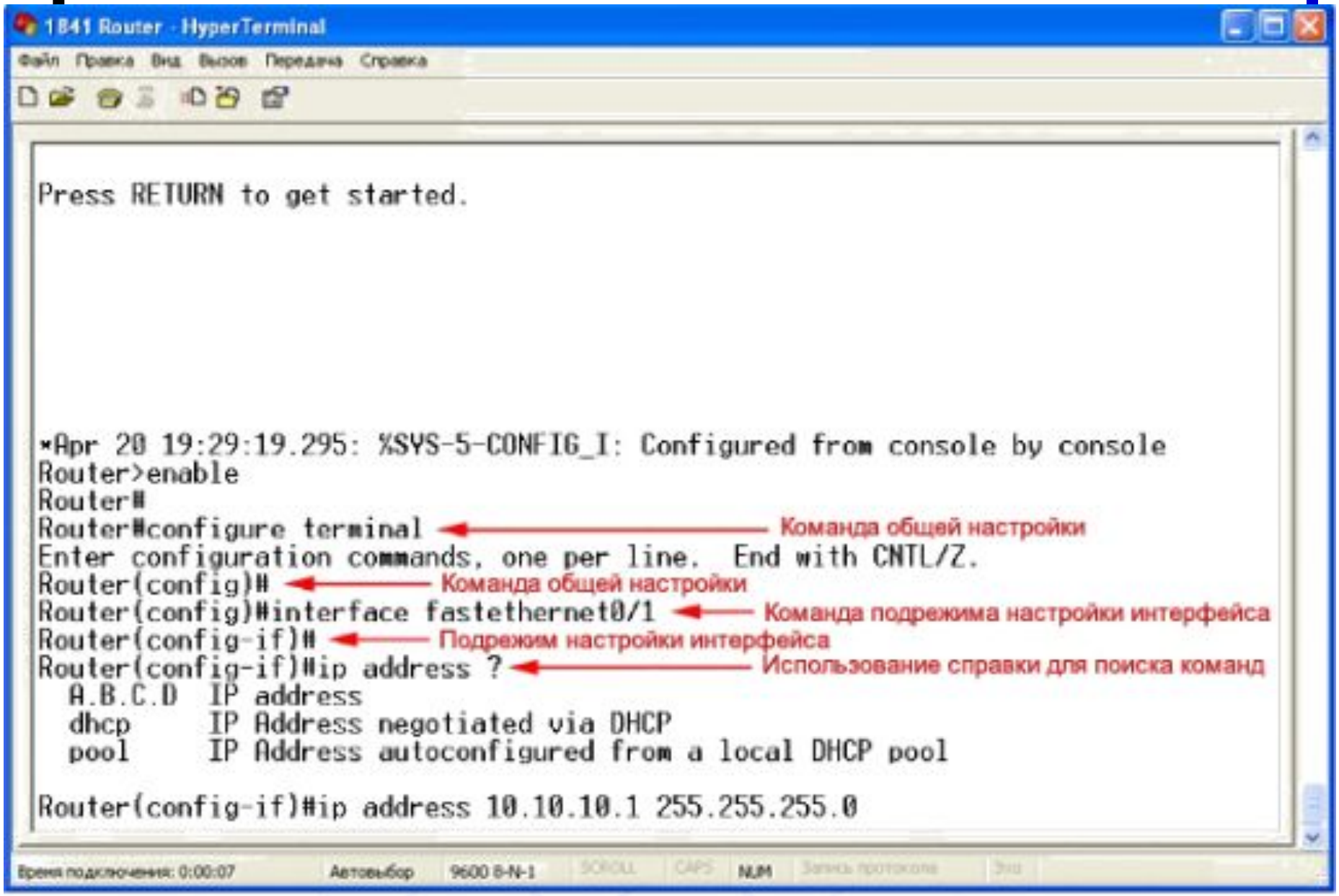
  или

  config t

- В этом режиме в командной строке отображается

  Router(config)#

  Помните, что введенные в этом режиме команды выполняются немедленно и отражаются на работе устройства.


1841 Router - HyperTerminal
Файл Правка Вид Вызов Передача Справка
Press RETURN to get started.
*Apr 20 19:29:19.295: %SYS-5-CONFIG_I: Configured from console by console
Router>enable
Router#
Router#configure terminal
Команда общей настройки
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Команда общей настройки
Router(config)#interface fastethernet0/1
Команда подрежима настройки интерфейса
Router(config-if)#
Подрежим настройки интерфейса
Router(config-if)#ip address ?
Использование справки для поиска команд
A.B.C.D IP address
dhcp IP Address negotiated via DHCP
pool IP Address autoconfigured from a local DHCP pool
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Время подключения: 0:00:07
Автовыбор
9600 8-N-1
SCROLL
CAPS
NUM
Запись протокола
Эхо

Контекстная справка

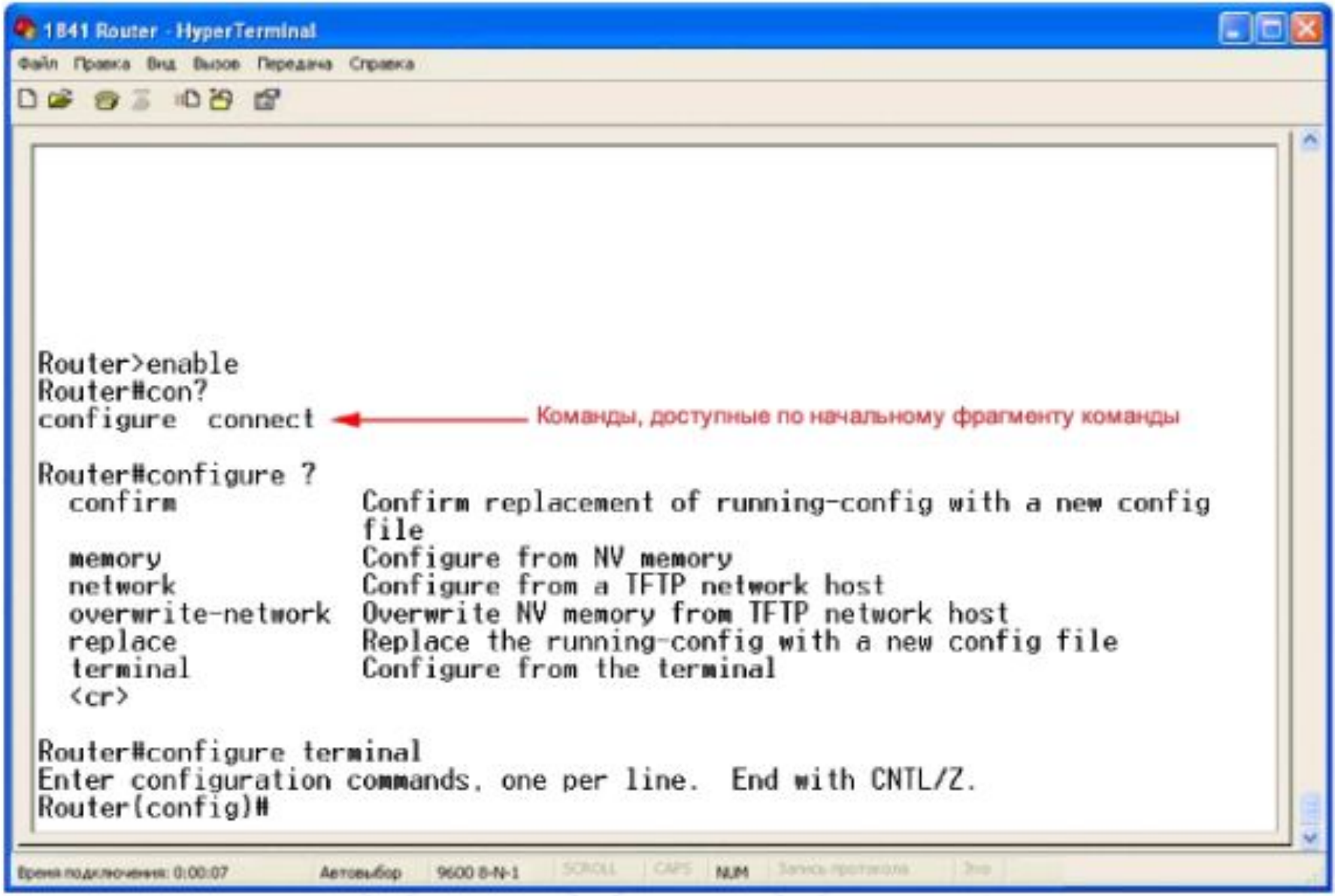
- Если ввести в командную строку **help** или **?**, отображается краткое описание справки:

Router# help

- В контекстной справке есть предложения по выполнению команды. Если первые несколько символов команды известны, нужно их ввести, а затем вставить знак **?**.

- В справке можно в любой момент уточнить дополнительные параметры команды. Для этого вводится часть команды, пробел и знак **?**. Например, если ввести в строку **configure**, пробел и знак вопроса, отобразится список возможных вариантов команды настройки. Чтобы закончить строку команды, выберите один из вариантов.

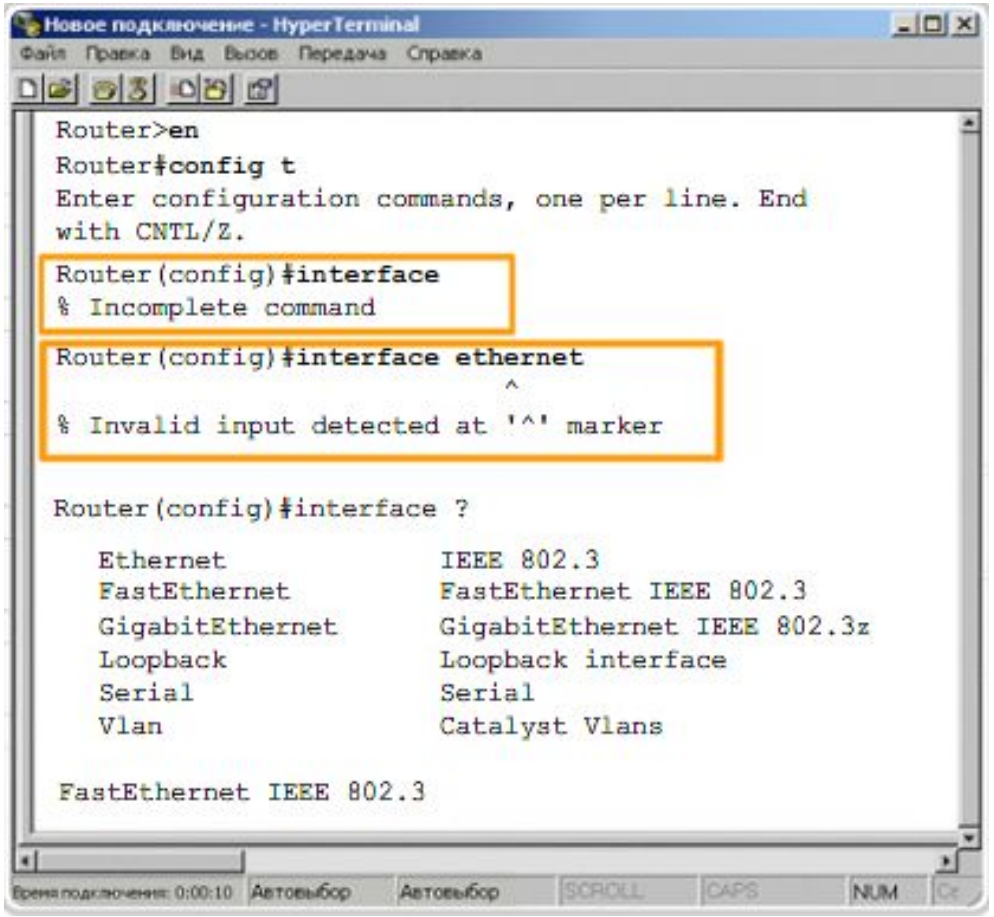
Контекстная справка



Сообщения об ошибке

- Сообщения об ошибке помечаются значком **%**. Например, если команда **interface** вводится без дополнительных параметров, появится сообщение о том, что она не полная (**% Incomplete command.**).

- В CLI есть функция поиска ошибки в виде индикатора, символа перевода каретки (**^**). Символ **^** появляется в том месте строки команды, где находится неправильный или нераспознанный символ.



История команд и клавиатурные сочетания

- *История команд* - включается по умолчанию (10 строк). Чтобы изменить количество запоминаемых командных строк, используется команда

  terminal history size

  или

  history size.

  Максимальное количество команд - 256.

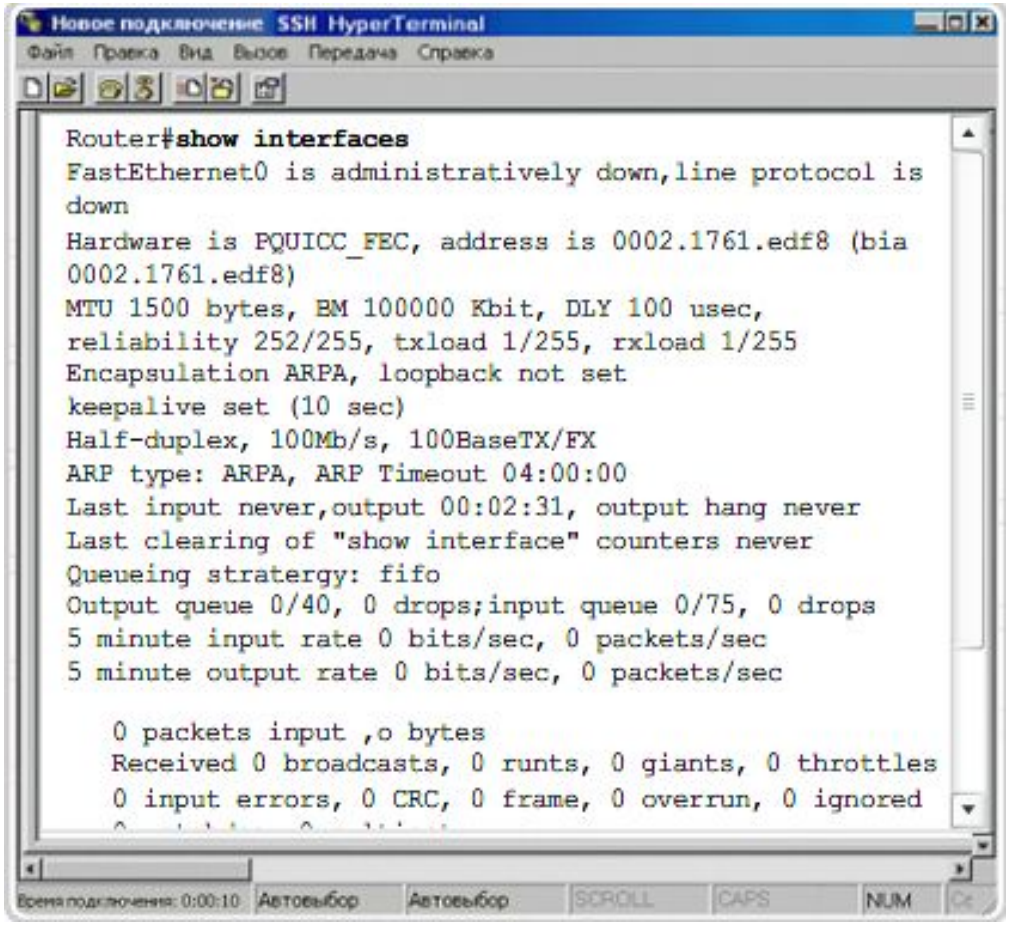
- Чтобы вызвать из буфера последнюю команду, нажмите **Ctrl-P** или кнопку со стрелкой вверх.

- Чтобы вернуться к более недавней команде из буфера, нажмите **Ctrl-N** или кнопку со стрелкой вниз.

- *Клавиатурные сочетания* - CLI распознает частично введенные команды по первым уникальным символам. Например, введите **int** вместо **interface**. Нажмите кнопку **Tab**, и CLI автоматически закончит команду. Кнопка **Tab** подтверждает, что маршрутизатор «понял» предложенную команду.

Команды show

- С помощью команды **show** можно отобразить состояние практически любого процесса или функции маршрутизатора. Наиболее популярны следующие команды **show**:
  - **show running-config;**
  - **show interfaces;**
  - **show arp;**
  - **show ip route;**
  - **show users;**
  - **show version.**



Первоначальная настройка маршрутизатора

- Первоначальная конфигурация устройства IOS предусматривает настройку имени и пароля, контролирующего доступ к различным функциям устройства.
- Настройка уникального имени: **Router(config)# hostname [name]**
- Настройка пароля доступа в привилегированный режим:

  Router(config)# enable password [пароль]
  Router(config)# enable secret [пароль]

- Настройка пароля для доступа к консоли:

  Router(config)# line console 0
  Router(config-line)# password [пароль]
  Router(config-line)# login

- Настройка доступа к виртуальному порту:

  Router(config)# line vty 0 4
  Router(config-line)# password [пароль]
  Router(config-line)# login

- Шифрование всех паролей: **service password encryption**

Настройка интерфейса маршрутизатора

- Для настройки любого интерфейса необходимо:
  - указать тип интерфейса и номер порта;
  - ввести описание интерфейса;
  - настроить IP-адрес и маску подсети интерфейса;
  - при настройке последовательного интерфейса как устройства DCE надо ввести частоту синхронизации;
  - включить интерфейс.

```
Router(config)#interface serial 0/0
Router(config-if)#description connection to Router2
Router(config-if)#ip address 192.168.1.125   255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Маршрут по умолчанию и настройка DHCP

- Чтобы настроить маршрут по умолчанию Cisco ISR, нужно находиться в режиме глобальной конфигурации:

  Router(config)# ip route 0.0.0.0 0.0.0.0 <Next Hop IP Address>

  или

  Router(config)# ip route 0.0.0.0 0.0.0.0 <interface> <port number>

- При настройке **DHCP** в CLI нужно:
  - создать пул адресов DHCP;
  - указать подсеть;
  - исключить IP-адреса;
  - указать доменное имя;
  - указать IP-адрес сервера DNS;
  - выбрать маршрутизатор по умолчанию;
  - установить время аренды;
  - проверить конфигурацию.

Пошаговая настройка DHCP

```
Router(config)# ip dhcp pool LAN-address
Router(dhcp-config)#
```

Шаг 1. Создание пула адресов DHCP

Перейдите в режим привилегированного доступа EXEC, по запросу введите пароль, затем войдите в режим глобального конфигурирования. Создайте имя пула адресов сервера DHCP. На маршрутизаторе допускается существование более одного пула адресов. Командная строка Cisco IOS войдет в режим конфигурации пула адресов DHCP. Используйте следующие команды:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp pool LAN-address
```

В данном примере создан пул адресов с именем "LAN-address"

```
Router(dhcp-config)# network 172.16.0.0 255.255.0.0
```

Шаг 2. Задание сети или подсети

Укажите адрес сети или подсети, а также маску подсети пула адресов DHCP. Используйте следующую команду:

```
Router(dhcp-config)#network 172.16.0.0 255.255.0.0
```

В зависимости от версии IOS маски подсети можно указать с помощью префикса /16.

Пошаговая настройка DHCP

```
Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103
```

Шаг 3. Исключение IP-адресов

Вспомните, что сервер DHCP полагает, что все другие IP-адреса в подсети пула адресов DHCP могут быть назначены клиентам DHCP. Исключите адреса из пула, чтобы сервер DHCP не смог их назначить. При необходимости исключения определенного диапазона адресов, достаточно указать начальный и конечный адрес. Используйте следующую команду:

```
Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103
```

В примере исключены 4 адреса: 172.16.1.100, 172.16.1.101, 172.16.1.102 и 172.16.1.103, чтобы сервер DHCP не смог назначить их узлам. Эти адреса может статически назначить администратор.

```
Router(dhcp-config)# domain-name cisco.com
```

Шаг 4. Указание доменного имени

Укажите доменное имя клиента. Используйте следующую команду:

```
Router(dhcp-config)#domain-name cisco.com
```

Клиенты в данном примере получили при конфигурировании DHCP доменное имя cisco.com. Доменное имя необязательно указывать при конфигурировании DHCP, сервер DHCP и без него сможет работать. О том, необходимо ли или нет указывать доменное имя, знает системный администратор.

Пошаговая настройка DHCP

```
Router(dhcp-config)# dns server 172.16.1.103 172.16.2.103
```

Шаг 5. IP-адрес сервера DNS

Укажите IP-адрес DNS-сервера, имеющийся для клиента DHCP. Требуется только один IP-адрес. На одной линии можно сконфигурировать до восьми IP-адресов. При перечислении нескольких DNS-серверов они вводятся в порядке важности. Используйте следующую команду:

```
Router(dhcp-config)#dns server 172.16.1.103 172.16.2.103
```

В данном примере клиенты могут использовать два DNS-сервера: первичный и вторичный. Чтобы узлы имели возможность преобразовывать имена узлов и URL-адреса для получения сетевых услуг, необходимо сконфигурировать не менее одного DNS-сервера.

```
Router(dhcp-config)# default-router 172.16.1.100
```

Шаг 6. Задание шлюза по умолчанию

Укажите IP-адрес маршрутизатора по умолчанию для клиентов DHCP в сети. Как правило, это IP-адрес интерфейса LAN маршрутизатора. С помощью этой команды задается шлюз по умолчанию для клиентских устройств в сети, которые будут пользоваться DHCP. После загрузки клиент DHCP начинает отсылать пакеты своему маршрутизатору по умолчанию. IP-адрес должен находиться в той же подсети, что и IP-адреса клиентов, назначенные маршрутизатором. Требуется только один IP-адрес. Используйте следующую команду:

```
Router(dhcp-config)#default-router 172.16.1.100
```

Клиенты в данном примере используют интерфейс маршрутизатора с адресом 172.16.1.100 в качестве шлюза по умолчанию.

Пошаговая настройка DHCP

```
lease {days [hours] [minutes]| infinite}
end
```

Шаг 7. Указание длительности аренды

DHCP предоставляет информацию об IP-адресах при каждом включении узла и подключении к сети. Время аренды определенного IP-адреса определенным узлом, заданное по умолчанию, составляет один день. Если узел не возобновляет аренду данного адреса, то после окончания срока аренды сервер DHCP может назначить этот адрес любому другому узлу. При необходимости время аренды адреса можно изменить. Это последний шаг процесса конфигурирования услуги DHCP на маршрутизаторе. Введите команду end для выхода из режима настройки сервера DHCP и возврата в режим глобального конфигурирования. Используйте следующие команды:

```
lease {days [hours] [minutes]| infinite}
end
```

В примере исключены 4 адреса: 172.16.1.100, 172.16.1.101, 172.16.1.102 и 172.16.1.103, – чтобы сервер DHCP не смог назначить их узлам. Эти адреса может статически назначить администратор. Сервер DHCP не сможет их назначить.

Пошаговая настройка DHCP

```
Router# show running-config
```

Шаг 8. Проверка конфигурации

Проверьте конфигурацию DHCP путем просмотра текущей конфигурации. Используйте следующую команду: **show running-config** DHCP DHCP:

```
!
ip dhcp pool LAN-addresses
domain-name cisco.com
network 172.16.0.0 255.255.0.0
ip dhcp excluded-address 172.16.1.100 172.16.1.103
dns-server 172.16.1.103 172.16.2.103
default-router 172.16.1.100
lease infinite
!
```

```
Router# show running-config
```

Настройка NAT

```
Router(config)# interface fastethernet 0/0
```

Шаг 1. Указание интерфейса

Перед началом настройки услуг NAT на маршрутизаторе Cisco перейдите в режим привилегированного доступа EXEC, по запросу введите пароль, затем войдите в режим глобальной конфигурации. Укажите интерфейс, соединяющий узел с локальной сетью. После этого вы войдете в режим конфигурирования интерфейса.

Используйте следующие команды:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 0/0
```

```
Router(config-if)# ip address 172.31.232.182 255.255.255.0
```

Шаг 2. Задание первичного IP-адреса

С помощью следующей команды укажите первичный IP-адрес внутреннего интерфейса:

```
Router(config-if)# ip address 172.31.232.182 255.255.255.0
```

Настройка NAT

```
Router(config-if)# ip nat inside
Router(config-if)# exit
```

Шаг 3. Указание внутреннего интерфейса

Задайте этот интерфейс в качестве интерфейса, соединяющего маршрутизатор с внутренней частью сети, а затем выйдите из режима конфигурирования внутреннего интерфейса и вернитесь в режим конфигурирования. Используйте следующие команды:

```
Router(config-if)# ip nat inside
Router(config-if)# exit
```

```
Router(config)# interface serial 0/0
```

Шаг 4. Конфигурирование внешнего интерфейса

Выполните конфигурирование внешнего интерфейса. Укажите интерфейс, соединяющий маршрутизатор с Интернет-провайдером, и вернитесь в режим конфигурирования интерфейса. Используйте следующую команду:

```
Router(config)# interface serial 0/0
```

Настройка NAT

```
Router(config-if)# ip address 209.165.201.1 255.255.255.252
```

Шаг 5. Задание первичного IP-адреса

Укажите первичный IP-адрес внешнего интерфейса. Используйте следующую команду:

```
Router(config-if)# ip address 209.165.201.1 255.255.255.252
```

```
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Шаг 6. Задание внешнего IP-адреса

Настройка NAT

```
Router(config)# ip nat inside source static 172.31.232.14 209.165.202.130
Router(config)# exit
```

Шаг 7. Определение преобразования сетевых адресов для сервера

С помощью следующей команды укажите механизм преобразования:

```
Router(config)# ip nat inside source static 172.31.232.14 209.165.202.130
```

В данном примере внутренний адрес 172.31.232.14 сервера всегда преобразуется во внешний адрес 209.165.202.130. Используйте следующую команду для преобразования. После этого выйдите из режима глобальной конфигурации.

Настройка NAT

```
show running-config
```

Шаг 8. Проверка конфигурации

Проверьте конфигурацию статического NAT. Используйте следующую команду:

```
show running-config
```

Пример:

```
!
interface fastethernet 0/0
ip address 172.31.232.182 255.255.255.0
ip nat inside
!
interface serial 0/0
ip address 209.165.201.1 255.255.255.252
ip nat outside
ip nat inside source static 172.31.232.14 209.165.202.130
```

Сохраните текущую конфигурацию в файл начальной конфигурации.

Резервная копия файла начальной конфигурации

- Файлы конфигурации можно *сохранять* на сетевом сервере с использованием протокола TFTP:
  - Введите команду **copy startup-config tftp**.
  - Введите IP-адрес узла, где будет храниться файл конфигурации.
  - Введите имя файла конфигурации или оставьте имя по умолчанию.
  - Подтвердите командой "yes".
- Текущую копию текущей конфигурации также можно сохранить на сервере TFTP с помощью команды **copy running-config tftp**.
- Чтобы *восстановить* файл конфигурации из резервной копии, у маршрутизатора должен быть хотя бы один настроенный интерфейс, а сам он должен иметь возможность подключиться к серверу TFTP через сеть.
  - Введите команду copy tftp running-config.
  - Введите IP-адрес удаленного узла, где находится сервер TFTP.
  - Введите имя файла конфигурации или оставьте имя по умолчанию.
  - Подтвердите имя файла конфигурации и адрес tftp-сервера.

Автономные коммутаторы

- Каждый порт коммутатора может работать в режиме полного дуплекса или полудуплекса. В режиме полудуплекса он может либо получать, либо отправлять сообщения. В режиме полного дуплекса можно и отправлять, и принимать сообщения одновременно.

- Порт и подключенное устройство должны находиться в одинаковом режиме. В противном случае возникнет несовпадение, избыточное количество коллизий и ухудшение связи.

- Скорость и режим дуплекса порта можно настроить вручную или использовать автоматический выбор. Автоматический выбор производится в том случае, если порт автоматически определяет скорость и режим дуплекса подключенного устройства. У многих коммутаторов Cisco автоматический выбор включается по умолчанию. Для успеха процесса оба устройства должны его поддерживать.

Первоначальная настройка коммутатора

- Существует несколько вариантов настройки и управления коммутатором для ЛВС Cisco:
  - интерфейс командной строки Cisco IOS (CLI);
  - Cisco Network Assistant;
  - Cisco Device Manager;
  - программа управления CiscoView;
  - протокол Simple Network Management Protocol.

- В некоторых из этих вариантов для подключения к коммутатору используется IP или веб-обозреватель. Чтобы воспользоваться средством управления на базе IP или открыть сеанс Telnet для работы с коммутатором Cisco, нужно настроить IP-адрес коммутатора.

Первоначальная настройка коммутатора

- Чтобы работать с коммутатором через средства управления на базе IP или Telnet, нужно настроить IP-адрес.

- На коммутаторе заранее настроена одна виртуальная локальная сеть, VLAN 1, с помощью которой можно подключаться к средствам управления.

```
Switch> enable
    Switch# configure terminal
    Switch(config)# interface vlan 1
    Switch(config-if)# ip address 192.168.1.2 255.255.255.0
    Switch(config-if)#no shutdown
    Switch(config-if)#exit
    Switch(config)# ip default-gateway 192.168.1.1
    Switch(config)# end
    Switch#copy running-configuration startup-configuration
```

CDP

- *Протокол обнаружения Cisco (CDP)* - это средство сбора информации, используемое коммутатором, ISR или маршрутизатором для обмена данными о других непосредственно подключенных устройствах Cisco. CDP работает только на уровне 2.

- Два устройства Cisco, непосредственно подключенные и находящиеся в одной и той же локальной сети, называются *соседними*.

- CDP собирает следующие данные:
  - идентификатор устройства - настроечное имя узла;
  - список адресов - адрес уровня 3, при наличии;
  - идентификатор порта - непосредственно подключенный порт, например: serial 0/0/0;
  - список возможностей - функция или функции устройства;
  - платформа - аппаратная платформа устройства, например, Cisco 1841.

  Команды

  show cdp neighbors
  show cdp neighbors detail

  отображают информацию, полученную устройствами Cisco от непосредственно подключенных соседних устройств.

Сведения о соседних устройствах

```
R3#show cdp neighbors
Capability Codes: R - Router, T- Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Hose, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch           Fas 0/0            133         S I       WS-C2950-2Fas 0/11
R2               Ser 0/0/           149        R S I      Cisco 1841Ser 0/0/1
```

Подробные сведения о соседних устройствах

```
R3#show cdp neighbors detail
---------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial10/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK-9M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical support: http://www.cisco.com/techsupport
```

Отключение CDP

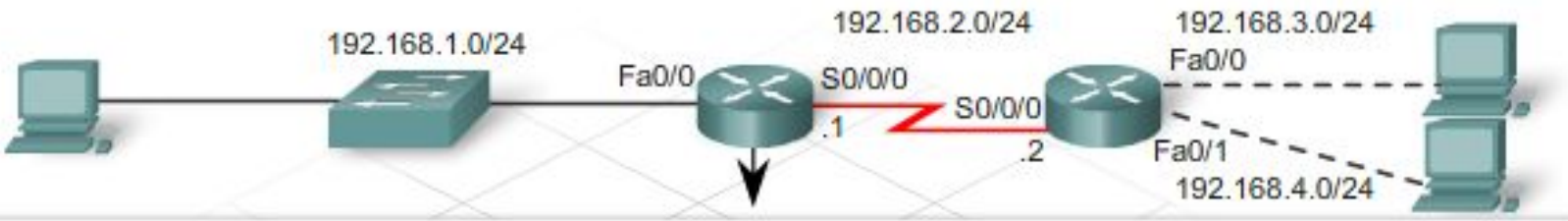
```
!To disable CDP globally use...
R3(config)#no cdp run
!
!or, to disable CDP on only an interface...
R3(config-if)#no cdp enable
```

Маршрутизация

- **Маршрутизация** – это способ направления сообщений по различным сетям, посредством которого устройства доставляют сообщения получателям.
- **Таблица маршрутизации -** это файл данных, который находится в ОЗУ и хранит сведения о подключенных напрямую и удаленных сетях. В таблице маршрутизации каждая сеть связана либо с выходным интерфейсом, либо со следующим переходом.
- **Выходной интерфейс -** это физический путь, который используется маршрутизатором для перемещения данных ближе к адресу назначения. **Следующий переход -** это интерфейс подключенного маршрутизатора, который перемещает данные ближе к адресу конечного назначения.

Маршрутизация

- Маршрут состоит из четырех основных *компонентов*:
  - значение получателя;
  - маска;
  - адрес шлюза или интерфейса;
  - стоимость маршрута или метрика маршрута.




```
R1#show ip route
Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R   192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:26, Serial0/0/0
C   192.168.1.0/24 is directly connected, FastEthernet0/0
C   192.168.2.0/24 is directly connected, Serial0/0/0
S   192.168.3.0/24 [1/0] via 192.168.2.2
```

Виды маршрутов

- **Прямые маршруты**

  После выхода настроенных интерфейсов в рабочий режим маршрутизатор будет хранить адреса непосредственно подключенных локальных сетей в виде прямых маршрутов в таблице маршрутизации (обозначаются префиксом **C**). Они автоматически обновляются при перенастройке или отключении маршрута.

- **Статические маршруты**

  Статические маршруты не изменяются до тех пор, пока администратор не перенастроит их вручную (обозначаются буквой **S**). У статических маршрутов *самое малое административное расстояние*.

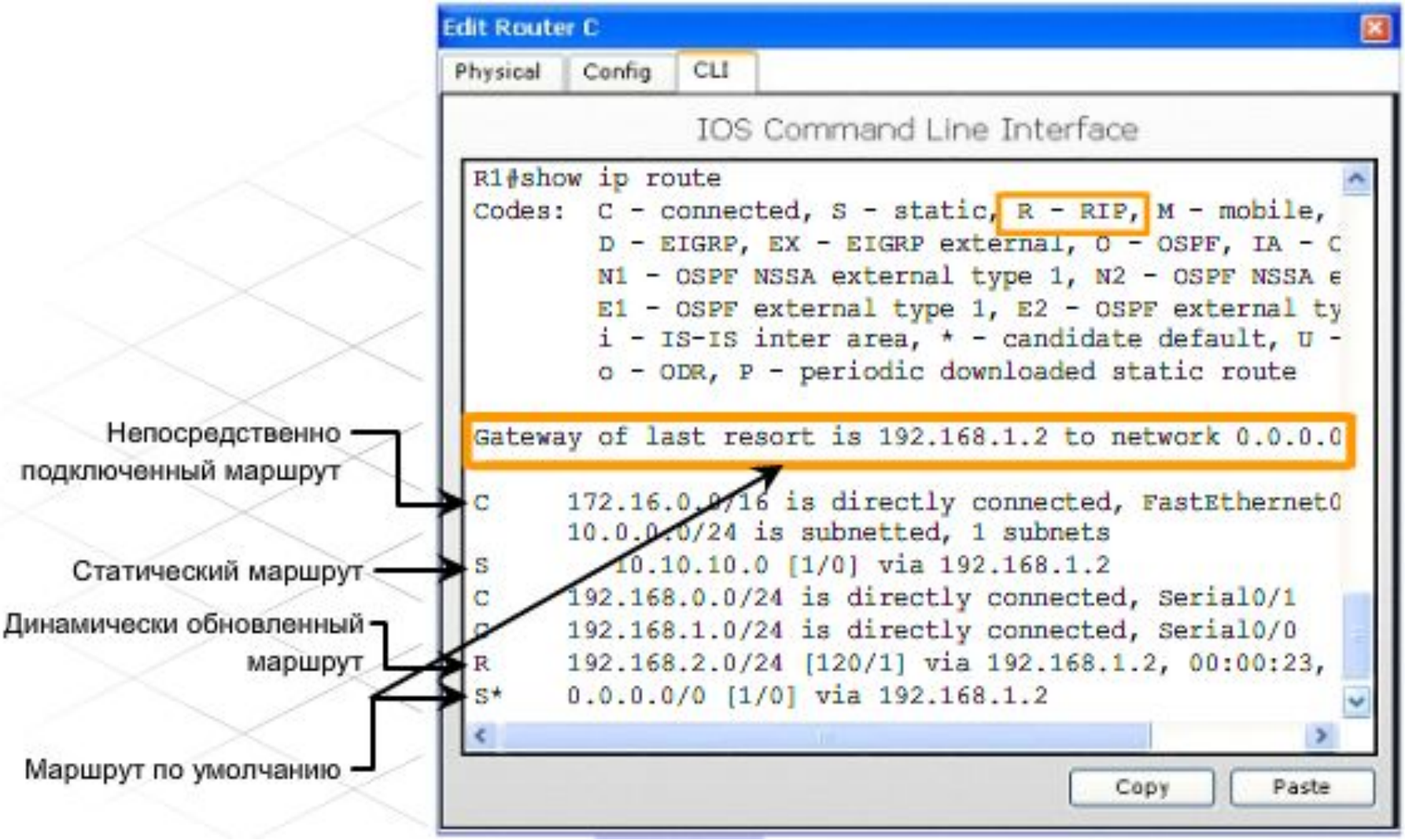
- **Динамические (динамически обновляемые) маршруты**

  Динамические маршруты автоматически создаются и обновляются протоколами маршрутизации (обозначаются приставкой, характеризующей тип протокола, создавшего маршрут. Например, **R** обозначает информационный протокол маршрутизации (**RIP**))

- **Маршрут по умолчанию**

  Для сетей, путь к которым отсутствует в таблице маршрутизации, используется шлюз, указанный в маршруте по умолчанию. Маршрут по умолчанию является *статическим* маршрутом.

Виды маршрутов



Настройка статического маршрута

- Подключитесь к маршрутизатору по консольному кабелю.
- Откройте окно "HyperTerminal", чтобы подключиться к первому из маршрутизаторов, которые требуется настроить.
- Войдите в привилегированный режим, набрав **enable** в приглашении **Router1>**.

  Router1>enable

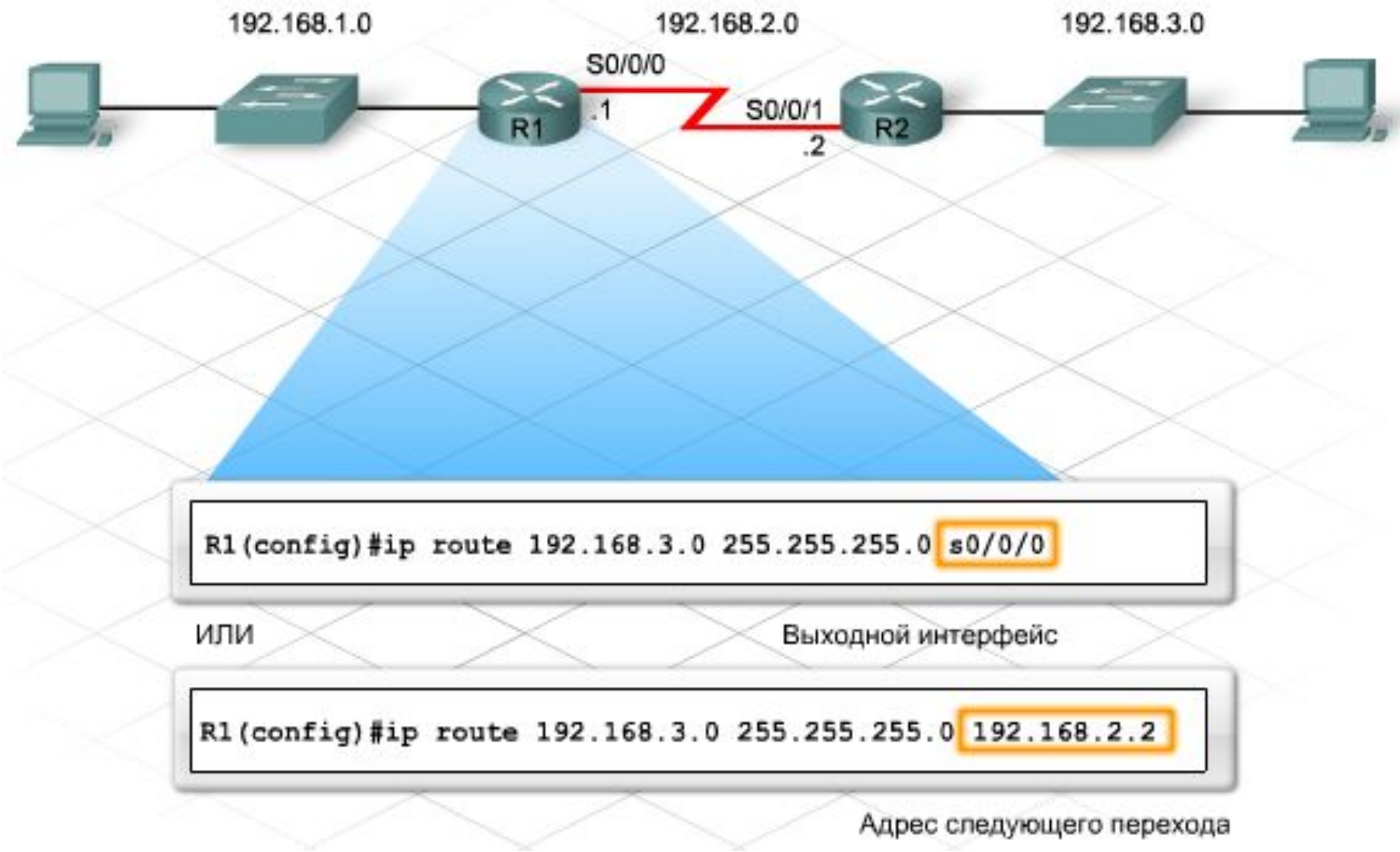
  Router1#
- Войдите в режим глобальной настройки.

  Router1#config terminal

  Router1(config)#
- Настройте статический маршрут, выполнив команду IOS **ip route** в следующем формате:

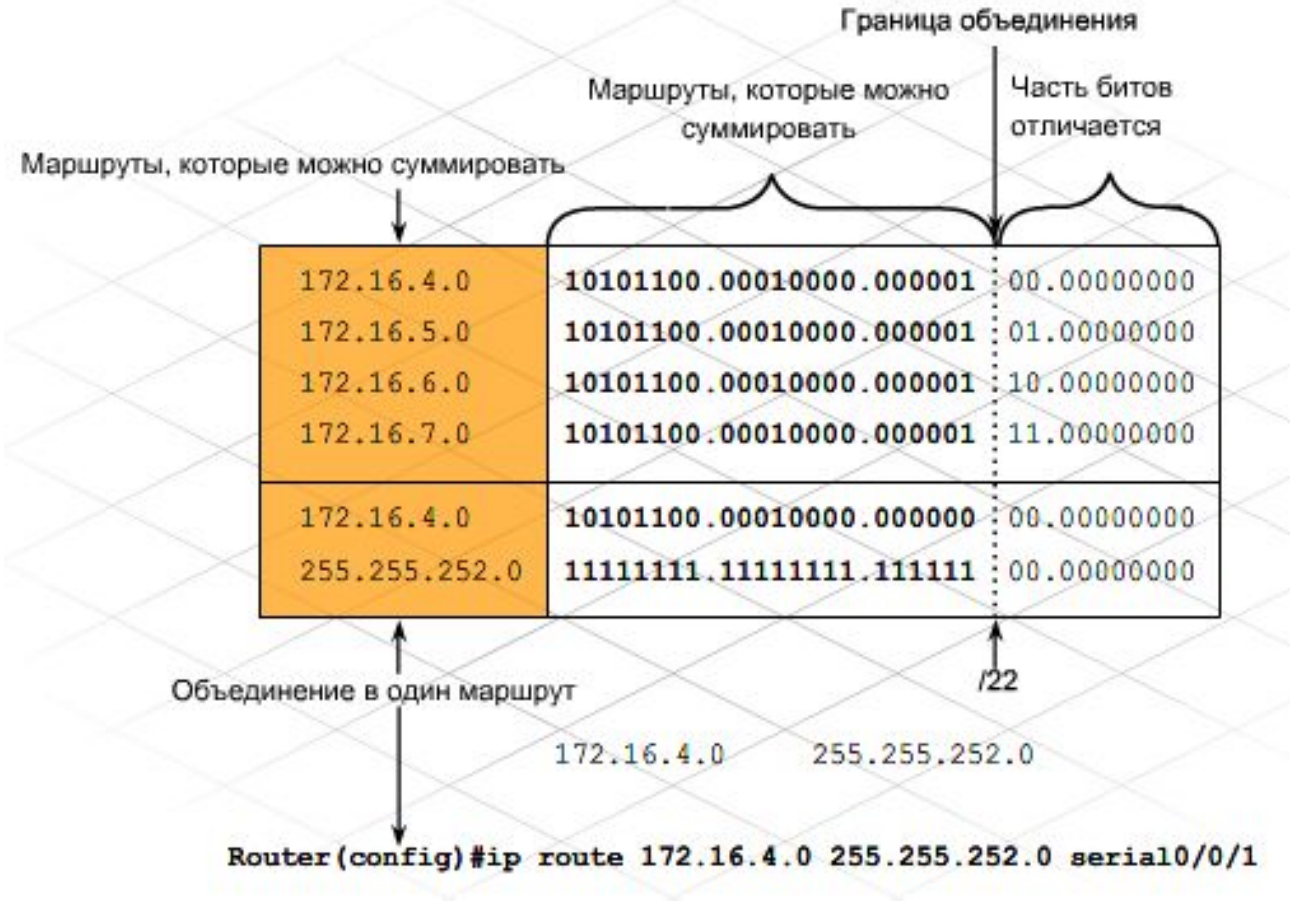
ip route [сеть_назначения] [маска_подсети] [адрес_шлюза]

Настройка статического маршрута



Суммирование маршрутов

- Один статический маршрут объединяет несколько статических маршрутов, если:
  - сети назначения объединены в единый сетевой адрес;
  - все статические маршруты используют один и тот же IP-адрес выходного интерфейса или следующего перехода.



«Плавающий» статический маршрут

- В зависимости от корпоративных служб WAN статические маршруты могут обеспечивать резервное копирование при отказе соединения основной WAN. В этом случае в целях резервного копирования используется функция *плавающих статических маршрутов*.
- По умолчанию административное расстояние статического маршрута меньше административного расстояния маршрута, полученного по протоколу динамической маршрутизации. Запись плавающего статического маршрута будет отображена в таблице маршрутизации, только если динамические сведения утеряны.
- Создание «плавающего» статического маршрута:

Router(config)#

ip route 192.168.4.0 255.255.255.0 192.168.9.1 200

Динамическая маршрутизация

- Для динамического управления информацией, поступающей с собственных интерфейсов и других маршрутизаторов, маршрутизаторы используют *протоколы маршрутизации*.

- Способ, которым протокол маршрутизации определяет наилучший маршрут к сети назначения, называется **алгоритмом маршрутизации**.

- **Алгоритмы маршрутизации** подразделяются на два класса: *вектор расстояния* и *состояние соединения*. Каждый из них предполагает использование различных методов для определения оптимального маршрута в сеть назначения.

- Состояние обновления всех маршрутизаторов в сети с учетом нового маршрута называется **схождением маршрутизаторов**.

Маршрутизация на основе векторов расстояния

- Алгоритм маршрутизации на основе вектора расстояния анализирует информацию, поступающую от других маршрутизаторов, в свете двух основных критериев:
  - расстояние – насколько удалена сеть от данного маршрутизатора;
  - вектор – в каком направлении следует пересылать пакеты для данной сети?

- Расстояние в маршруте представляется *стоимостью* или *метрикой*, которая может характеризовать один из следующих параметров:
  - число участков маршрута;
  - административные накладные расходы;
  - полоса пропускания;
  - скорость передачи;
  - вероятность задержек;
  - надежность.

- Компонент вектора или направления в маршруте представляет собой адрес следующего участка пути к сети, указанной в маршруте.

Протокол RIP

- Протокол маршрутной информации (RIP) – это протокол маршрутизации на основе векторов расстояния. Он нашел широкое применение в тысячах сетей по всему миру.
- Основные *характеристики* RIP:
  - изначально закреплен в документе RFC 1058;
  - реализован на основе вектора расстояния;
  - использует число участков маршрута в качестве метрики для выбора маршрута;
  - относит метрики выше 15 к недостижимым маршрутам;
  - по умолчанию рассылает содержимое таблицы маршрутизации каждые 30 секунд.
- RIP обладает *недостатками*:
  - допускается не более 15 участков маршрута, т.е. сеть может содержать не более 16 последовательно соединенных маршрутизаторов;
  - непосредственно подключенным соседним маршрутизаторам периодически рассылаются полные копии всей таблицы маршрутизации – в крупных сетях каждое обновление может сопровождаться значительным всплеском трафика;
  - длительное схождение после изменений в крупных сетях.

RIPv1 и RIPv2

- Протокол **RIPv1** не отправляет сведения о маске подсети в форме обновлений маршрутов, и поэтому не поддерживает **VLSM** и **CIDR**. Протокол **RIPv1** автоматически объединяет сети на классовой границе, трактуя все сети как классы по умолчанию A, B и C.
- **RIPv2** - *протокол бесклассовой маршрутизации*, который поддерживает **VLSM** и **CIDR**. Поле маски подсети включено в обновления версии 2. Протокол **RIPv2** дает возможность отключить автоматическое объединение маршрутов.
- **RIPv1** выполняет *широковещательную рассылку* своих обновлений для **255.255.255.255**.
- **RIPv2** выполняет *многоадресную рассылку* своих обновлений для **224.0.0.9**.
- Протокол **RIPv2** имеет механизм *аутентификации*, а **RIPv1** - нет.

Настройка RIP

- Перед настройкой RIP необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора. Затем можно перейти к настройке RIP.

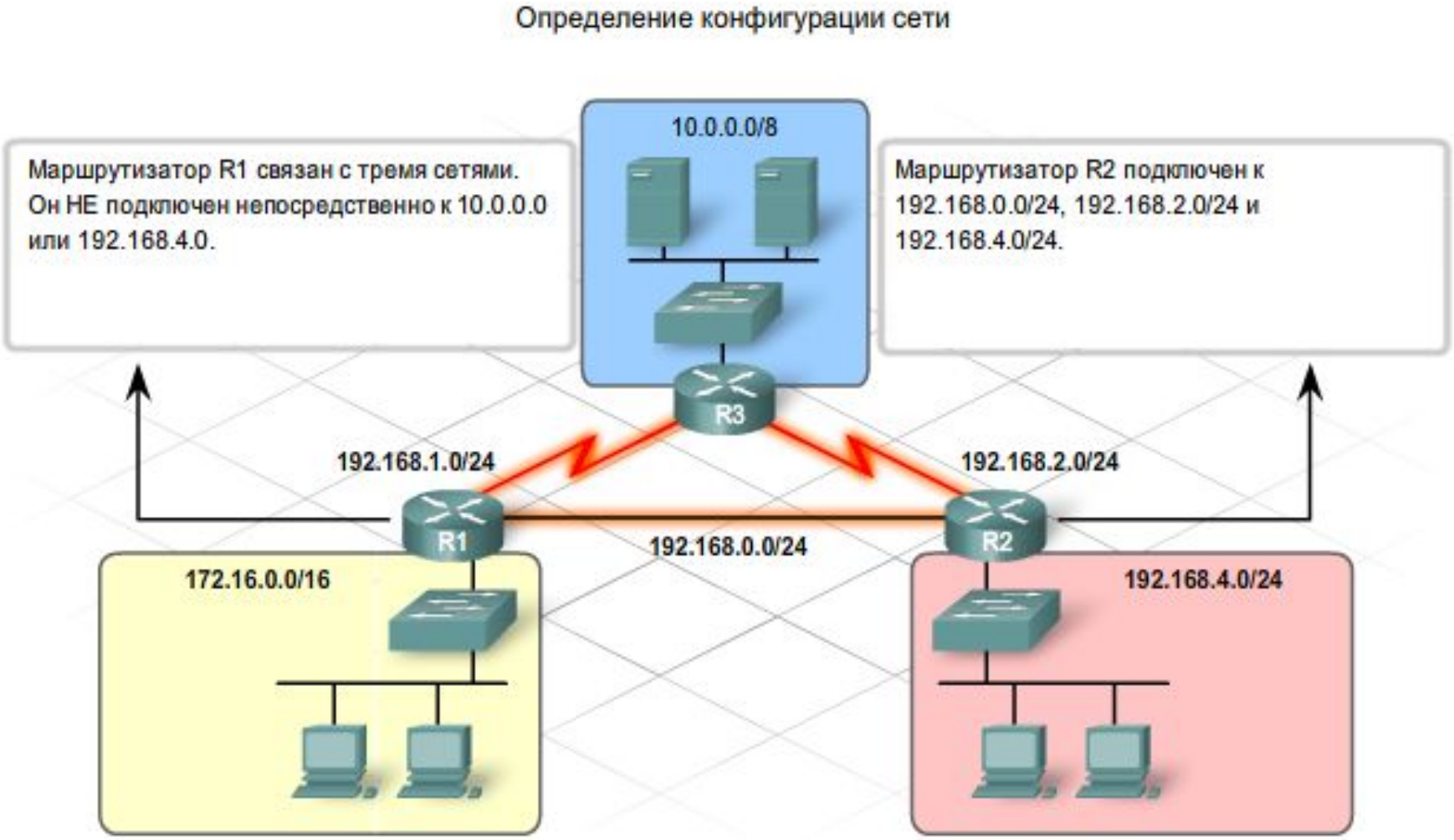
- Настройка RIP в самом базовом виде требует знания трех команд:

  Router(config)#router rip

  Router (config-router)#version 2

  Router(config-router)#network [номер-сети]

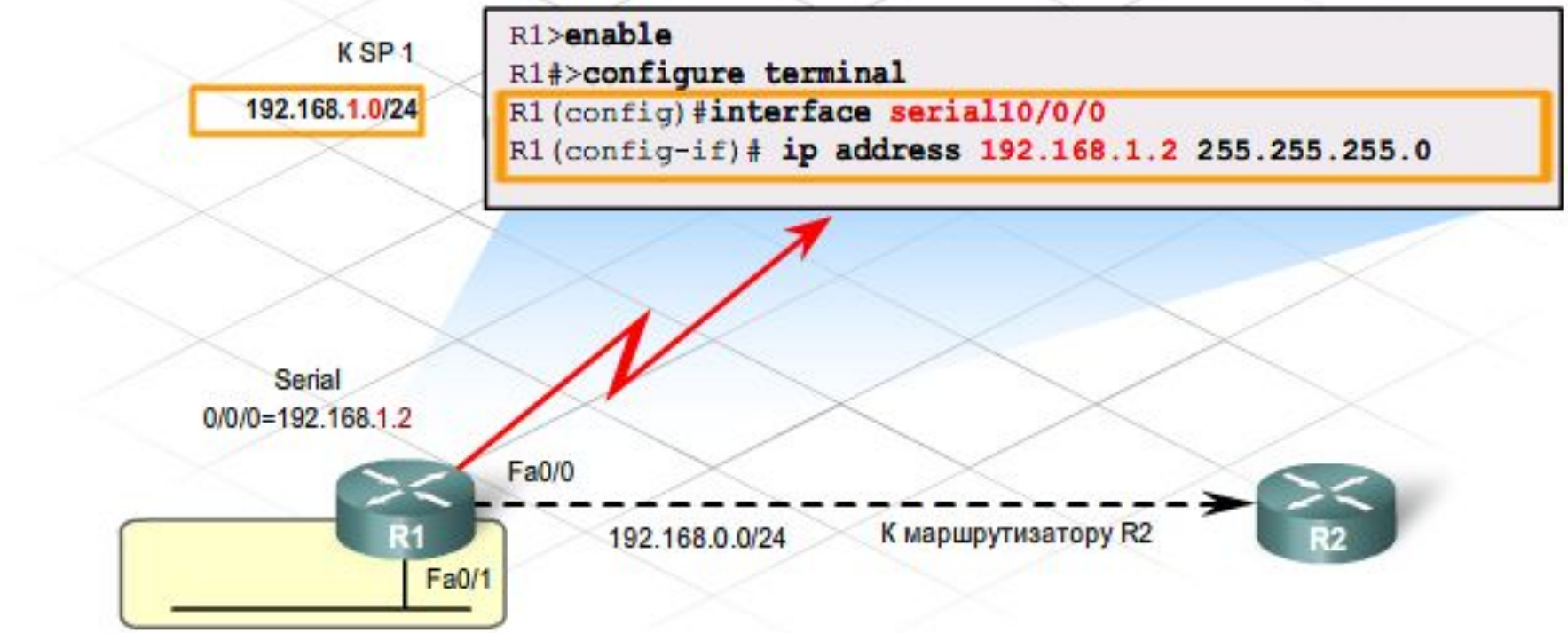
Настройка RIP



Настройка RIP

Настройка адреса последовательного интерфейса

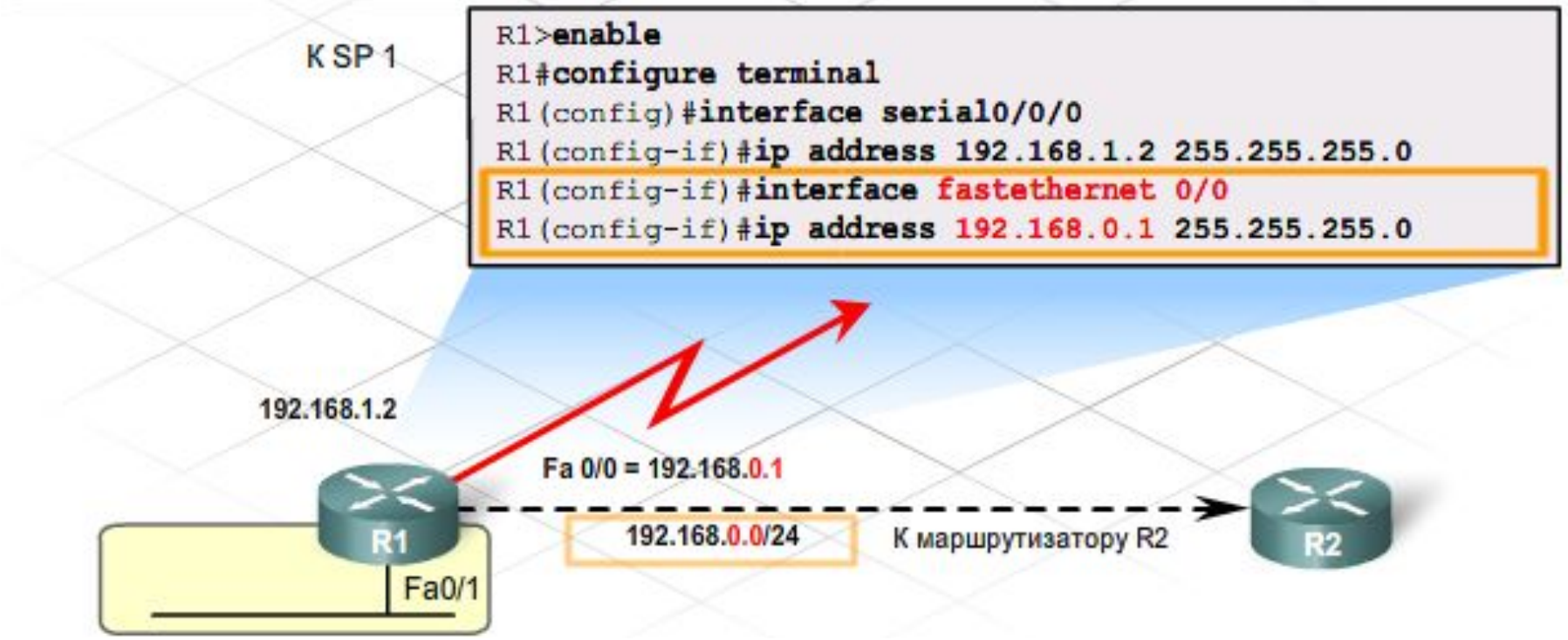
Для маршрутизатора R1 требуется настроить три интерфейса. Serial 0/0/0 подключен к маршрутизатору R3, Fastethernet 0/0 - к маршрутизатору R2 и Fastethernet 0/1 - к производственной сети 172.16.0.0/16. Вначале настройте Serial 0/0/0.



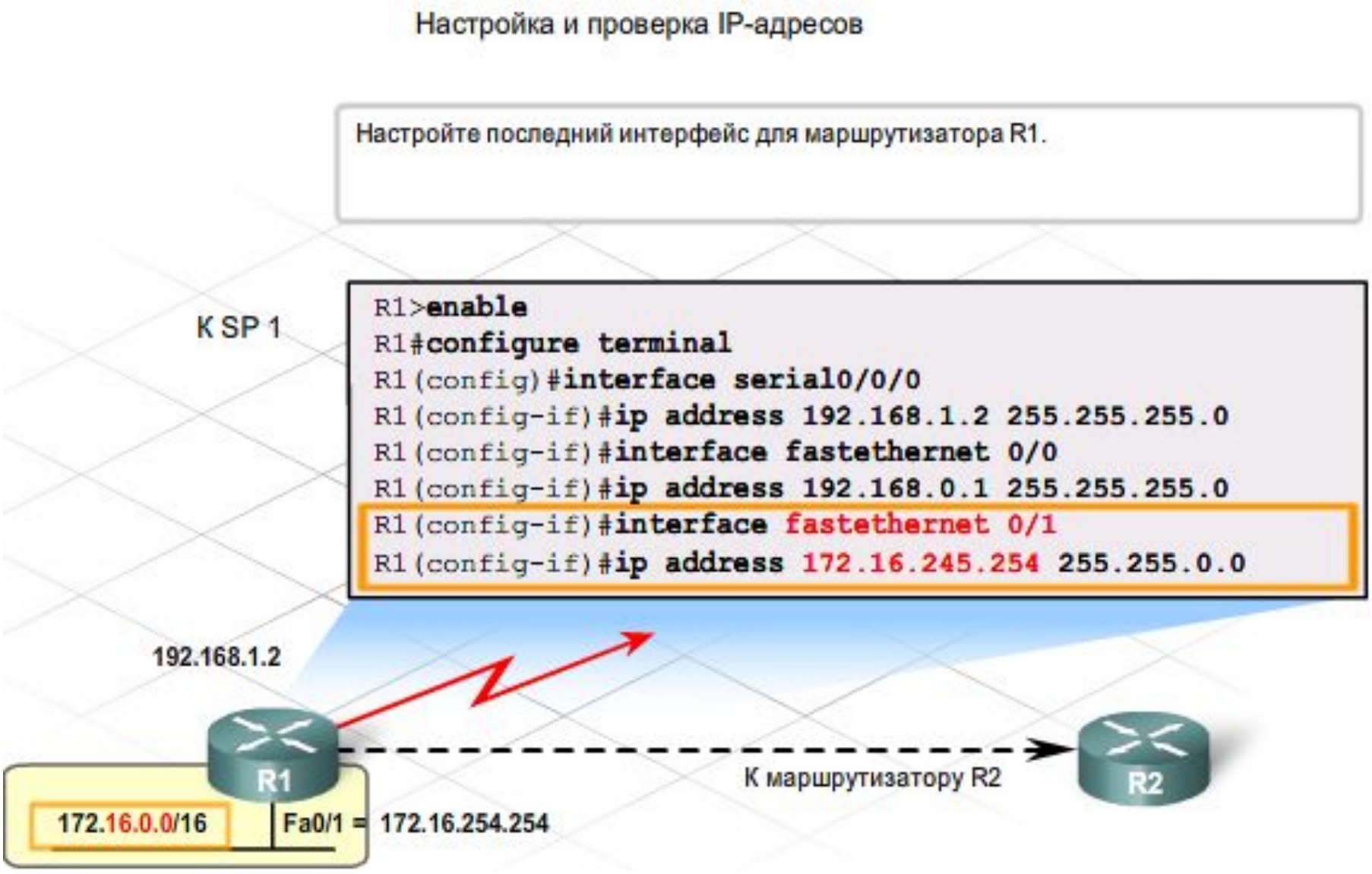
Настройка RIP

Настройка интерфейса Fast Ethernet

Для каждого из трех интерфейсов назначьте не использовавшийся до этого IP-адрес из сети, к которой подключен интерфейс. Fastethernet 0/0 указывает на маршрутизатор R2 и находится в сети 192.168.0.0/24. Назначьте для этого интерфейса первый используемый IP-адрес этой сети.



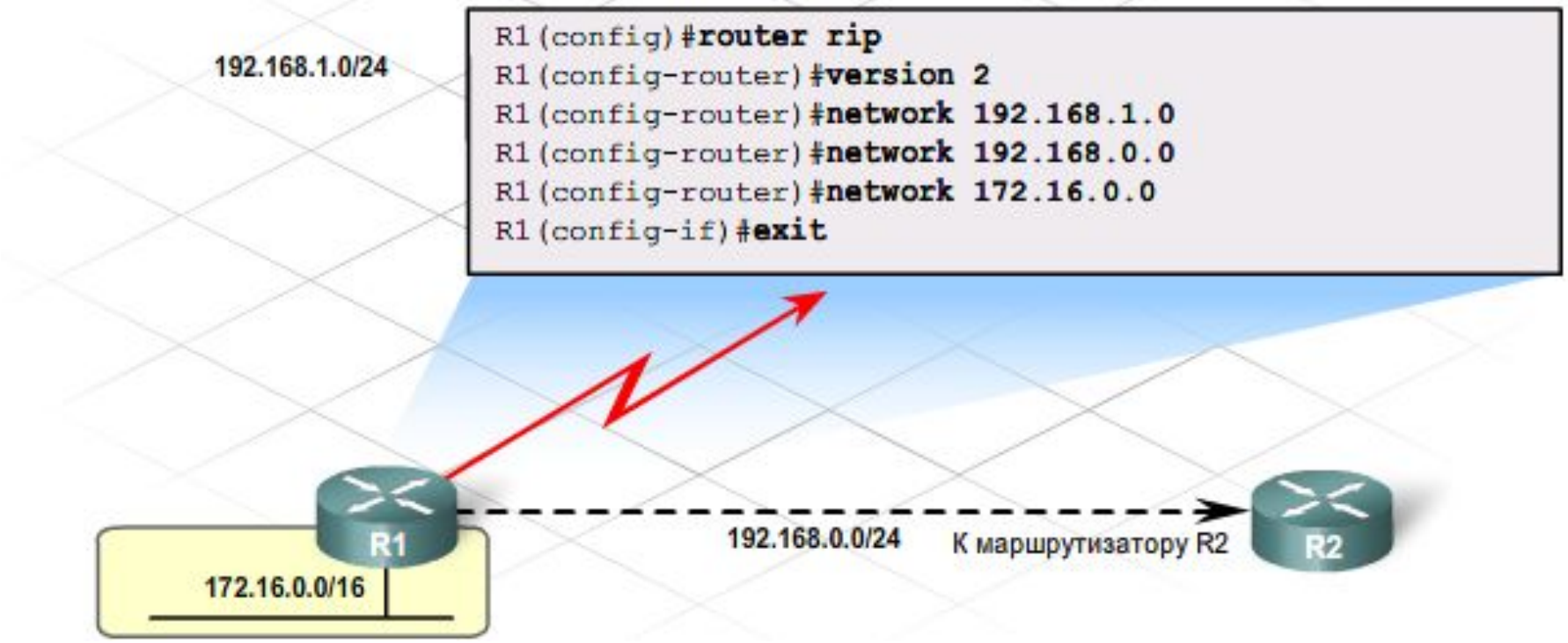
Настройка RIP



Настройка RIP

Настройка и проверка протокола RIP

Укажите версию 2 протокола RIP и передайте маршрутизатору информацию о сетях для оповещения. Для каждой непосредственно подключенной сети используйте команду network. Маршрутизатор R1 подключен к трем сетям, поэтому вход в эти сети производится здесь.



Настройка RIP

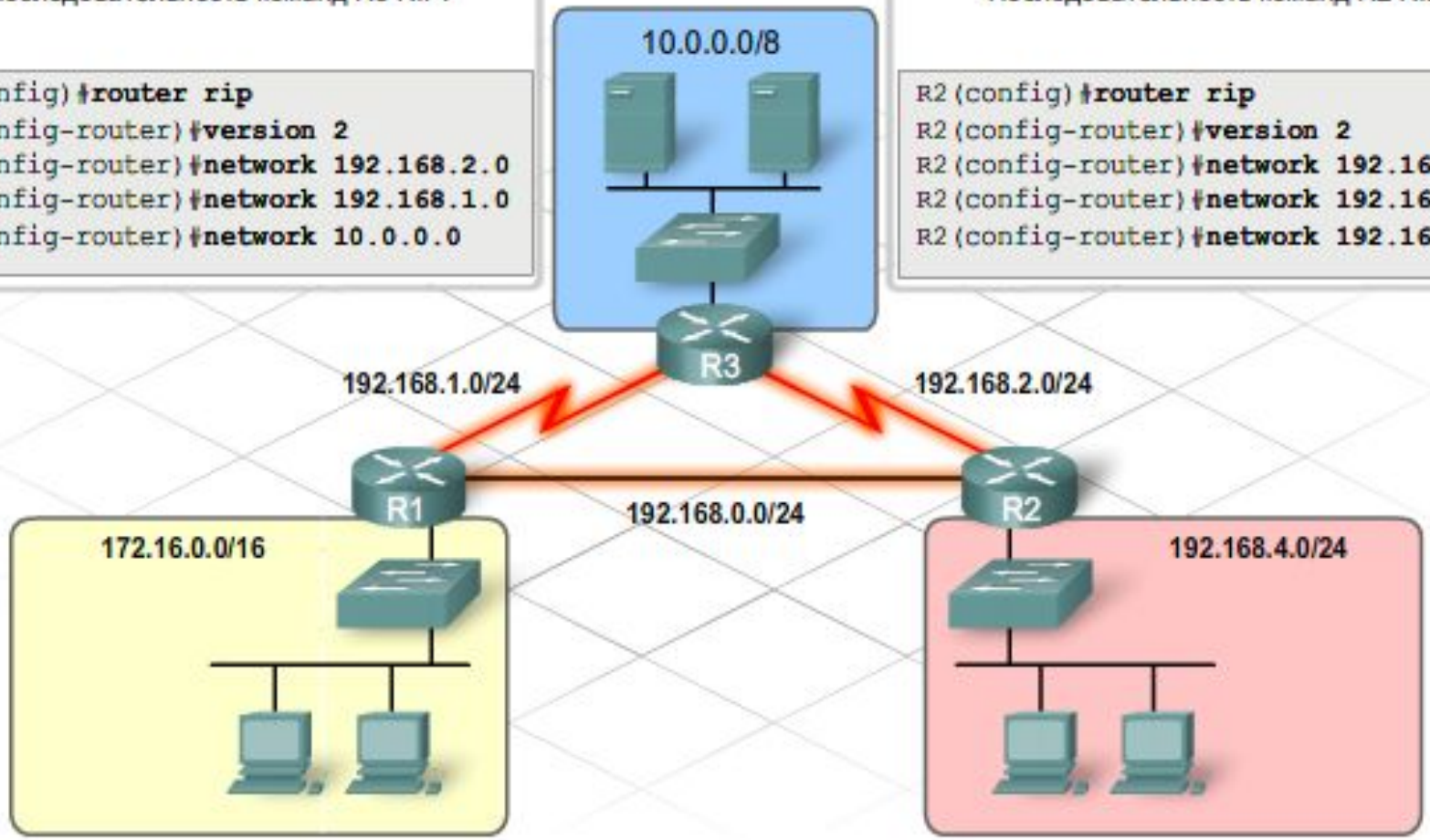
Завершение настройки всех маршрутизаторов

Последовательность команд R3 RIP:

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.1.0
R3(config-router)#network 10.0.0.0
```

Последовательность команд R2 RIP:

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.0.0
R2(config-router)#network 192.168.4.0
```



Дополнительные настройки

- Чтобы настроить аутентификацию MD5, перейдите к интерфейсу, используемому протоколом **RIPv2**, и введите команду

  ip rip authentication mode md5.

  Эта команда шифрует все обновления, отправляемые с этого интерфейса.

- Протокол **RIPv2** распространяет маршрут по умолчанию соседним маршрутизаторам вместе с обновлениями маршрутов. Для этого создайте маршрут по умолчанию и добавьте команду

  redistribute static

  в конфигурацию RIP.

Проверка работоспособности RIP

- Команда **ping**
- Команда **show ip protocols**
- Команда **show ip route**
- Команда **debug ip rip** позволяет проследить за извещениями о конкретных сетях в пересылаемых обновлениях маршрутов.

Проблемы протокола RIP

- Первая *проблема* - точности таблицы маршрутизации (возникает за счет автосуммирования).
- *Решение*: **Router(config-router)#no auto-summary**

- Другая *проблема* - широковещательный режим обновлений.
- *Решение:*

  Router(config-router)#

  passive-interface тип интерфейса номер интерфейса

- Ошибки в сведениях о сети могут вызвать в обновлениях маршрутов и трафике *петли*, которые ведут счет до бесконечности.

Проблемы протокола RIP

- *Петли маршрутизации* отрицательно сказываются на производительности сети. В протоколе RIP предусмотрено несколько функций для устранения этой проблемы:
  - обратный запрет;
  - разделение горизонта;
  - таймер удержания;
  - обновления при включении.

- *Обратный запрет* определяет для метрики маршрута значение 16, и он становится недостижим.

- *Разделение горизонта* требует, чтобы маршрутизатор, получающий сведения маршрутизации для интерфейса, не мог отправить обновление для той же сети из этого же интерфейса.

- *Таймер удержания* стабилизирует маршруты. Таймер удержания отказывается принимать обновления маршрутов с большей метрикой для той же сети назначения на период, когда маршрут становится неактивным. Если в течение времени удержания исходный маршрут снова становится активным или маршрутизатор получает сведения о маршруте с более низкой метрикой, маршрутизатор устанавливает маршрут в таблице маршрутизации и немедленно начинает им пользоваться. Время удержания по умолчанию равно 180 секундам, в шесть раз больше стандартного периода обновления.

Протокол EIGRP

- *Расширенный протокол маршрутизации внутреннего шлюза* (EIGRP) – это собственный усовершенствованный протокол маршрутизации Cisco с использованием вектора расстояния.
- *Основные характеристики EIGRP:*
  - расчет стоимости маршрута на основе нескольких метрик - двумя основными задачами протокола EIGRP являются обеспечение беспетлевой среды маршрутизации и быстрой конвергенции. Им используется составная метрика, которая, главным образом, основана на пропускной способности и задержке.
  - возможности протоколов на основе вектора расстояния, связанные со следующим участком и метрикой, объединены с дополнительными функциями баз данных и обновлений;
  - максимальное число участков маршрута – 224.

Протокол EIGRP

- В отличие от RIP, **EIGRP** не ограничивается использованием содержимого *таблицы маршрутизации маршрутизатора*. Для **EIGRP** создаются две дополнительные таблицы базы данных: *таблица соседних маршрутизаторов* и *таблица топологии*.

- В *таблице соседних маршрутизаторов* хранятся данные о соседних маршрутизаторах в локальных сетях, подключенных напрямую. Эта таблица содержит такую информацию, как IP-адрес, тип и полоса пропускания интерфейса.

- **EIGRP** формирует *таблицу топологии* на основе извещений от соседних маршрутизаторов. Таблица топологии содержит все маршруты, объявленные соседними маршрутизаторами.

Протокол EIGRP

- В *таблице топологии* определяются до четырех основных беспетлевых маршрутов к адресу назначения.

- *Резервные маршруты*, называемые *возможными преемниками*, отображаются в *таблице топологии*, но отсутствуют в таблице маршрутизации. Если не действует основной маршрут, лучшим маршрутом становится возможный преемник. Это замещение происходит при условии, что объявленное расстояние возможного преемника меньше допустимого расстояния текущего преемника до адреса назначения.

- Если в таблице топологии размещены сведения о множестве различных путей до сети назначения, то в *таблице маршрутизации* отображаются только оптимальные маршруты, называемые лучшими маршрутами.

Протокол EIGRP

- **EIGRP** выполняет *многоадресную рассылку частичных обновлений,* касающихся конкретных изменений, только тем маршрутизаторам, которым эти сведения необходимы, а не всем маршрутизаторам области. Адрес многоадресной рассылки **224.0.0.10**.

- Вместо отправки периодических обновлений маршрутов протокол **EIGRP** отсылает небольшие *пакеты приветствия* для обновления сведений о своих соседях.

- По умолчанию в каналах со скоростью больше T1 происходит многоадресная рассылка пакетов приветствия через каждые 5 секунд, а в каналах со скоростью T1 и меньше - через каждые 60 секунд.

- *Время удержания* - это период ожидания протоколом **EIGRP** пакета приветствия. Обычно время удержания в три раза больше интервала приветствия. По истечении времени удержания, когда **EIGRP** объявляет маршрут неактивным, алгоритм **DUAL** выполняет перерасчет топологии и обновляет таблицу маршрутизации.

Метрики и конвергенция протокола EIGRP

- Для определения лучшего маршрута до адреса назначения EIGRP использует составное значение метрики. Эта *метрика* определяется на основе следующих значений:
  - полоса пропускания;
  - задержка;
  - надежность;
  - нагрузка.

- **Пропускная способность -** метрика пропускной способности является статическим значением, отображаемым в Кбит/с. У большинства серийных интерфейсов значение пропускной способности по умолчанию равно 1544 Кбит/с.

- **Метрика задержки** - статическое значение на основе типа выходного интерфейса. Значение по умолчанию равно 20 000 микросекунд для серийных интерфейсов и 100 микросекунд для интерфейсов Fast Ethernet.

Метрики и конвергенция протокола EIGRP

- **Метрика надежности** означает частоту ошибок в канале. В отличие от задержки метрика надежности обновляется автоматически в зависимости от условий канала. Ее значение равно от 0 до 255. Надежность, равная 255/255, показывает канал со стопроцентной надежностью.

- **Нагрузка** отражает объем трафика в канале. Малое значение нагрузки предпочтительнее высокого. Например, значение 1/255 означает канал с минимальной нагрузкой, а 255/255 - канал, загруженный на 100%.

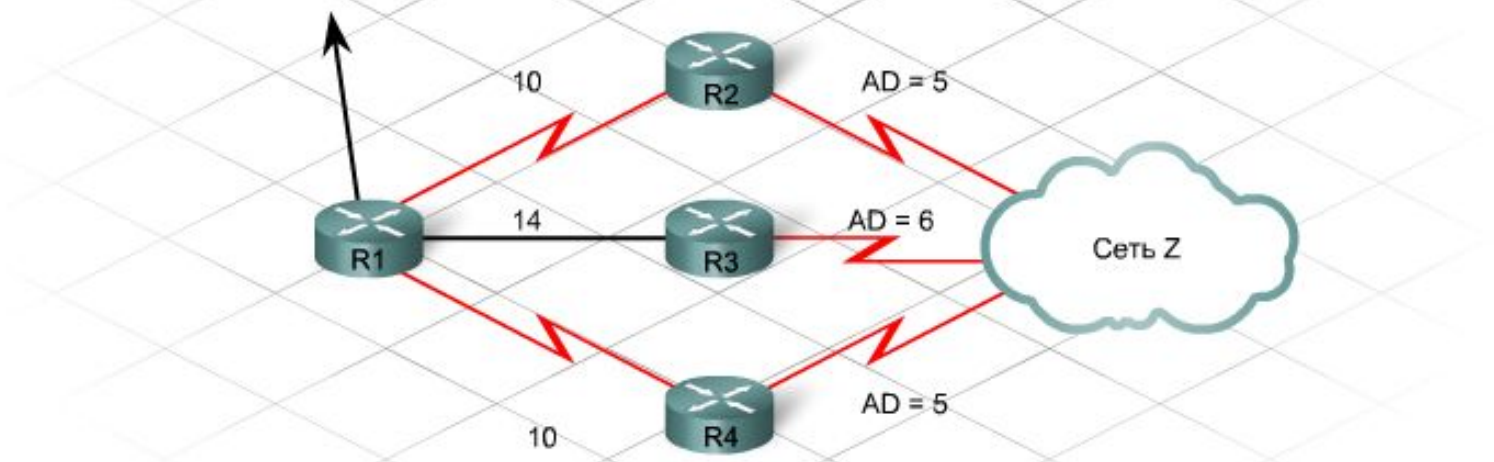
- В таблице топологии **EIGRP** используются метрики для расчета значений *возможного расстояния* (FD) и *заявленное расстояния* (AD) или *объявленного расстояния* (RD). Алгоритму **DUAL** эти значения необходимы для определения лучших путей и возможных преемников.

- *Возможное расстояние* - это лучшая метрика EIGRP по пути к адресу назначения от маршрутизатора.

- *Объявленное расстояние* - это лучшая метрика, полученная от соседа.

Метрики и конвергенция протокола EIGRP

Маршрутизатор R2 — это лучший маршрут к сети Z	FD = 15	AD = 5
Маршрутизатор R3 — это возможный преемник к сети Z	FD = 20	AD = 6
Маршрутизатор R4 — это лучший маршрут к сети Z	FD = 15	AD = 5



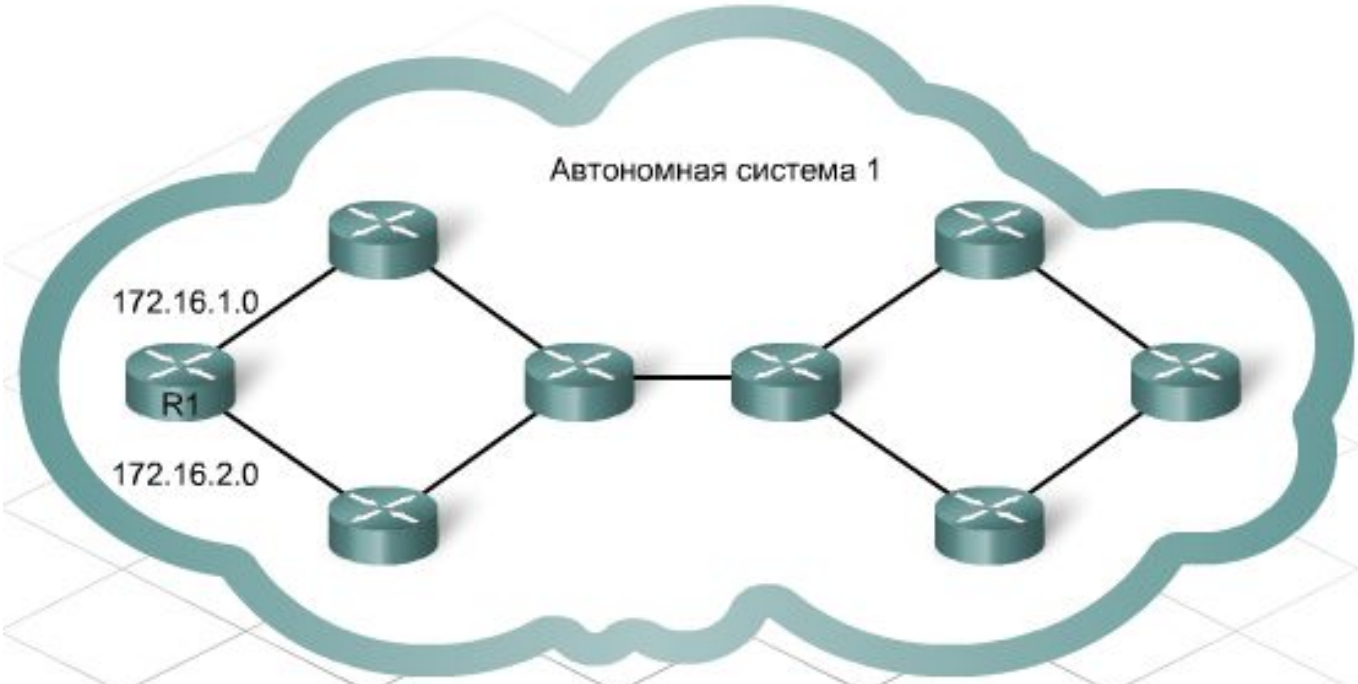
Возможное расстояние (FD):

Минимальное расстояние (метрика) пути от маршрутизатора к сети назначения.

Заявленное расстояние (AD) или объявленное расстояние (RD):

Расстояние (метрика) по направлению к пункту назначения, объявленное вышестоящим соседним устройством. *Расстояние соседнего маршрутизатора*

Настройка EIGRP



Шаг 1

```
R1(config)#router eigrp ?
   <1-65535>   Autonomous system number
R1(config)#router eigrp 1
```

Шаг 2

```
R1(config-router)#network 172.16.0.0
```

Настройка EIGRP

- Чтобы настроить EIGRP для передачи сведений только о некоторых подсетях, вставьте *групповую маску* после номера сети. Чтобы определить групповую маску, вычтите маску подсети из 255.255.255.255.

- Добавьте команду **eigrp log-neighbor-changes** для просмотра изменений в смежностях соседей.

- Для последовательных каналов, которые не соответствуют пропускной способности **EIGRP** в 1,544 Мбит/с, следует добавить команду **bandwidth** с указанием после фактической скорости канала (в Кбит/с).

Аутентификация EIGRP

- Для *аутентификации* EIGRP требуется предварительный ключ. Протокол EIGRP позволяет администраторам управлять ключами через цепочку ключей. Настройка аутентификации EIGRP состоит из двух шагов: создание ключа и включение аутентификации с его использованием.
- Чтобы создать ключ, выполните следующие команды.

  key chain имя_цепочки

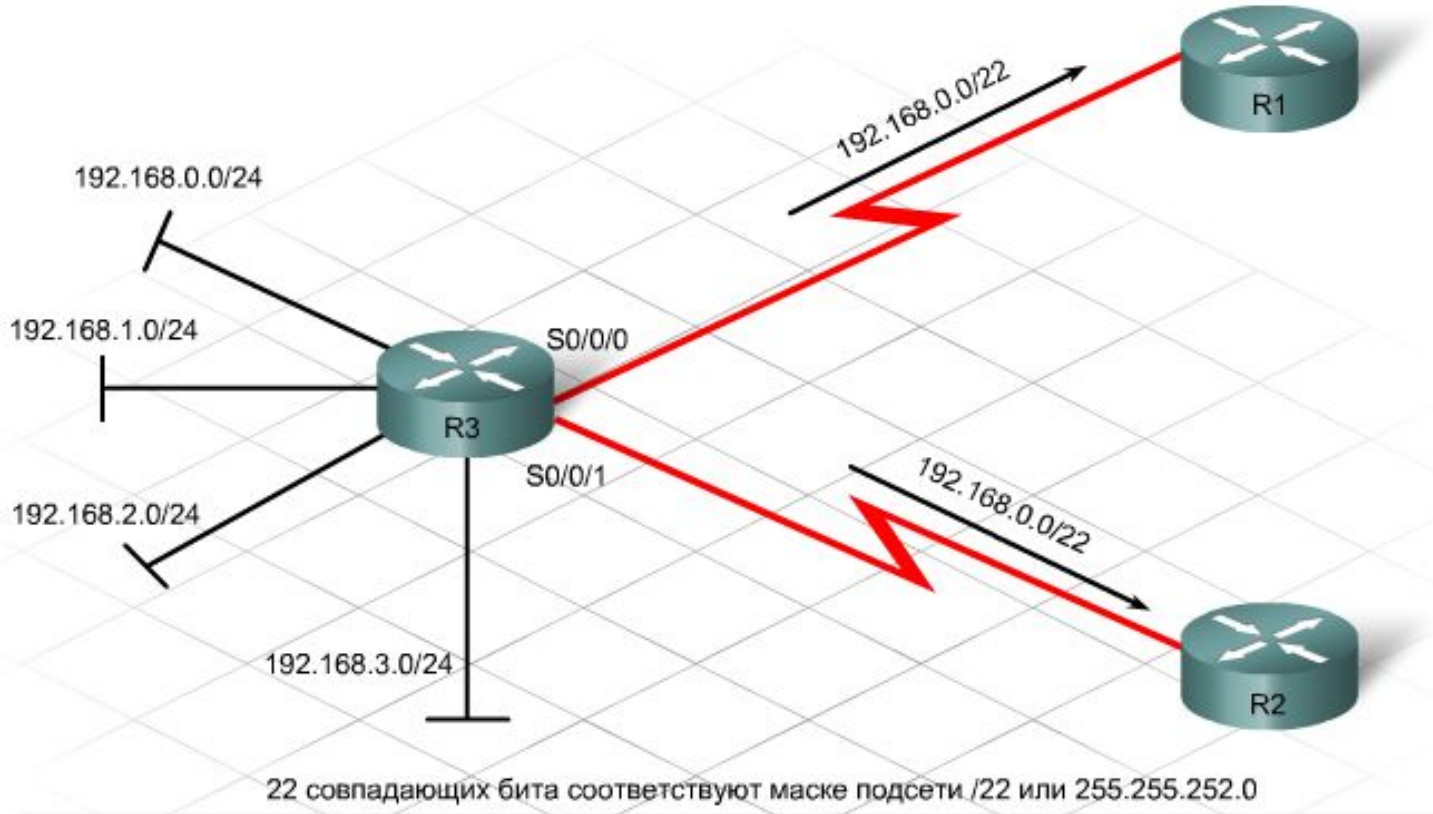
  key идентификатор ключа

  key-string текст
- Ключ служит для включения аутентификации MD5 для EIGRP с помощью следующих команд настройки интерфейса:

  ip authentication mode eigrp md5

  ip authentication key-chain eigrp имя_цепочки AS

Объединение маршрутов



22 совпадающих бита соответствуют маске подсети /22 или 255.255.252.0

```
R3(config)#interface serial 0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

Проверка работы протокола

- **show ip protocols** - позволяет удостовериться, что EIGRP передает сведения о верных сетях. Отображает номер автономной системы и административное расстояние.
- **show ip route** - проверяет наличие полученных маршрутов EIGRP в таблице маршрутизации. Отображает лучшие маршруты и всех возможных преемников. Отображает возможное и объявленное расстояние
- **show ip eigrp neighbors details** - проверяет формы смежностей EIGRP. Отображает IP-адреса и интерфейсы соседних маршрутизаторов
- **show ip eigrp traffic** - отображает количество и типы отправляемых и получаемых пакетов EIGRP
- **debug eigrp packet** - отображает передачу и получение всех пакетов EIGRP.
- **debug eigrp fsm** - отображает активность возможного преемника, чтобы определить состояние маршрутов (обнаружены, установлены или удалены протоколом EIGRP).

Проблемы и ограничения протокола

- не работает в средах различных поставщиков, поскольку является собственным протоколом компании Cisco;
- оптимальнее всего функционирует в сетях плоского типа;
- у маршрутизаторов должна совпадать автономная система, и его невозможно разделить на группы;
- может создавать очень большие таблицы маршрутизации, которые требуют больших пакетов обновлений и пропускной способности;
- использует больший объем памяти и вычислительных ресурсов по сравнению с протоколом RIP;
- работает эффективно, если не изменять параметры по умолчанию;
- для его обслуживания необходимы администраторы с глубокими техническими знаниями протокола и сети.

Протокол OSPF

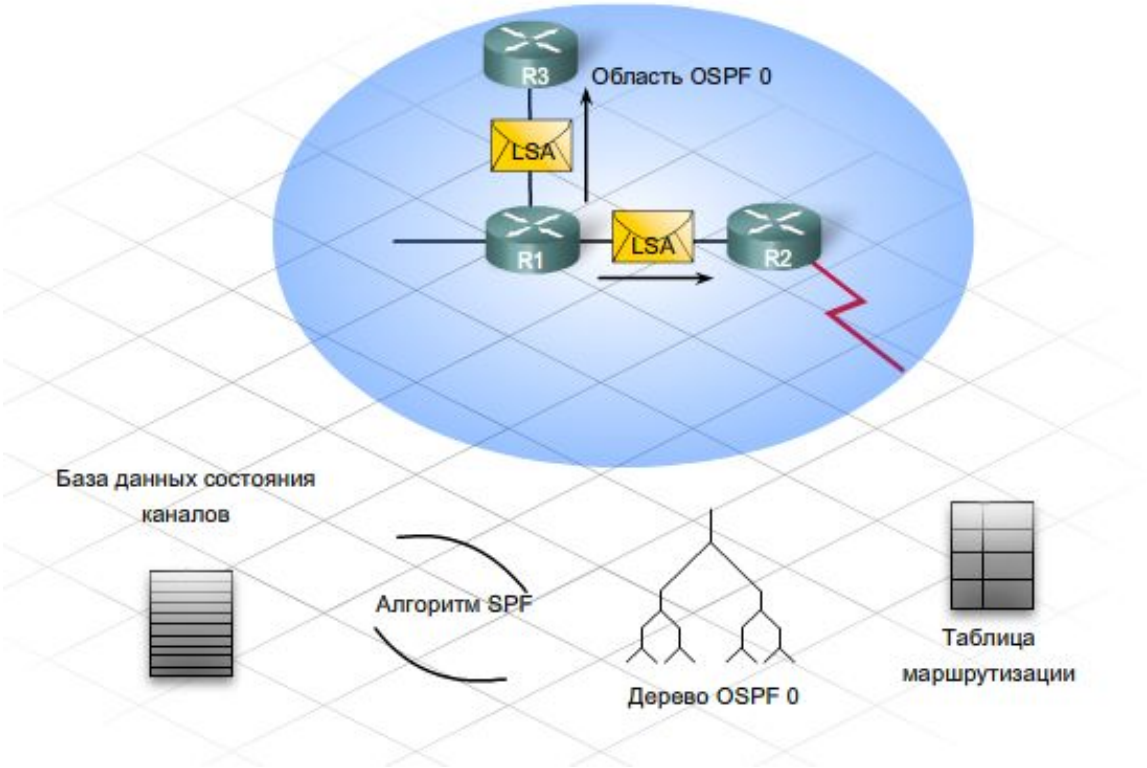
- Алгоритм маршрутизации, основанный на *состоянии канала*, ведет полную базу данных об удаленных маршрутизаторах и схеме их соединений.
- В маршрутизации на основе *состояния канала* присутствуют следующие *атрибуты*:
  - таблица маршрутизации – список известных маршрутов и интерфейсов;
  - объявление о состоянии канала (LSA) – компактный пакет для обмена сведениями о маршрутизации между маршрутизаторами. LSA описывает состояние интерфейсов (каналов связи) маршрутизатора и содержит другие сведения, например IP-адрес каждого канала;
  - топологическая база данных – концентрирует информацию, извлеченную маршрутизатором из всех LSA;
  - алгоритм SPF (первоочередное определение кратчайших маршрутов) – расчет дерева SPF на основании информации из базы данных. Дерево SPF представляет собой карту сети с точки зрения конкретного маршрутизатора. Содержимое этого дерева используется при построении таблицы маршрутизации.

Протокол OSPF

- Протокол **OSPF** - это открытый стандарт протокол маршрутизации, разработанный Инженерной группа по развитию Интернета (IETF) для поддержки IP-трафика.
- Его основными характеристиками являются:
  - использование алгоритма SPF для расчета пути к месту назначения с наименьшей стоимостью;
  - рассылка обновлений маршрутов только при изменении топологии; периодическая рассылка полной таблицы маршрутизации не производится;
  - ускоренная сходимость;
  - поддержка VLSM и изолированных подсетей;
  - аутентификация маршрутов.

Протокол OSPF

- Маршрутизаторы, на которых выполняются протоколы OSPF, создают полную карту сети со своей точки обзора.
- Протокол OSPF не выполняет автоматического суммирования на границах главной сети.
- В решениях по протоколам OSPF, предлагаемых компанией Cisco, для определения стоимости канала используется пропускная способность. Эта метрика стоимости используется протоколом OSPF для определения наилучшего маршрута.



Протокол OSPF

- Конвергенция достигается, если все маршрутизаторы выполнят следующие действия:
  - получат информацию о каждом месте назначения в сети;
  - обработают данную информацию с использованием алгоритма SPF;
  - обновят свои таблицы маршрутизации.

- Маршрутизаторы OSPF устанавливают и поддерживают соседские отношения, или отношения смежности, с другими маршрутизаторами OSPF, подключенными к сети. *Смежность* - это продвинутая форма соседских отношений между маршрутизаторами, желающими обмениваться информацией о маршрутизации. При инициации маршрутизаторами отношения смежности с соседними маршрутизаторами начинается обмен обновлениями информации о состоянии каналов. Маршрутизаторы достигают состояния смежности FULL (полное), когда они имеют синхронизированные данные в своей базе данных состояний каналов.

- Перед тем как стать полностью смежным с соседним маршрутизатором, тот или иной маршрутизатор проходит через несколько изменений состояния.
  - Init (инициация);
  - 2-Way (двусторонний режим);
  - Exstart;
  - Exchange (обмен информацией);
  - Loading (загрузка);
  - Full (полное);

- Протокол приветствия посылает очень маленькие пакеты приветствия к подключенным напрямую маршрутизаторам OSPF на адрес многоадресной рассылки **224.0.0.5**. Пакеты посылаются каждые 10 секунд по каналам Ethernet и широковещательным каналам и каждые 30 секунд по нешироковещательным каналам.

Протокол OSPF

- В широковещательном окружении маршрутизатор достигнет состояния full только с **назначенным маршрутизатором (DR)** и **резервным назначенным маршрутизатором (BDR)**. Все прочие соседние маршрутизаторы будут отображаться в состоянии 2-way.

- В широковещательных сегментах сети есть только по одному маршрутизатору DR и BDR. Все прочие маршрутизаторы должны иметь соединение с маршрутизатором DR и BDR. При отказе какого-либо канала маршрутизатор, имеющий информацию о данном канале, посылает информацию на маршрутизатор DR, используя адрес многоадресной рассылки **224.0.0.6**. Маршрутизатор DR отвечает за рассылку информации об изменении на все остальные маршрутизаторы OSPF по адресу многоадресной рассылки **224.0.0.5**.

- Маршрутизатором DR назначается маршрутизатор *с самым высоким* в пределах локальной сети идентификатором маршрутизатора. Маршрутизатором BDR назначается маршрутизатор со вторым по величине идентификатором.

Протокол OSPF

- **Идентификатором** маршрутизатора является какой-либо IP-адрес, который определяется следующим:
  - Значением, настроенным с использованием команды **router-id**.
  - Если при помощи команды **router-id** не установлено никакого значения, то высшим **IP**-адресом, настроенным в петлевом интерфейсе.
  - Если отсутствует какой-либо настроенный петлевой интерфейс, то высшим **IP**-адресом в любом активном физическом интерфейсе.

- Идентификатор маршрутизатора можно просматривать при помощи следующих принадлежащих группе show команд: **show ip protocols, show ip ospf** или **show ip ospf interface**.

- Администратор может принудительно назначить маршрутизаторы DR и BDR путем настройки приоритета с использованием команды настройки интерфейса:

  ip ospf priority номер.

Области OSPF

- Все сети OSPF начинаются с области 0, также называемой *областью магистрали*. По мере расширения сети могут создаваться другие области, смежные с областью 0. Этим другим областям может назначаться любой номер до 65535. Максимально допустимое число маршрутизаторов в одной области составляет 50.

- Сеть OSPF имеет двухслойную иерархическую конструкцию. Область 0, также называемая *областью магистрали*, находится наверху, а все прочие области расположены на следующем уровне. Все немагистральные области должны напрямую соединяться с областью 0. Эта группа областей создает автономную систему OSPF (AS).

- Маршрутизатор, через который какая-либо область соединяется с областью магистрали, называется *пограничным маршрутизатором области* (ABR). Маршрутизатор, через который какая-либо область соединяется с другим протоколом маршрутизации, таким как EIGRP, или статические маршруты перераспределяются в область OSPF, называется *пограничным маршрутизатором автономной системы* (ASBR).

Настройка протокола OSPF в одной области

- **Шаг 1.** Выполните команду OSPF

  router(config)#router ospf <id процесса>

  Идентификатор процесса выбирается администратором, он может представлять собой любое число в диапазоне от 1 до 65535.

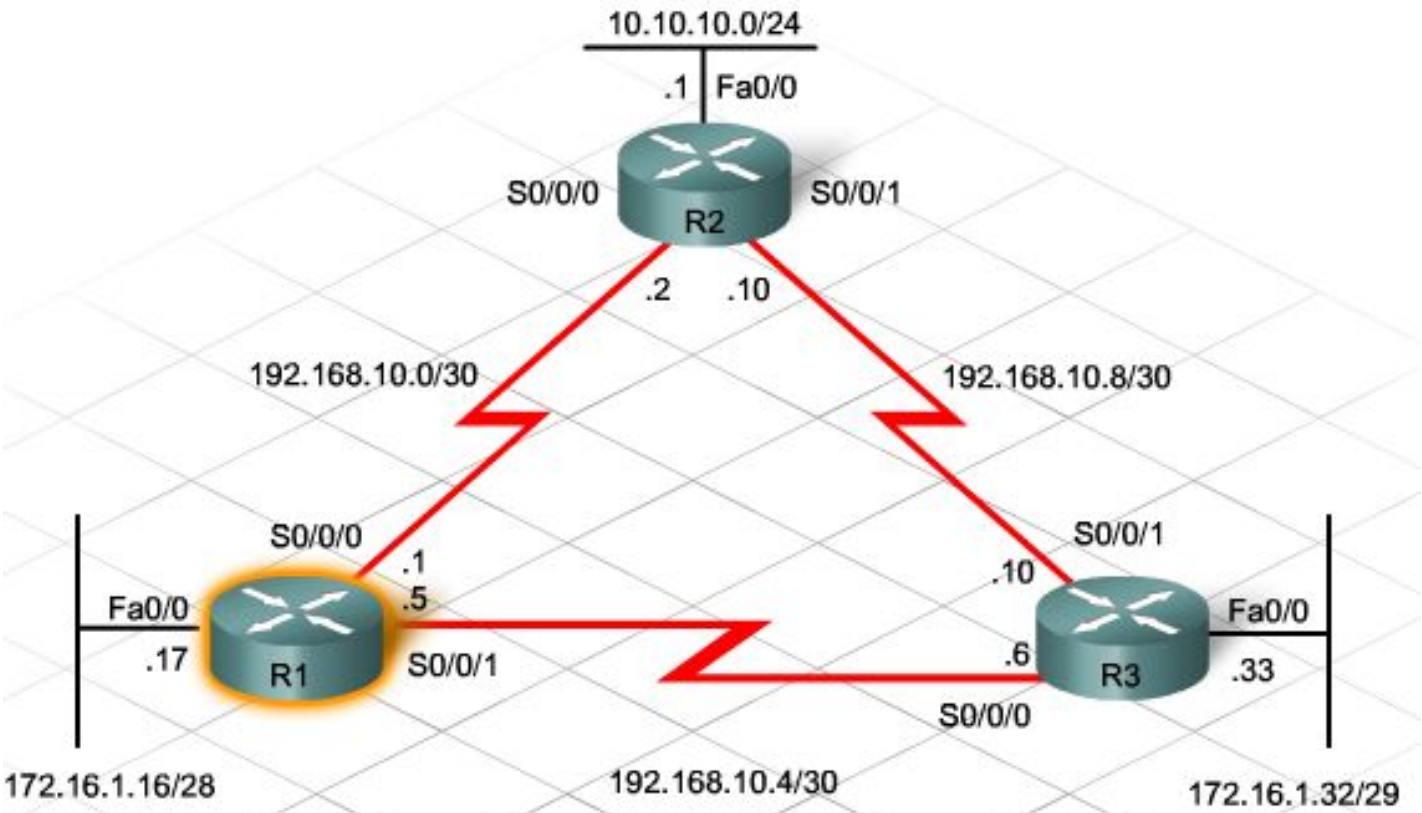
- **Шаг 2.** Объявите сети

  Router(config-router)#

  network <адрес сети> <групповая маска>

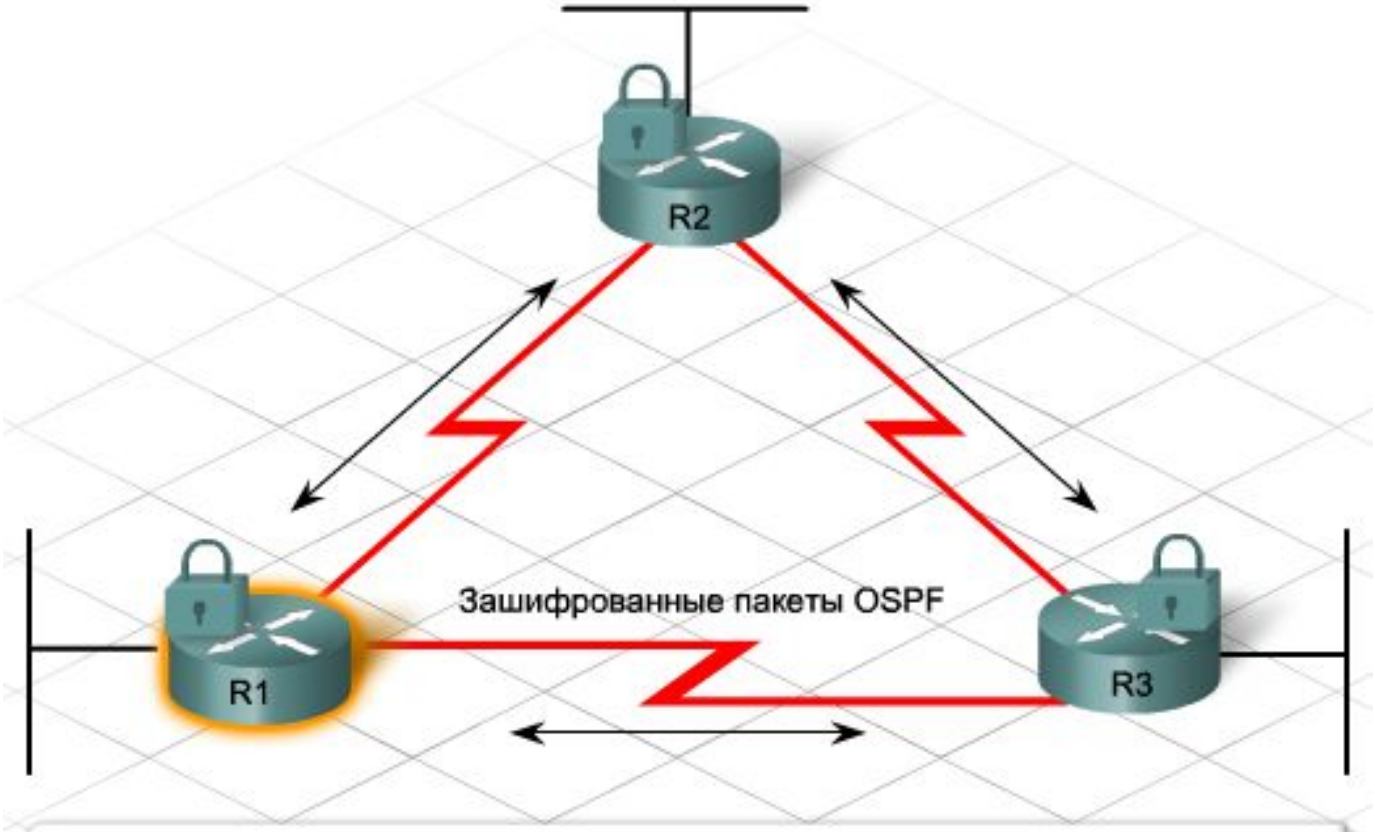
  область <id области>

Настройка протокола OSPF в одной области




```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

Настройка аутентификации OSPF




```
R1(config)#router ospf 18
R1(config-router)#network 10.0.0.0  0.0.0.255 area 0
R1(config-router)#area 0 authentication message-digest
R1(config)#interface serial0/0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#ip ospf message-digest-key 10 md5 areapassword
```

Настройка параметров протокола

- Маршрутизатор выбирает *назначенный маршрутизатор* на основании высшего значения любого из следующих параметров, в такой последовательности:
  - Приоритет интерфейса. Приоритет интерфейса устанавливается командой **priority**.
  - Идентификатор маршрутизатора. Идентификатор маршрутизатора устанавливается командой **OSPF router-idconfiguration**.
  - Высший адрес петлевого интерфейса. По умолчанию в качестве идентификатора маршрутизатора используется петлевой интерфейс с высшим IP-адресом. Протокол OSPF поддерживает петлевые интерфейсы, поскольку они являются не физическими, а логическими. Логические интерфейсы всегда имеют приоритет.
  - Высший адрес физического интерфейса. В качестве идентификатора маршрутизатора маршрутизатор использует высший активный IP-адрес одного из своих интерфейсов. Эта возможность вызывает проблему, если интерфейсы прекращают работу или перенастраиваются.
- После изменения идентификатора маршрутизатора или приоритета интерфейса необходимо сбросить значения отношений смежности соседних маршрутизаторов. Используйте команду **clear ip ospf process**. Этой командой вводятся в действие новые значения.

Настройка параметров протокола

- Еще одним параметром, требующим изменения, является *пропускная способность*.

- В протоколе OSPF при настройке с использованием команды **bandwidth interface** или **ip ospf cost interface** достигается одинаковый результат. При помощи обеих команд указывается точное значение, используемое OSPF для определения оптимального пути.

- Командой **bandwidth** изменяется значение пропускной способности, используемое для расчета метрики стоимости протокола OSPF. Чтобы напрямую изменить стоимость интерфейса, используйте команду **ip ospf cost**.

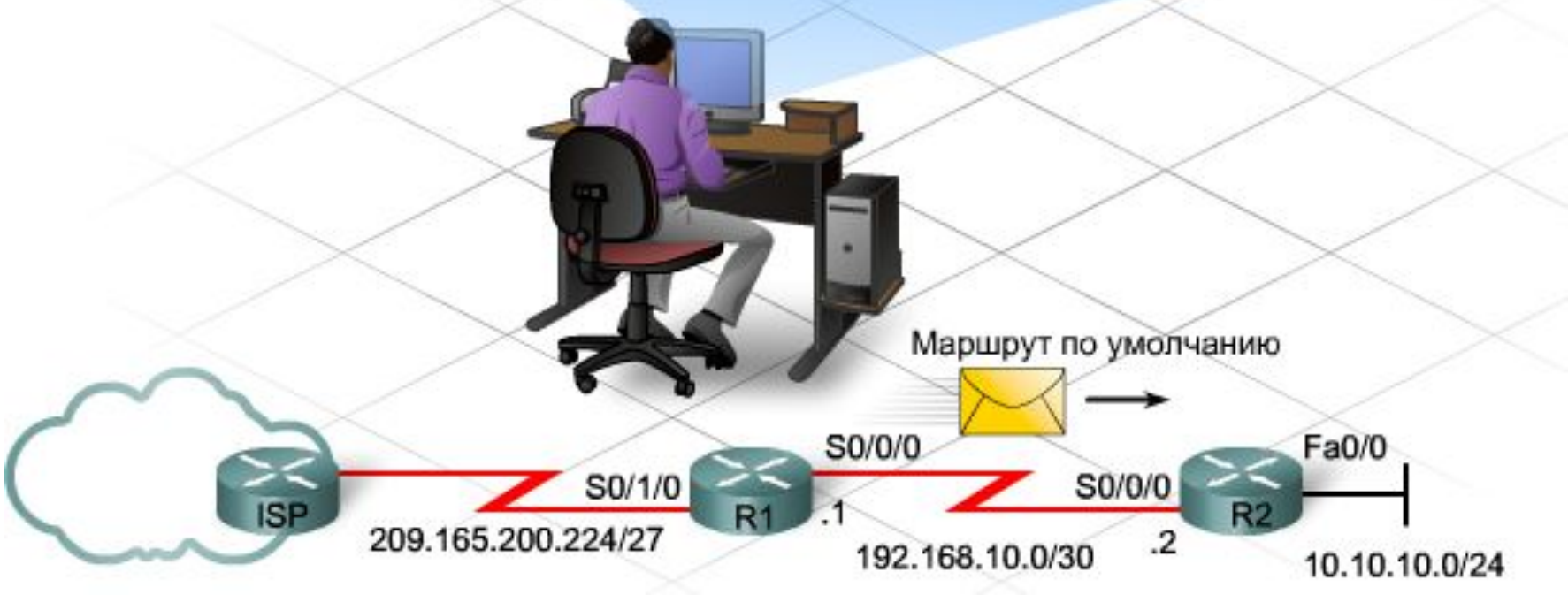
- Еще одним параметром, связанным с метрикой стоимости OSPF, является *эталонная пропускная способность*, которая используется для расчета стоимости интерфейса, также называемой стоимостью канала. Эталонная пропускная способность изменяется использованием команды OSPF **auto-cost reference-bandwidth**.

Проверка работоспособности

- **show ip ospf neighbor** используется, чтобы проверить создание отношений смежности с соседними маршрутизаторами.
- **show ip protocols** - отображает информацию, такую как идентификатор маршрутизатора, сети, объявляемые маршрутизатором OSPF, а также IP-адреса смежных соседних маршрутизаторов.
- **show ip ospf** - отображает идентификатор маршрутизатора и данные по процессу OSPF, таймеры и информацию об области. Эта команда также отображает время последнего выполнения алгоритма SPF.
- **show ip ospf interface** - отображает такую информацию, как идентификатор маршрутизатора, стоимость типа сети и настройки таймеров.
- **show ip route** - проверяет, выполняется ли отправка и получение маршрутов каждым маршрутизатором через OSPF.

Маршрут по умолчанию

```
R1(config)#ip route 0.0.0.0  0.0.0.0  serial 0/0/1
R1(config)#router ospf 1
R1(config-router)#default-information originate
```



Настройка суммирования OSPF

- Пусть имеется 4 подсети:
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.3.0/24

  Все четыре сегмента сети возможно суммировать и объявить как одну суперсеть 192.168.0.0 /22. Это позволит сократить число сетей, рассылающих объявления в области OSPF. Также снижаются требования к памяти и число записей в рассылаемых обновлениях маршрутизатора.

- Для настройки маршрутизатора OSPF ASBR на суммирование этих сегментов сети в режиме настройки маршрутизатора выполните следующую команду:

  area 0 range 192.168.0.0 255.255.252.0

Проблемы и ограничения протокола OSPF

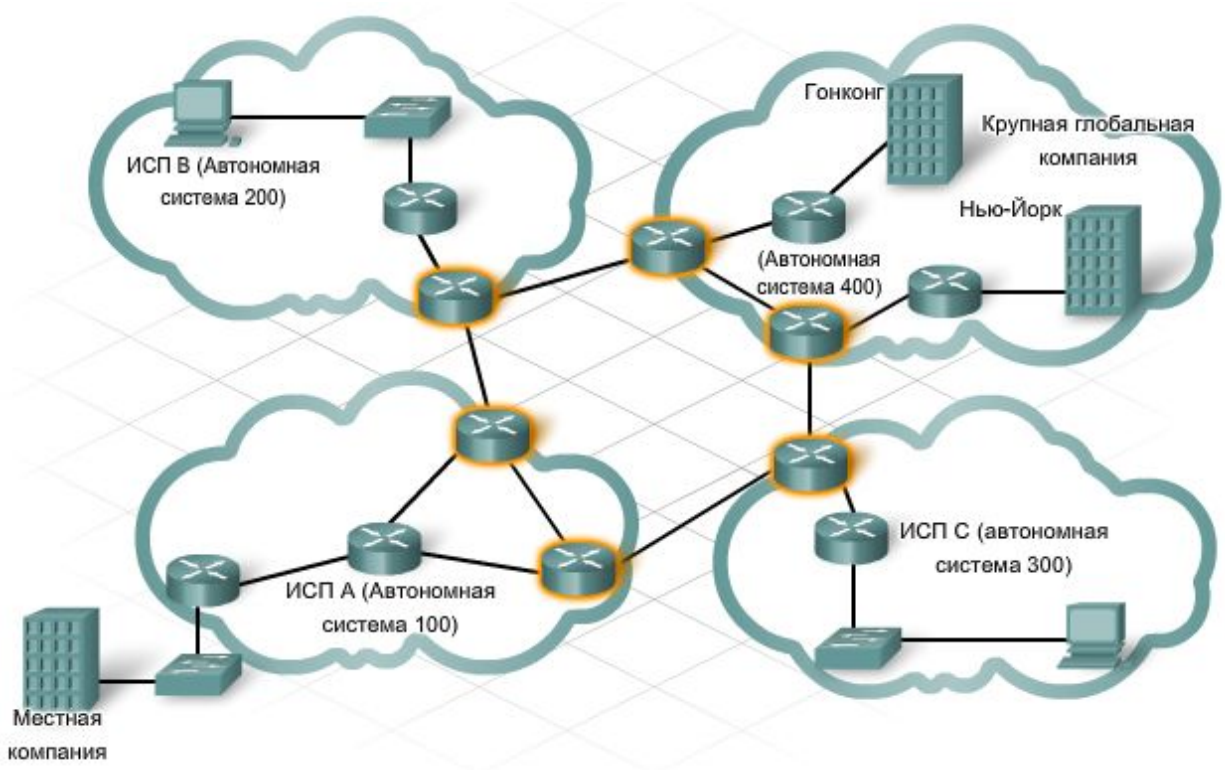
Преимущества:

- использование пропускной способности как метрики;
- быстрая конвергенция с использованием обновлений при включении;
- ограничение петель маршрутизации, благодаря согласованному представлению топологии сети;
- принятие решений о маршрутизации на основе самой последней информации;
- уменьшение размера базы данных состояний каналов — уменьшение числа расчетов SPF;
- более быстрая конвергенция;
- отображение топологии области на каждый маршрутизатор;
- поддержка CIDR и VLSM;
- иерархическая структура с использованием областей.

Недостатки:

- требуется больше памяти и более мощный процессор;
- более сложное и дорогостоящее внедрение;
- требуется администратор, разбирающийся в данном протоколе;
- первоначальная лавинная рассылка объявлений о состоянии канала (LSA) заметно снижает производительность сети.

Протоколы внешней маршрутизации



- AS представляет собой несколько сетей в ведении одного административного органа, для которых применяется единая внутренняя политика маршрутизации. Идентификатором AS служит уникальный номер автономной системы (ASN). ASN в Интернете подчиняются правилам контроля и регистрации.

Протоколы внешней маршрутизации

- Протоколы EGP выполняются на внешних маршрутизаторах, расположенных на границе автономной системы. Внешние маршрутизаторы также называются граничными шлюзами.

- Внешние маршрутизаторы обмениваются информацией о путях к различным сетям, используя внешние протоколы. Назначение внешних протоколов маршрутизации – поиск оптимального пути через Интернет в виде последовательности автономных систем.

- Самый распространенный внешний протокол маршрутизации в Интернете сегодня – *протокол граничного шлюза* (BGP). По оценкам 95% автономных систем используют BGP. Текущая версия BGP – четвертая (BGP-4), актуальное описание которой содержится в документе RFC 4271.

Протоколы внешней маршрутизации

- Маршрутизация пакетов через Интернет осуществляется в несколько этапов
  - Узел-источник отправляет пакет, предназначенный для удаленного узла в другой автономной системе.
  - Внутренние маршрутизаторы продолжают передавать пакет, выбирая маршруты по умолчанию, пока в итоге пакет не достигнет внешнего маршрутизатора на границе локальной автономной системы.
  - Внешний маршрутизатор ведет базу данных по всем автономным системам, с которыми он связан. Эта база данных достижимости сообщает маршрутизатору, что путь к сети адресата проходит через несколько AS и что следующий участок пути проходит через напрямую подключенный внешний маршрутизатор на соседней автономной системе.
  - Внешний маршрутизатор направляет пакет на следующий участок пути, которым является внешний маршрутизатор в соседней автономной системе.
  - Пакет достигает соседней автономной системы, где внешний маршрутизатор обращается к собственной базе данных достижимости и пересылает пакет к следующей автономной системе в пути.
  - Процесс повторяется на каждой автономной системе до тех пор, пока внешний маршрутизатор автономной системы-адресата не распознает IP-адрес получателя пакета как относящийся к внутренней сети данной автономной системы.
  - Конечный внешний маршрутизатор направляет пакет маршрутизатору на следующем внутреннем участке, присутствующему в его таблице маршрутизации. С этого момента пакет обрабатывается так же, как любой локальный пакет и пересылается посредством внутренних протоколов маршрутизации через несколько внутренних участков до узла-получателя.

Настройка и проверка BGP

- Первый шаг в активации BGP на маршрутизаторе состоит в настройке номера автономной системы. Это делается с помощью следующей команды:

  router bgp [номер AS]

- Следующий шаг – идентификация маршрутизатора провайдера, который будет выступать соседним узлом BGP для обмена информацией с маршрутизатором в помещении клиента (CPE). Соседний маршрутизатор идентифицируется следующей командой:

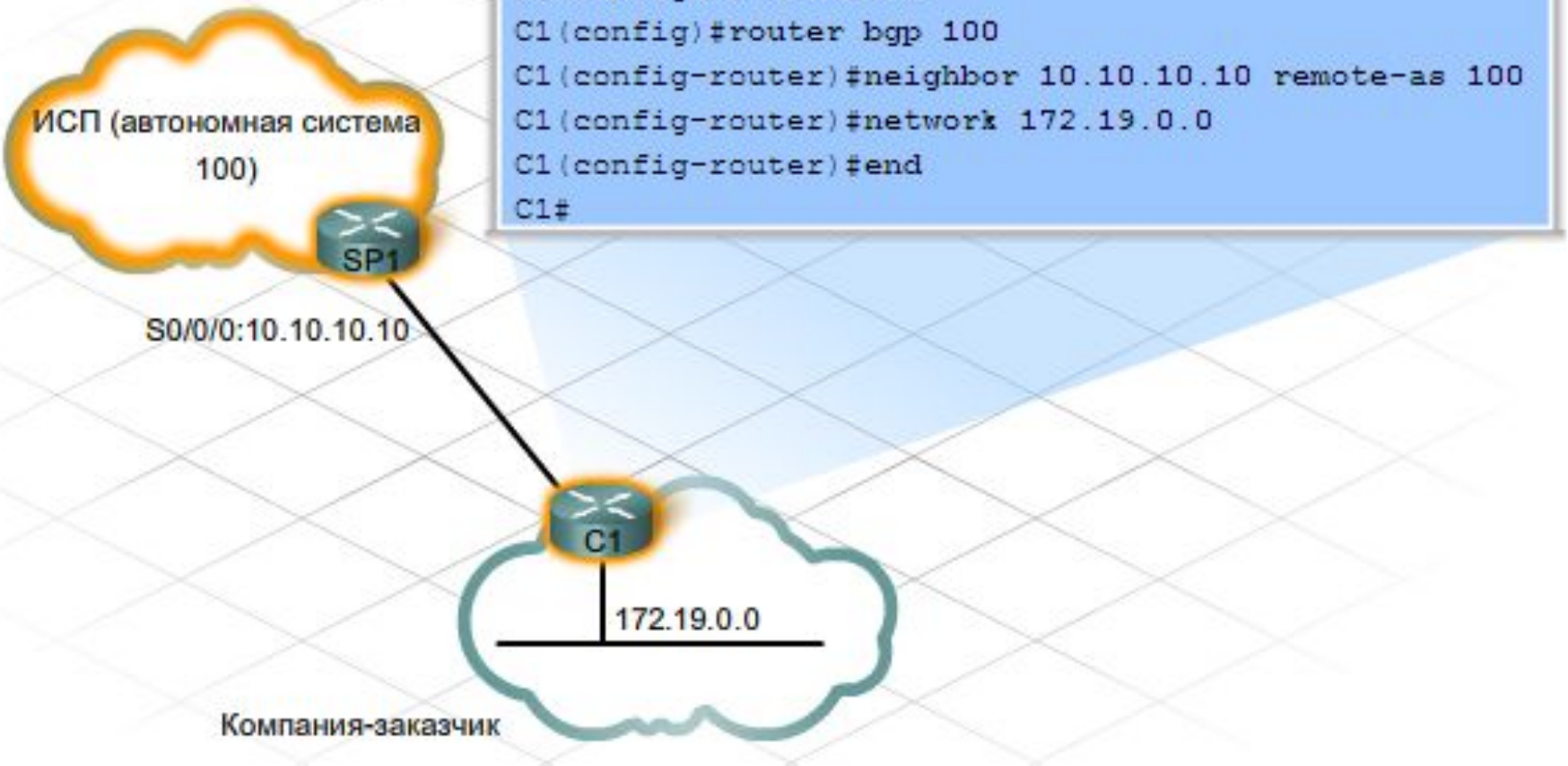
  neighbor [IP-адрес] remote-as [номер AS]

- Клиентам Интернет-провайдера, имеющим собственные зарегистрированные блоки IP-адресов, может быть необходима возможность объявления маршрутов к своим внутренним сетям в Интернете. Объявление внутренних маршрутов посредством BGP осуществляется по команде "network". Формат команды "network":

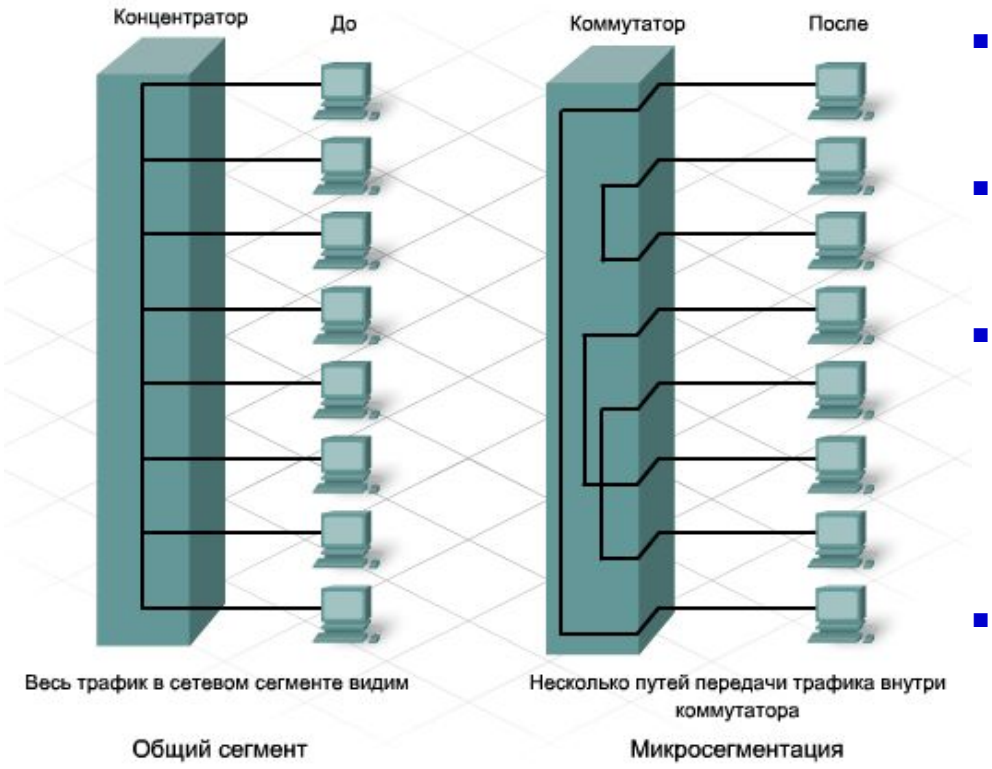
  network [адрес сети]

Настройка и проверка BGP

```
C1>enable
C1#configure terminal
C1(config)#router bgp 100
C1(config-router)#neighbor 10.10.10.10 remote-as 100
C1(config-router)#network 172.19.0.0
C1(config-router)#end
C1#
```



Коммутация и сегментация в сети



- Коммутатор – сетевое устройство 2 уровня;
- Коммутаторы могут поддерживать *симметричную* и *асимметричную* коммутацию.
- Коммутаторы, все порты которых работают на одинаковой скорости, называются симметричными.
- Многие коммутаторы имеют два или более высокоскоростных портов. Эти порты для каскадирования используются для подключения к зонам с более высокими требованиями к полосе пропускания.
- Сферы применения таких портов:
  - подключение к другим коммутаторам;
  - каналы связи с серверами или серверными фермами;
  - подключение к другим сетям.

Многоуровневая коммутация

- **Уровень 2**

  Коммутаторы уровня 2 являются аппаратными. Они пересылают трафик со скоростью, соответствующей скорости передачи среды, используя внутренние схемы, которые физически соединяют каждый порт со всеми остальными портами. Процесс пересылки использует MAC-адрес и наличие MAC-адреса назначения в таблице MAC-адресов. Коммутатор 2-го уровня пересылает трафик только внутри одного сетевого сегмента или подсети.

- **Уровень 3**

  Коммутация 3-го уровня, или многоуровневая коммутация, объединяет аппаратную коммутацию и аппаратную маршрутизацию в одном устройстве.

  Многоуровневый коммутатор объединяет функции коммутатора 2-го уровня и маршрутизатора 3-го уровня. Коммутация 3-го уровня выполняется в интегральной схеме прикладной ориентации (ASIC).

Методы пересылки кадров

- **Пересылка с буферизацией**

  Полный кадр считывается и сохраняется в памяти перед передачей устройству назначения. Коммутатор проверяет целостность битов в кадре, вычисляя значение циклического контроля четности (CRC). Если рассчитанное значение CRC совпадает со значением в поле CRC кадра, коммутатор пересылает кадр через порт назначения.

- **Сквозная коммутация**

  Сквозная коммутация включает два метода:

  - *быстрая пересылка*
  - *коммутация с исключением фрагментов*.

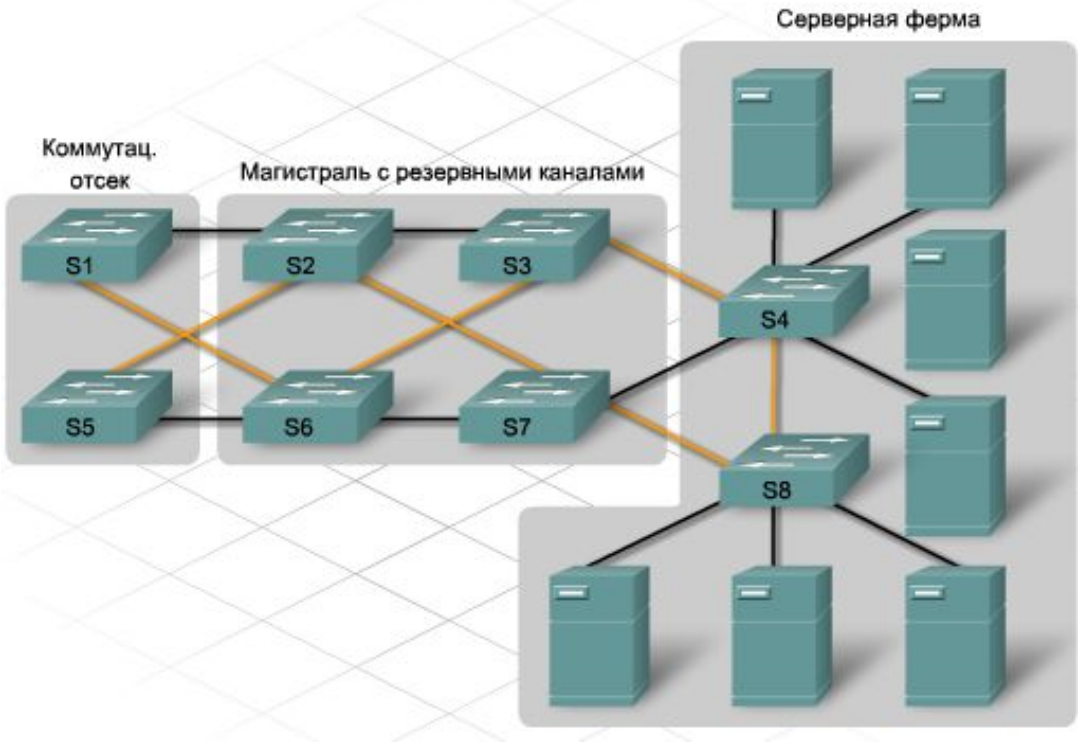
  При использовании обоих методов коммутатор пересылает кадр, не дожидаясь его полного приема.

Методы пересылки кадров

- *Быстрая пересылка* — самый быстрый метод коммутации. Коммутатор пересылает кадры из порта назначения сразу после считывания MAC-адреса. Этот метод характеризуется наименьшим запаздыванием, но может пересылать коллизионные и поврежденные фрагменты. Этот метод коммутации лучше всего работает в стабильной сети с небольшим количеством ошибок.

- При *коммутации с исключением фрагментов* коммутатор считывает первые 64 байта кадра перед началом пересылки этого кадра из порта назначения. Минимальный допустимый кадр Ethernet составляет 64 байта. Кадры меньшего размера, как правило, являются результатом коллизий и называются кадрами с недопустимо малой длиной, или пакет-"коротышка". Проверка первых 64 байт позволяет предотвратить пересылку коллизионных фрагментов коммутатором.

Резервирование в коммутируемой сети



- *Резервирование* обозначает наличие двух разных путей к одному месту назначения.
- Резервирование коммутаторов реализуется путем создания нескольких каналов между ними. Резервные каналы в коммутируемой сети снижают перегрузку и поддерживают высокую доступность и распределение нагрузки.

Проблемы резервирования

- **Широковещательные штормы** - широковещательная природа трафика Ethernet приводит к образованию **петель коммутации**. Кадры циклически распространяются во всех направлениях, вызывая "**шторм**" пакетов. Шторм занимает всю доступную полосу пропускания, блокируют создание новых сетевых подключений и разрывают существующие подключения.

- **Множественная передача кадров** - если узел посылает одноадресный кадр узлу назначения и MAC-адрес не представлен ни в одной из таблиц MAC-адресов подключенных коммутаторов, все коммутаторы выполняют лавинную рассылку этого кадра из всех портов. В сети с петлями кадр может вернуться к исходному коммутатору. Процесс повторяется, что приводит к образованию нескольких копий кадра в сети.

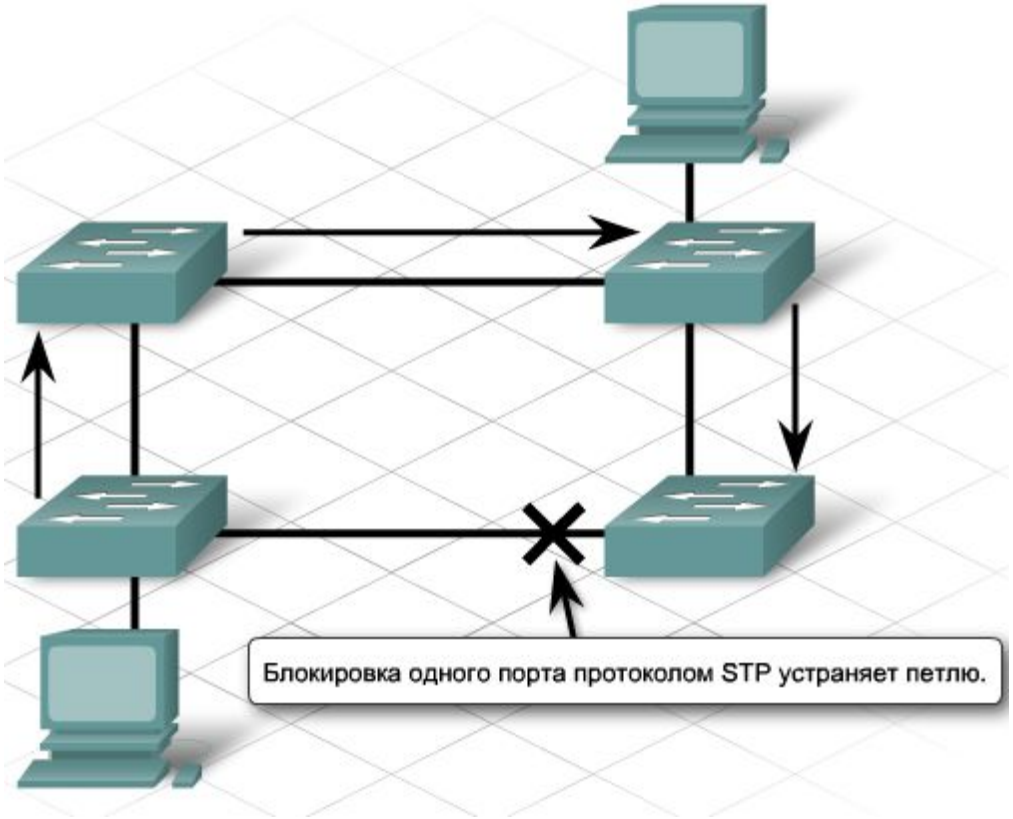
  В результате узел назначения получает несколько копий кадра. Это становится причиной трех проблем:

  - неэффективное расходование полосы пропускания;
  - неэффективное расходование циклов ЦП;
  - потенциальное дублирование транзакционного трафика.

- **Нестабильность базы данных MAC-адресов** - коммутаторы в резервируемой сети могут получать неверные данные о положении узла. Если в сети присутствует петля, один коммутатор может связать MAC-адрес назначения с двумя портами. Это приведет к путанице и неоптимальной пересылке кадров.

Протокол STP

- Протокол STP обеспечивает механизм отключения резервных каналов в коммутируемой сети. STP позволяет использовать резервирование, необходимое для надежной эксплуатации, без создания петель коммутации. STP основывается на открытых стандартах и используется для создания логической топологии без петель коммутации.



Протокол STP

Чтобы предотвратить образование петель, протокол STP:

- переводит часть интерфейсов в резервный или заблокированный режим;
- оставляет другие интерфейсы в режиме пересылки;
- перенастраивает сеть, активируя соответствующий резервный путь, если путь пересылки становится недоступным.

- **Корневой мост** — это основной мост или **центральная точка** в топологии STP.

- Корневой мост взаимодействует с другими коммутаторами с помощью *блоков данных протокола моста* (BPDU). BPDU — это кадры, которые рассылаются другим коммутаторам каждые 2 секунды.

- BPDU содержат следующие сведения:
  - идентификатор коммутатора-источника;
  - идентификатор порта-источника;
  - стоимость порта-источника;
  - значение таймеров устаревания;
  - значение таймера приветствия.

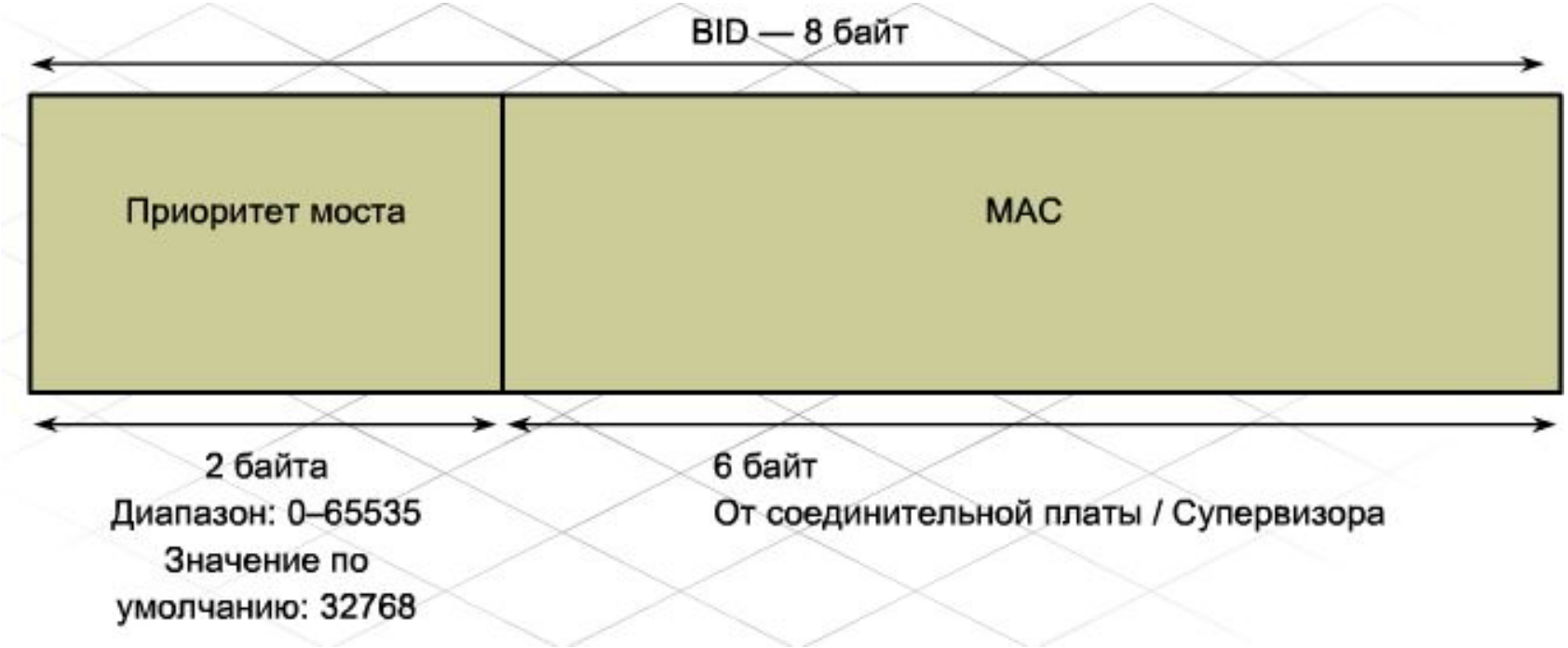
Режимы работы коммутатора

Блокирующий режим:	Режим прослушивания:	Режим обучения:	Режим пересылки:
• немигающий желтый; • принимает BPDU; • сбрасывает кадры данных; • не получает адреса; • переход в режим прослушивания занимает до 20 секунд.	• мигающий желтый; • прослушивает BPDU; • не пересылает кадры; • не заучивает MAC-адреса; • определяет, есть ли у коммутатора более одного магистрального порта, что может привести к образованию петли; • если петля есть – переход к блокирующему режиму; • если петли нет – переход к режиму обучения; • переход к режиму обучения – 15 сек (задержка при пересылке).	• мигающий желтый; • обрабатывает BPDU; • получает MAC-адреса из принятого трафика; • не пересылает кадры; • переход в режим пересылки – 15 секунд.	• мигающий зеленый; • обрабатывает BPDU; • получает MAC-адреса; • пересылает кадры.

Корневые мосты

- STP использует центральную точку сети, которая называется **корневым мостом** или **корневым коммутатором**, для определения портов, которые необходимо блокировать, и портов, которые следует перевести в режим пересылки. Корневой мост рассылает кадры BPDU с информацией о топологии сети всем остальным коммутаторам. Эта информация обеспечивает перенастройку сети в случае отказа.

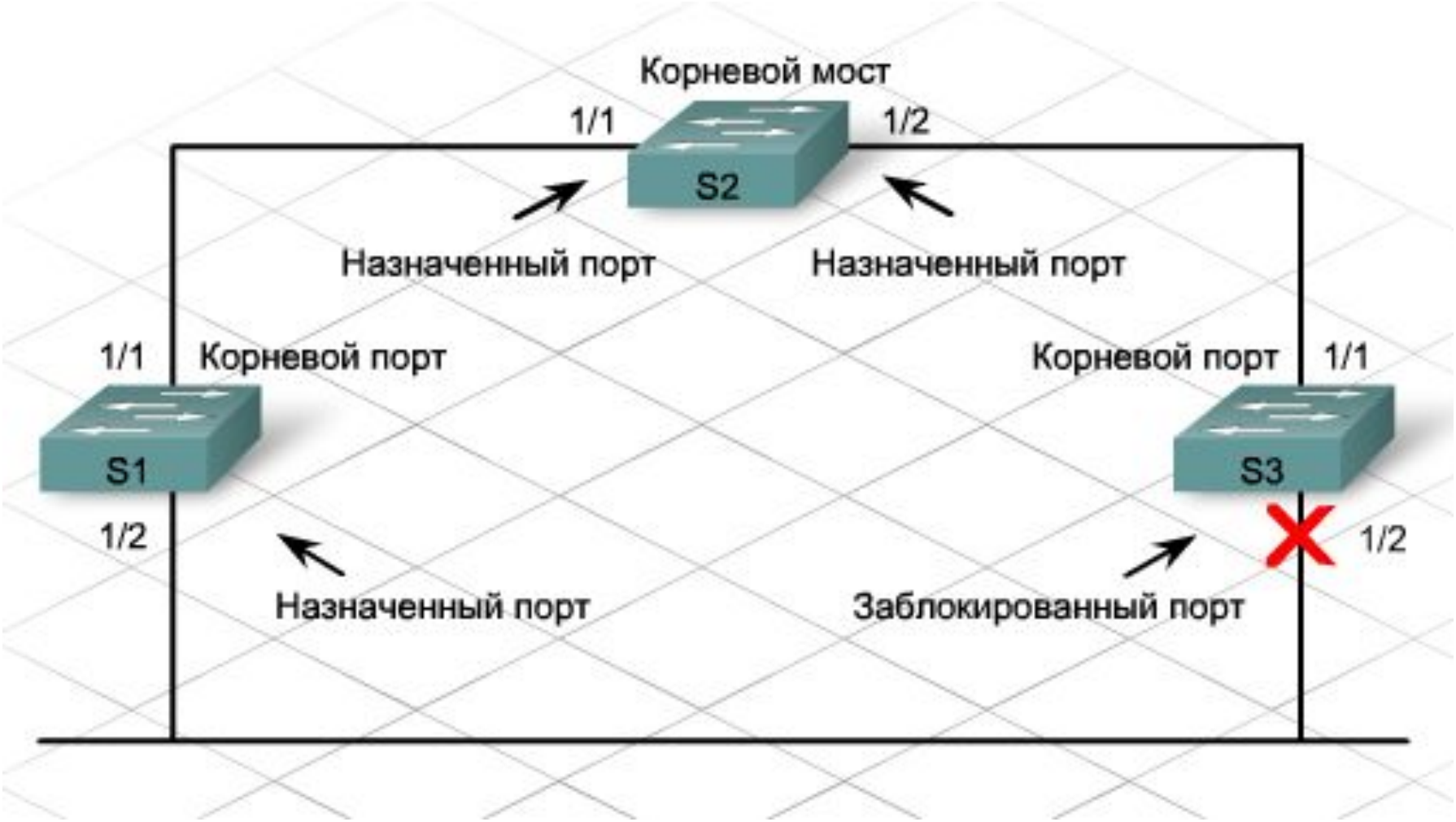
- В каждой сети работает только **один** корневой мост, который выбирается на основании идентификатора моста (BID). BID равняется сумме значения приоритета моста и его MAC-адреса.



Корневые мосты

- Мост с **наименьшим значением BID** становится **корневым**.
- STP использует три типа портов: *корневые порты, назначенные порты* и *заблокированные порты*.
- **Корневой порт** – порт с маршрутом оптимальной стоимости к корневому мосту назначается корневым. Коммутаторы вычисляют путь с наименьшей стоимостью, используя стоимость полосы пропускания каждого канала на пути к корневому мосту.
- **Назначенный порт** – назначенный порт пересылает трафик к корневому мосту, но не подключен к пути с наименьшей стоимостью.
- **Заблокированный порт** – заблокированный порт не пересылает трафик.

Корневые мосты



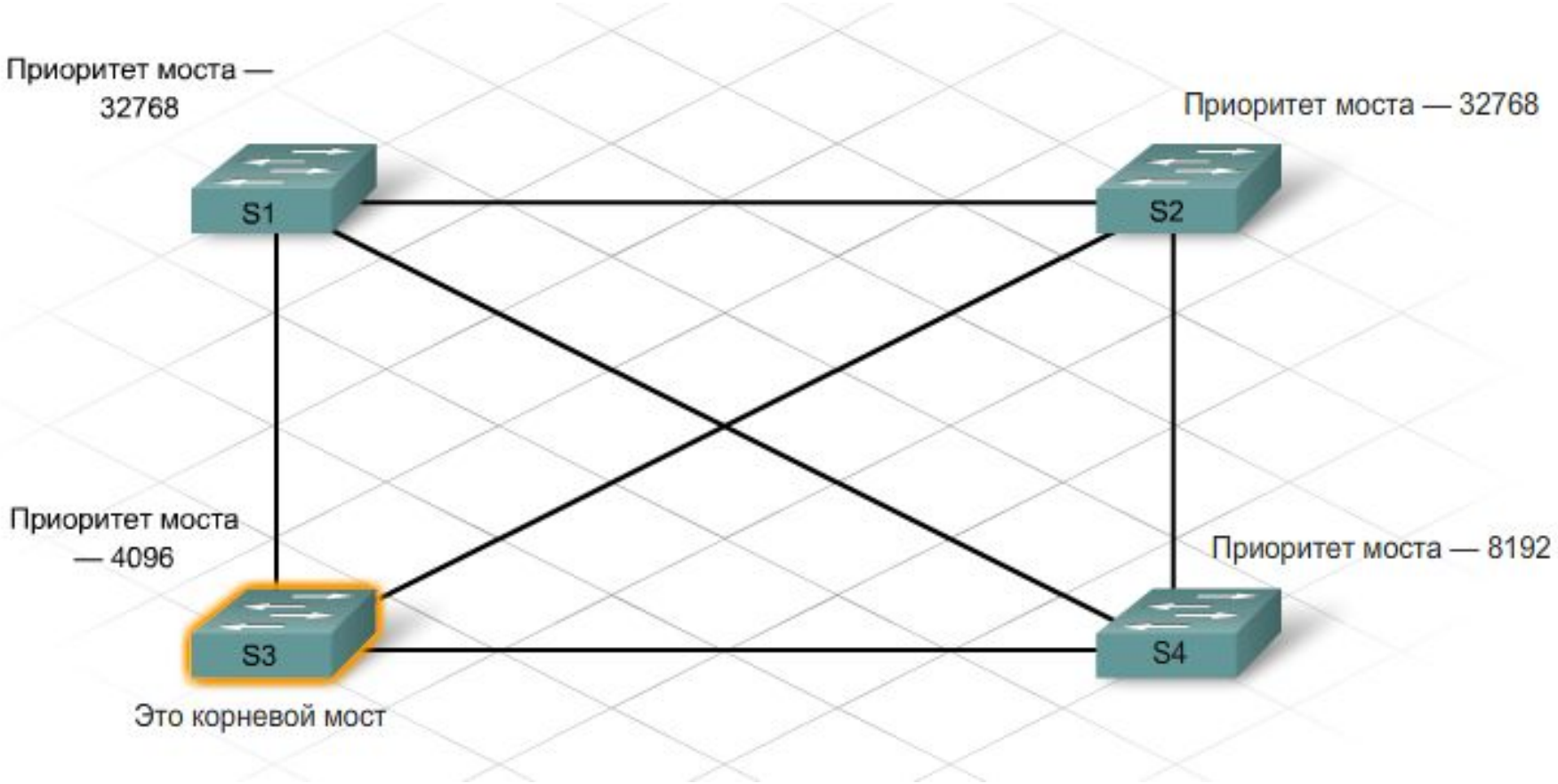
Настройка приоритета моста

- Задание приоритета:

  S3(config)#bridge priority 4096

- Восстановление приоритета по умолчанию:

  S3(config)#no bridge priority



Протокол STP в иерархической сети

- Если происходит отказ канала, STP перерассчитывается путем:
  - перевода некоторых портов из блокирующего режима в режим пересылки;
  - перевода некоторых портов из режима пересылки в блокирующий режим;
  - формирования нового дерева STP для предотвращения образования петель в сети.
- Время перерасчета сети – 50 секунд

- Усовершенствования STP (собственность компании Cisco):
- **PortFast**

  STP PortFast немедленно переводит порт доступа в *режим пересылки*, минуя режимы прослушивания и обучения.

- **UplinkFast**

  STP UplinkFast ускоряет выбор нового корневого порта при отказе коммутатора или канала, а также при перерасчете STP. Корневой порт немедленно переходит в *режим пересылки*, минуя режимы прослушивания и обучения, которые подразумеваются обычными процедурами STP.

- **BackboneFast**

  BackboneFast обеспечивает быструю конвергенцию после изменений топологии STP. Эта функция позволяет быстро восстанавливать подключение к магистрали. Функция BackboneFast используется на уровне распределения и центральном уровне, на которых соединяется несколько коммутаторов.

Команды show для проверки протокола STP

Для проверки работоспособности протокола STP используется несколько полезных команд.

- **show spanning-tree** — отображает идентификатор корневого моста, идентификатор моста и состояния портов
- **show spanning-tree summary** — отображает сводку состояний портов;
- **show spanning-tree root** — отображает конфигурацию и состояние корневого моста;
- **show spanning-tree detail** — отображает подробные сведения о портах;
- **show spanning-tree interface** — выводит состояние и конфигурацию интерфейса STP;
- **show spanning-tree blockedports** — отображает заблокированные порты.

Протокол RSTP

- Протокол **Rapid Spanning Tree Protocol (RSTP)**, определенный в стандарте IEEE 802.1w, значительно ускоряет перерасчет STP.

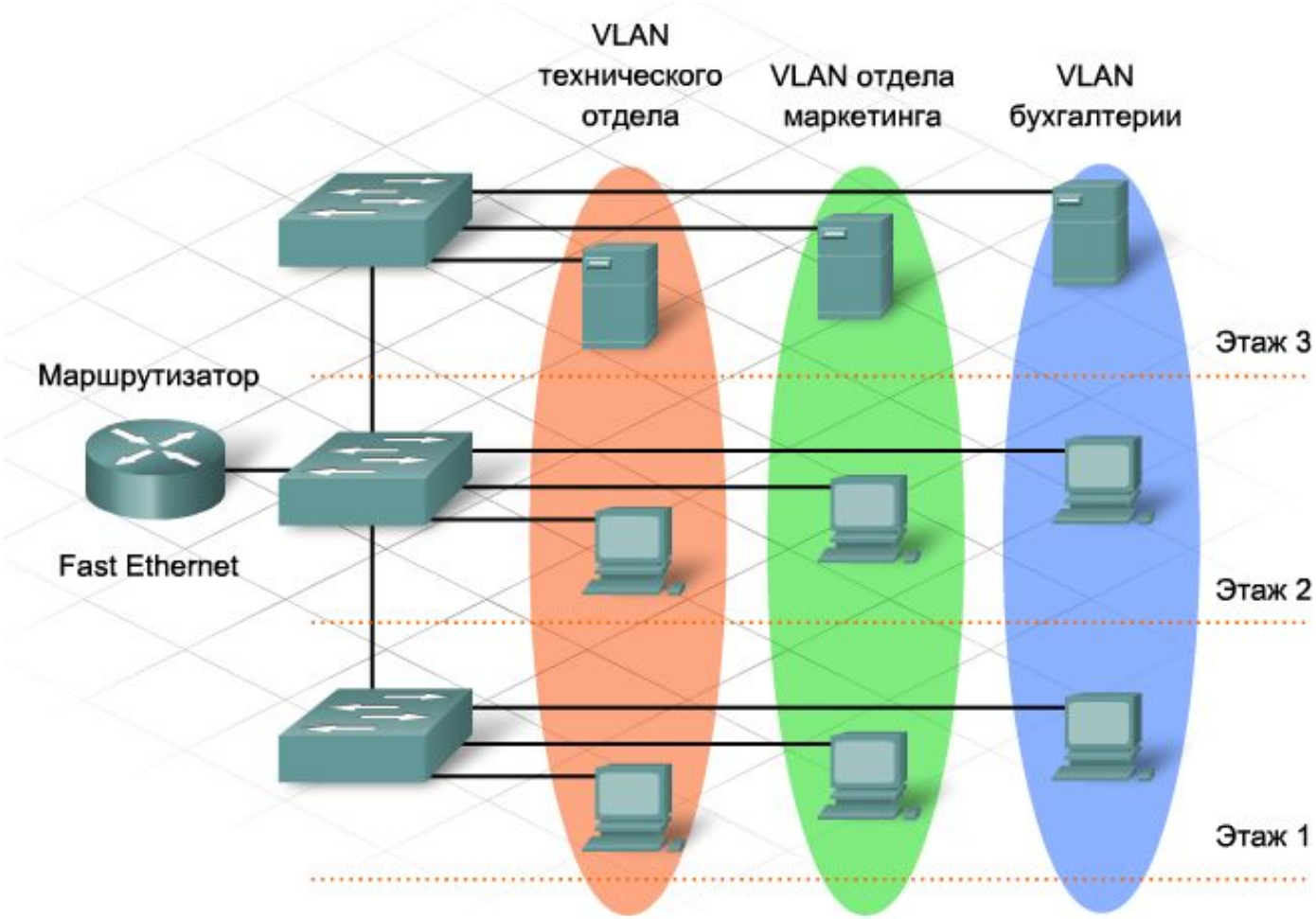
- Для обеспечения максимальной скорости переконфигурации протокол RSTP требует полнодуплексного соединения "точка-точка" между коммутаторами. Переконфигурация связующего дерева при использовании протокола RSTP занимает менее одной секунды, аналогичный процесс протокола STP занимает 50 секунд.

- Для ускорения перерасчета число режимов портов протокола RSTP уменьшено до трех: *отклонение (сброс)*, *обучение* и *пересылка*. Режим сброса аналогичен трем оригинальным режимам STP: блокировки, обучения и "отключен".

- Концепция *активная топология*. Все порты, которые не находятся в режиме сброса (не заблокированы), считаются частью активной топологии и немедленно переходят в режим пересылки.

VLAN

- **VLAN** — это логический домен широковещательной рассылки, который может охватывать несколько физических сегментов LAN. Она позволяет администратору объединять станции по логической функции, проектной группе или приложению независимо от физического положения пользователей.



VLAN

- Широковещательные кадры не пересылаются между VLAN, они остаются внутри одной VLAN.

- Каждая VLAN функционирует как отдельная локальная сеть. VLAN может охватывать один или несколько коммутаторов, что позволяет узлам работать так, как если бы они находились в одном сегменте.

- VLAN выполняют две основные функции:
  - ограничение широковещательных рассылок;
  - объединение устройств в группы; устройства, расположенные в одной VLAN, невидимы для устройств, расположенных в другой VLAN.

- Для передачи трафика между VLAN необходимо устройство 3-го уровня.

Назначение устройства во VLAN

- В коммутируемой сети устройство можно назначить во VLAN *статически* или *динамически*.

- Для задания **статической** принадлежности VLAN администратор должен вручную назначить каждый порт коммутатора в определенную VLAN. Например, порт fa0/3 можно назначить во VLAN 20. Любое устройство, подключающееся к порту fa0/3, автоматически становится членом VLAN 20.

- **Динамическая** принадлежность VLAN требует наличия сервера управления политикой VLAN (VMPS). VMPS содержит базу данных, которая сопоставляет MAC-адреса с сетями VLAN. Когда устройство подключается к порту, VMPS ищет его MAC-адрес в своей базе данных и временно назначает порт в соответствующую VLAN.

  Динамическая принадлежность VLAN требует более сложной настройки и организации, но формирует более гибкую структуру, чем статическая принадлежность VLAN. Перемещение, добавление и изменение компонентов в динамической VLAN выполняется автоматически и не требует вмешательства администратора.

Настройка VLAN

- Для настройки VLAN используются следующие команды режима глобальной конфигурации:

  Switch(config)#vlan vlan_number
  Switch(config-vlan)#name vlan_name
  Switch(config-vlan)#exit

- Используйте следующие команды для назначения отдельных портов в сети VLAN:

  Switch(config)#interface fa#/#
  Switch(config-if)#switchport access vlan vlan_number
  Switch(config-if)# exit

- Используйте следующие команды для назначения диапазонов портов в сети VLAN:

Switch(config)#interface range fa#/start_of_range - end_of_range
Switch(config-if)#switchport access vlan vlan_number
Switch(config-if)#exit

Настройка VLAN

```
Switch#configure terminal
Switch(config)#vlan 27
Switch(config-vlan)#name accounting
Switch(config-vlan)#exit
Switch(config)#interface fa0/13
Switch(config-if)#switchport access vlan 27
Switch(config-if)#exit
Switch(config)#vlan 28
Switch(config-vlan)#name engineering
Switch(config-vlan)#exit
Switch(config)#interface fa0/6-12
Switch(config-if)#switchport access vlan 28
Switch(config-if)#end
Switch#show vlan

VLAN    Name                Status     Ports
```

Проверка работоспособности VLAN

Для проверки и обслуживания VLAN используются следующие команды:

- **show vlan** – выводит подробный список номеров и имен VLAN, активных на коммутаторе, а также портов, назначенных в каждую из них; выводит статистику протокола STP, если он настроен, для каждой VLAN.
- **show vlan brief** – выводит сводный список, в котором отображаются только активные VLAN и их порты.
- **show vlan id номер_id –** выводит сведения об определенной VLAN по ее идентификатору.
- **show vlan name имя_vlan –** выводит сведения об определенной VLAN по ее имени.

Удаление VLAN

- Удаление VLAN:

  Switch(config)#no vlan номер_vlan

- Удаление порта из определенной VLAN:

  Switch(config)#interface fa#/#

  Switch(config-if)#no switchport access vlan номер_vlan

```
Switch(config)#interface fa0/8
Switch(config-if)#no switchport access vlan 28
Switch(config-if)#exit
Switch(config)#no vlan 27
Switch(config)#end
Switch#show vlan

VLAN    Name                Status     Ports
------- ------------------- ---------- -------------------------------
1       default             active     Fa0/1, Fa0/4, Fa0/5, Fa0/8
                                       Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                       Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                       Fa0/22, Fa0/23, Fa0/24
```

Магистральные порты

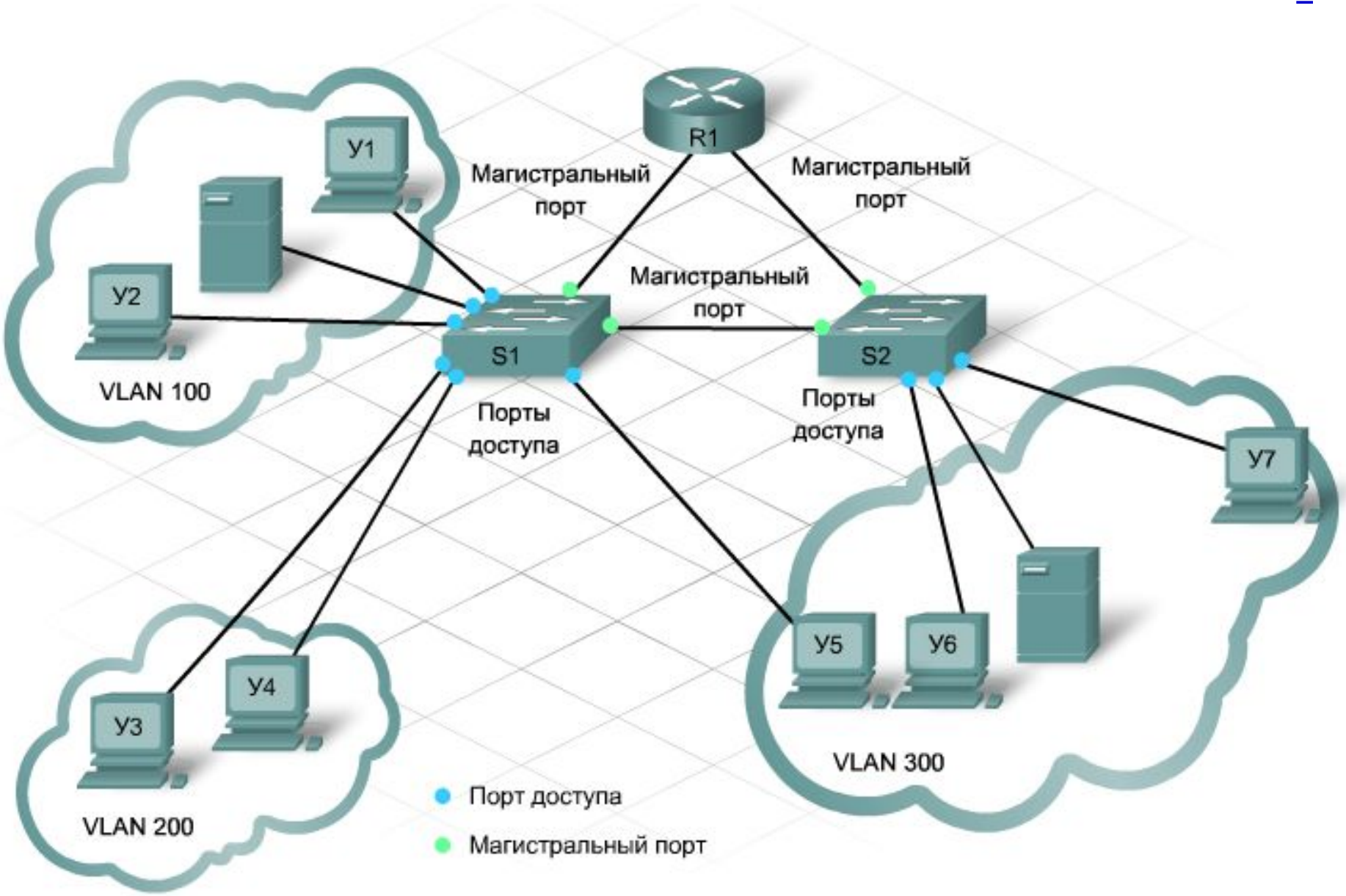
- Для портов коммутатора можно задать две разные роли. Порт может быть определен как **порт доступа** или как **магистральный порт**.

- **Порт доступа**

  Порт доступа принадлежит только одной VLAN. Как правило, отдельные устройства, такие как компьютеры и серверы, подключаются к портам такого типа. Если несколько компьютеров подключаются к одному порту доступа через концентратор, все устройства, подключенные к концентратору, будут принадлежать к одной VLAN.

- **Магистральный порт**

  Магистральный порт — это канал типа "точка-точка" между коммутатором и другим сетевым устройством. Магистральные подключения служат для передачи трафика нескольких VLAN через один канал и обеспечивают им доступ ко всей сети. Магистральные порты необходимы для передачи трафика нескольких VLAN между устройствами при соединении двух коммутаторов, коммутатора и маршрутизатора или коммутатора и сетевого адаптера узла с поддержкой транкинга 802.1Q.


R1
Магистральный порт
Магистральный порт
Магистральный порт
S1
S2
Порты доступа
Порты доступа
У1
У2
VLAN 100
У3
У4
VLAN 200
У5
У6
У7
VLAN 300
Порт доступа
Магистральный порт

Настройка магистрального порта

- По умолчанию порты коммутатора работают **в режиме доступа**. Чтобы настроить порт коммутатора в качестве **магистрального порта**, используйте следующие команды:

  Switch(config)#interface fa(controler # / port #)

  Switch(config-if)#switchport mode trunk

  Switch(config-if)#switchport trunk

  encapsulation {dot1q | isl | negotiate}

- Чтобы вернуть магистральный порт в режим доступа, введите одну из следующих команд:

  Switch(config)#interface fa(controler # / port #)

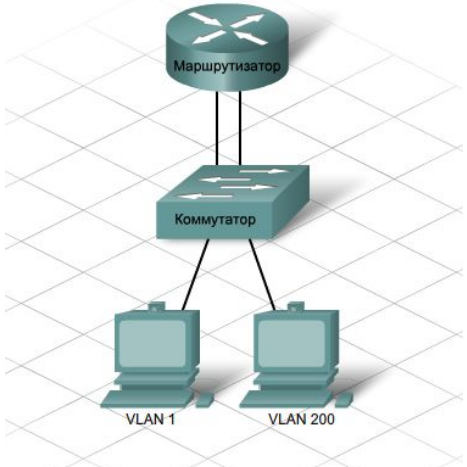
  Switch(config-if)#no switchport mode trunk

  или

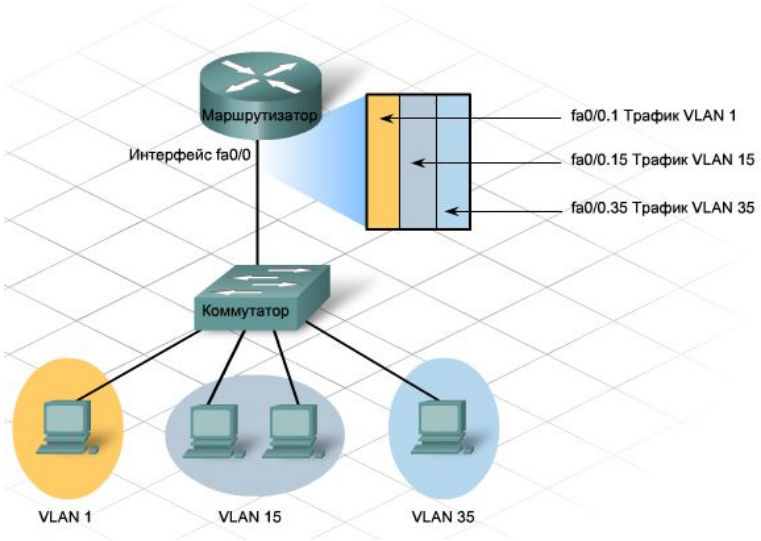
  Switch(config-if)#switchport mode access

Маршрутизация между VLAN

- Взаимодействие между VLAN с использованием подынтерфейсов требует настройки как маршрутизатора, так и коммутатора.
- Коммутатор
  - Настройте интерфейс коммутатора в качестве магистрального канала 802.1Q.
- Маршрутизатор
  - выберите интерфейс маршрутизатора не ниже FastEthernet 100 Мбит/с;
  - настройте подынтерфейсы с поддержкой инкапсуляции 802.1Q;
  - для каждой VLAN настраивается один подынтерфейс.



VLAN 1 может взаимодействовать с VLAN 200, если обе сети имеют подключение к маршрутизатору.



“Router-on-a-stick”

Чтобы настроить маршрутизацию между VLAN, выполните следующие действия:

- Настройте магистральный порт на коммутаторе.

  Switch(config)#interface fa0/2

  Switch(config-if)#switchport mode trunk

- На маршрутизаторе настройте интерфейс FastEthernet без IP-адреса и маски подсети.

  Router(config)#interface fa0/1

  Router(config-if)#no ip address

  Router(config-if)#no shutdown

“Router-on-a-stick”

- На маршрутизаторе настройте один подынтерфейс с IP-адресом и маской подсети для каждой VLAN. Каждый подынтерфейс использует инкапсуляцию 802.1Q.

  Router(config)#interface fa0/0.10

  Router(config-subif)#encapsulation dot1q 10

  Router(config-subif)#ip address 192.168.10.1 255.255.255.0

- Проверьте конфигурацию и работоспособность маршрутизации между VLAN с помощью следующих команд.

  Switch#show trunk

  Router#show ip interfaces

  Router#show ip interfaces brief

  Router#show ip route

Протокол VTP

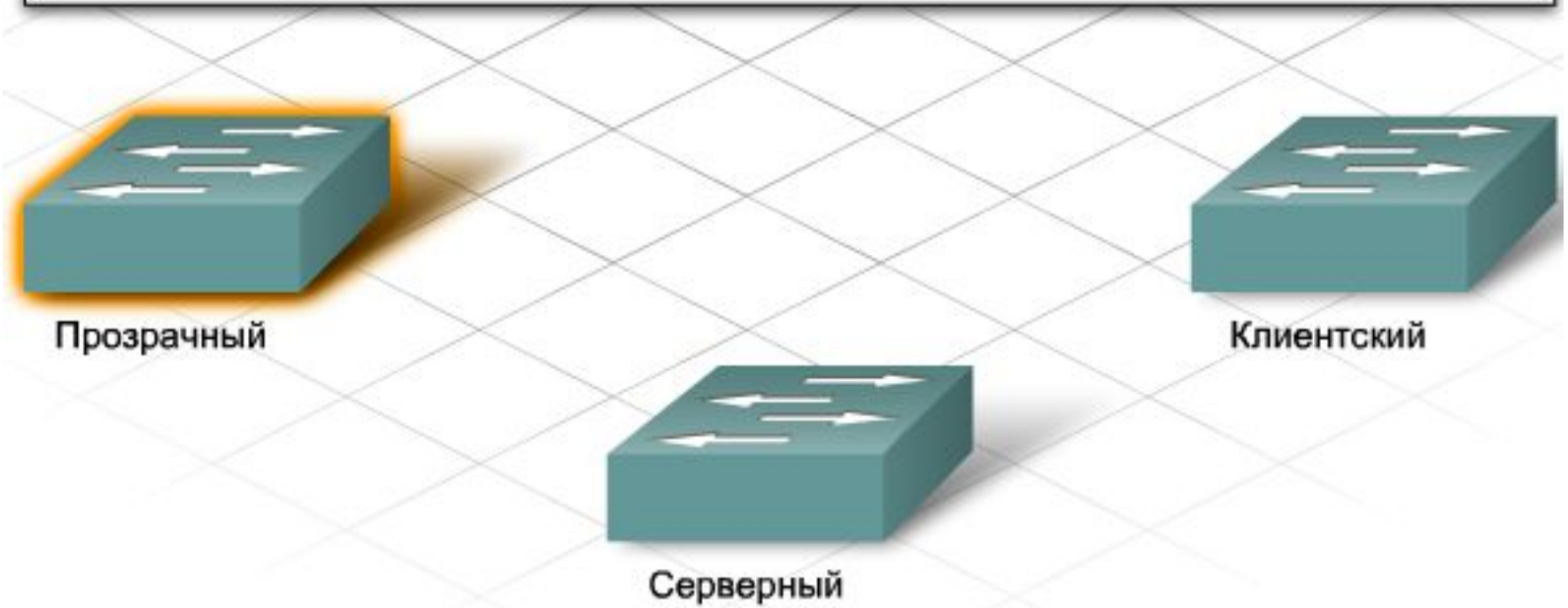
- Протокол **VTP** (*VLAN Trunking Protocol*) — это протокол обмена сообщениями 2-го уровня, который предоставляет метод управления базой данных VLAN с центрального сервера в сетевом сегменте. Маршрутизаторы не пересылают обновления VTP.

- VTP — это протокол обмена сообщениями с архитектурой "клиент-сервер", который добавляет, удаляет и переименовывает VLAN в одном домене VTP. Все коммутаторы под общим управлением являются частью домена. У каждого домена есть уникальное имя. Коммутаторы VTP обмениваются сообщениями VTP только с другими коммутаторами в домене.

- VTP использует три режима: **серверный**, **клиентский** и **прозрачный** (transparent). По умолчанию все коммутаторы являются серверами.

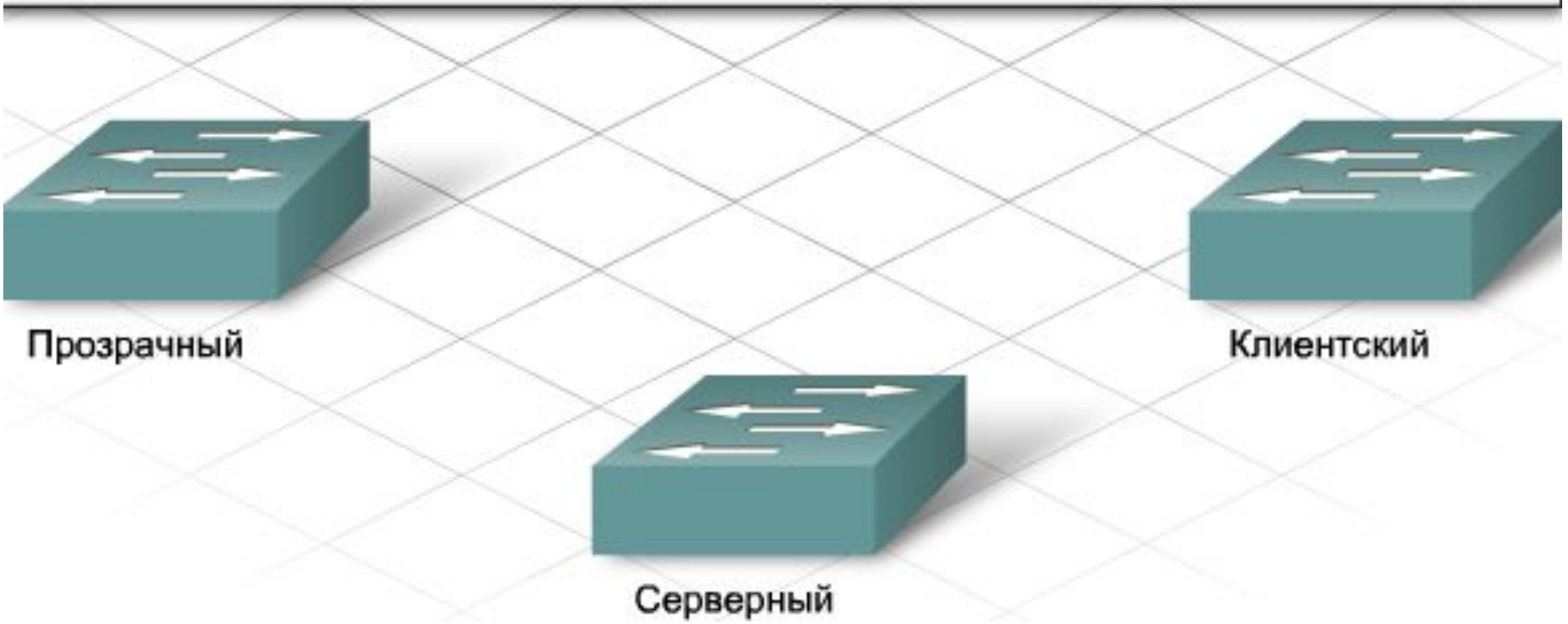
Прозрачный

- Пересылает объявления VTP.
- Игнорирует данные в сообщении VTP.
- Не изменяет базу данных при получении обновлений.
- Не рассылает обновления при изменении своей базы данных VLAN.



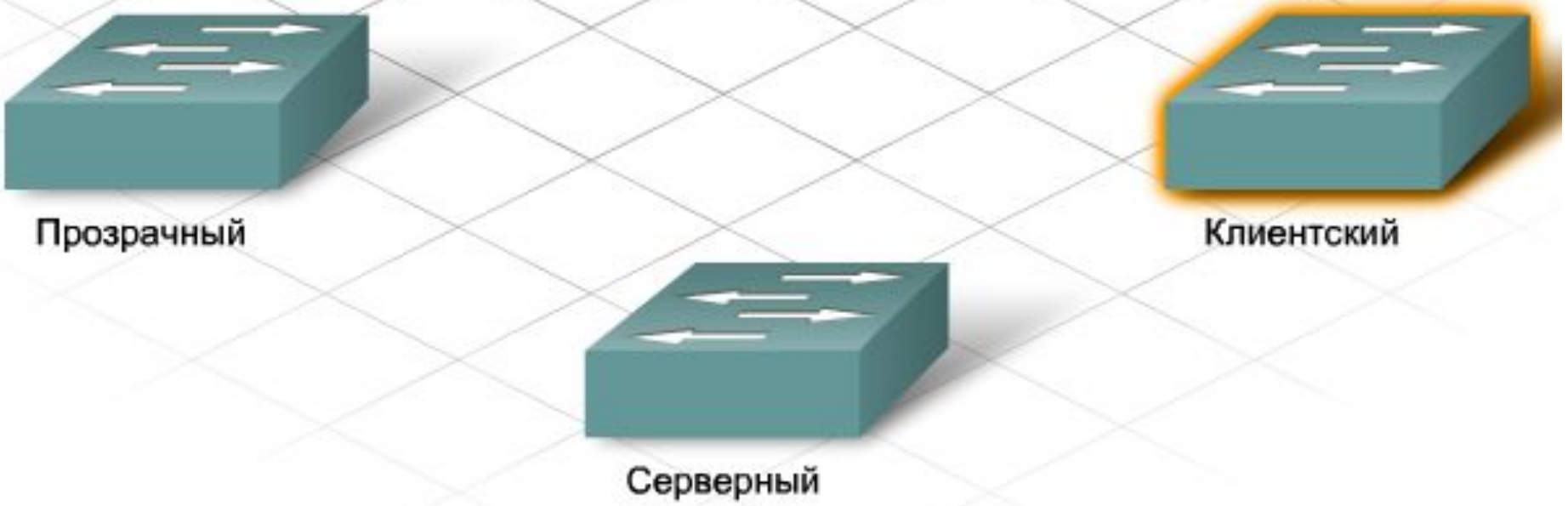
Серверный

- Создает, изменяет и удаляет VLAN и параметры конфигурации VLAN во всем домене.
- Сохраняет данные конфигурации VLAN в NVRAM коммутатора.
- Рассылает сообщения VTP со всех магистральных портов.



Клиентский

- Не создает, не изменяет и не удаляет данные VLAN.
- Изменяет свою базу данных при получении изменений VLAN от сервера.
- Рассылает сообщения VTP со всех магистральных портов



Типы сообщений VTP

- **Сводные объявления**

  Коммутаторы Catalyst рассылают сводные объявления каждые 5 минут, а также при изменении базы данных VLAN. Сводные объявления содержат текущее имя домена VTP и номер версии конфигурации.

  При добавлении, удалении или изменении VLAN сервер увеличивает номер версии конфигурации и отправляет сводное объявление.

  При получении пакета сводного объявления коммутатор сравнивает имя домена VTP со своим именем домена VTP. Если имена домена совпадают, коммутатор сравнивает номер версии конфигурации со своим номером. Если номер версии выше, отправляется запрос объявления.

- **Сокращенные объявления**

  Сокращенное объявление отправляется после сводного объявления. Сокращенное объявление содержит список данных VLAN. Сокращенное объявление содержит новые данные VLAN, основанные на сводном объявлении. Если в сети несколько VLAN, потребуется несколько сокращенных объявлений.

- **Запросы объявлений**

  VTP-клиенты используют запросы объявлений, чтобы запросить информацию о VLAN. Запросы объявлений необходимы, если коммутатор сброшен или изменено имя домена VTP. Коммутатор получает сводное объявление VTP с более высоким номером версии конфигурации, чем его собственный.

Настройка VTP

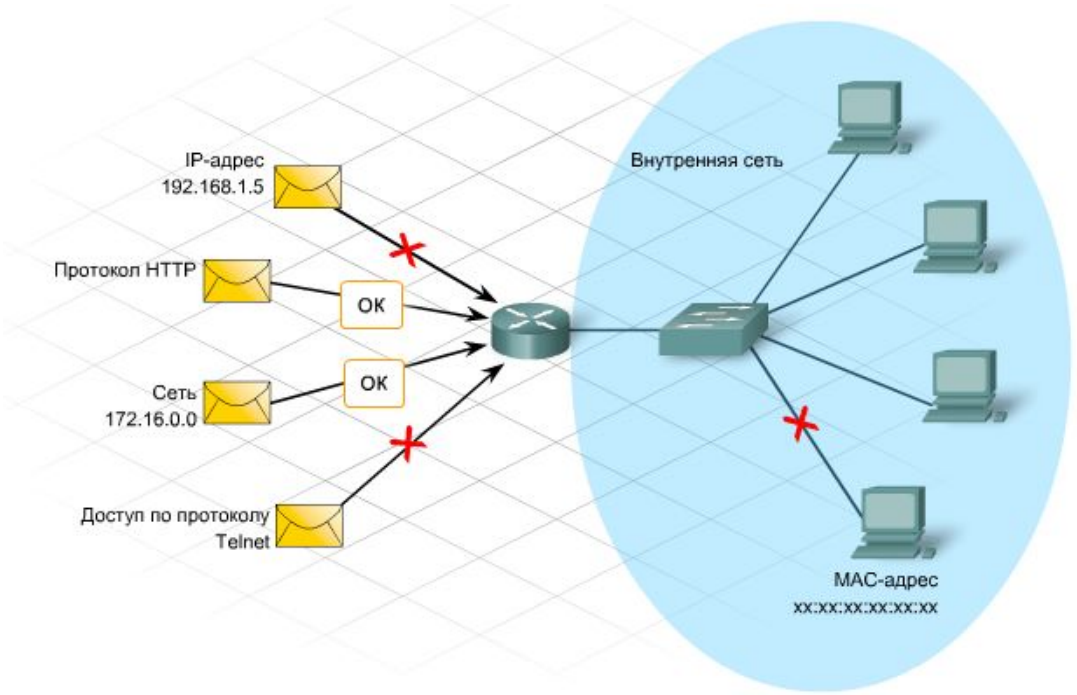
- При добавлении нового коммутатора в существующий домен VTP выполните следующие действия:
  - настройте протокол VTP в автономном режиме;
  - проверьте конфигурацию VTP;
  - перезагрузите коммутатор.

```
Switch(config)#vtp domain domain_name
Switch(config)#vtp mode {server | client | transparent}
Switch(config)#vtp password password
Switch(config)#end
Switch#copy running-config startup-config
```

Списки контроля доступа

- **Фильтрация представляет собой процесс анализа содержимого пакета с целью разрешения или блокировки его передачи**.

- Фильтрация пакетов может быть простой и сложной и может запрещать или разрешать трафик по следующим критериям:
  - исходный IP-адрес;
  - конечный IP-адрес;
  - MAC-адреса;
  - протоколы;
  - тип приложения.



Списки контроля доступа (ACL-списки)

- ACL-списки определяют трафик для нескольких целей:
  - указание внутренних узлов для NAT;
  - обнаружение и классификация трафика для обеспечения расширенных возможностей;
  - ограничение содержимого обновления маршрутизации;
  - ограничение отладочных выходных данных;
  - контроль доступа виртуальных терминалов к маршрутизаторам.

- Использование ACL-списков может быть сопряжено со следующими потенциальными проблемами:
  - дополнительная нагрузка на маршрутизатор для проверки всех пакетов означает меньшее время на фактическую пересылку пакетов;
  - плохо организованные ACL-списки создают даже еще большую нагрузку на маршрутизатор и могут нарушить работоспособность сети;
  - неправильно размещенные ACL-списки блокируют допустимый трафик и разрешают запрещенный.

Типы ACL-списков

- Стандартный ACL-список является самым простым из трех типов. При создании стандартного ACL-списка для IP-протокола, фильтрация по ACL-спискам осуществляется на основе исходного IP-адреса пакета. Стандартные ACL-списки определяются по присваиваемым им номерам. Номера из диапазона от 1 до 99 и от 1 300 до 1 999 присваиваются спискам доступа, разрешающим или блокирующим IP-трафик.

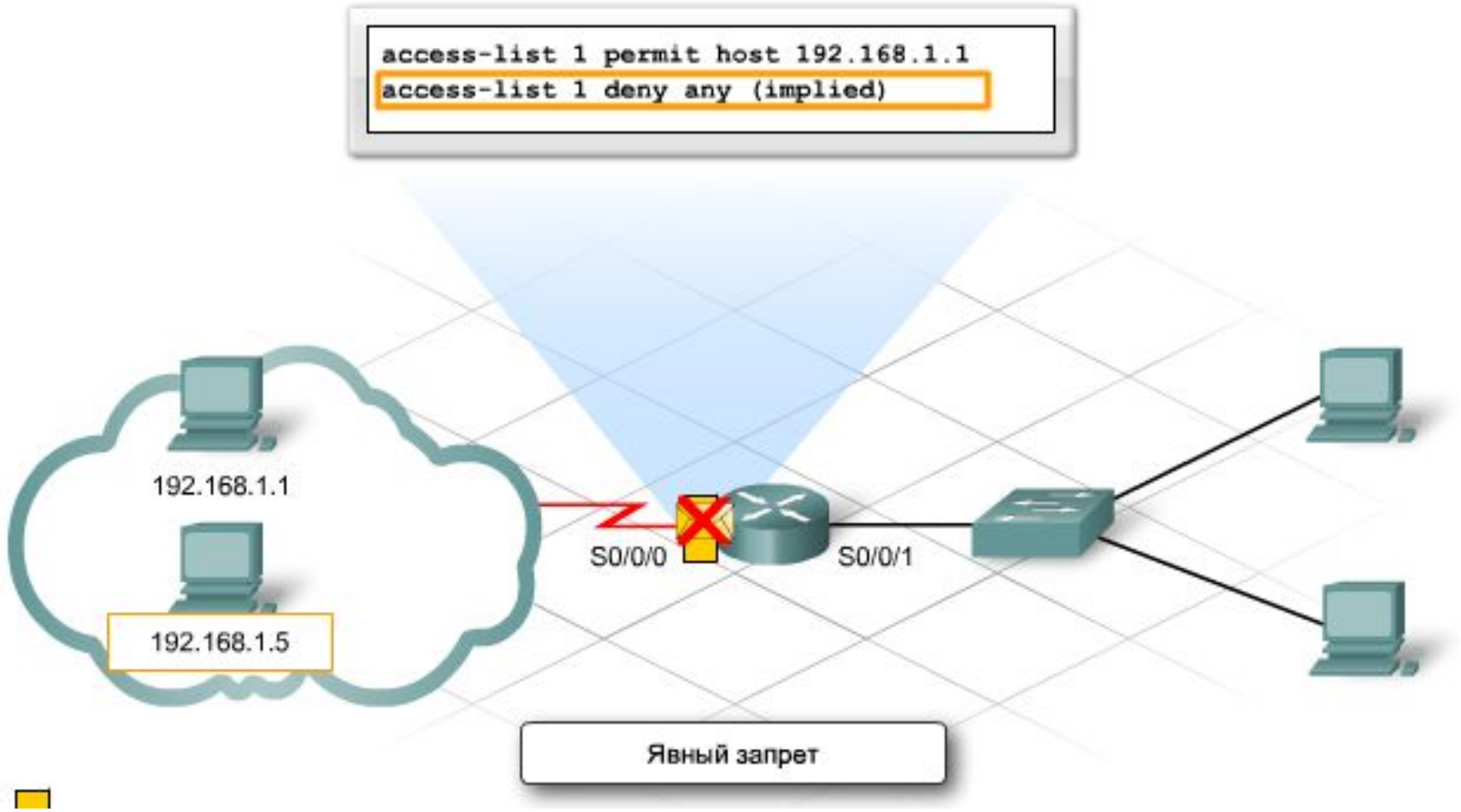
- Расширенные ACL-списки используются для фильтрации не только по исходному IP-адресу, но и по конечному IP-адресу, протоколу и номерам портов. Расширенным ACL-спискам присваиваются номера из диапазона от 100 до 199 и от 2 000 до 2 699.

Типы ACL-списков

- Именованные ACL-списки (NACL-списки) имеют формат стандартного или расширенного списка и обозначаются описательным именем, а не номером. При настройке именованных ACL-списков, маршрутизатор IOS использует режим подкоманды NACL.

Типы списков доступа IOS

Тип ACL-списка	Пример команды/инструкции ACL-списка	Назначение инструкции
Стандартный	`Router(config)#access-list 1 permit host 172.16.2.88`	• Разрешает конкретный IP-адрес
Расширенный	`Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet`	• Запрещает доступ из подсети 172.16.2.0/24 к любому другому узлу с помощью telnet
Именованный	`Router(config)#ip access-list standard permit-ip` `Router(config-ext-nacl)#permit host 192.168.5.47`	• Создает стандартный список доступа с именем permit-ip • Разрешает доступ с IP-адреса 192.168.5.47 • Первая команда переводит маршрутизатор в режим подкоманд NACL-списка.


access-list 1 permit host 192.168.1.1
access-list 1 deny any (implied)
192.168.1.1
192.168.1.5
S0/0/0
S0/0/1
Явный запрет

Входящий и исходящий списки доступа

- Администратор может использовать входящий или исходящий ACL-список для интерфейса маршрутизатора. Входящее или исходящее направление всегда рассматривается с точки зрения маршрутизатора. Трафик, поступающий через интерфейс, является ***входящим***, а отправляемый через интерфейс – ***исходящим***.

- При получении пакета по интерфейсу, маршрутизатор проверяет следующие параметры:
  - наличие ACL-списка, связанного с интерфейсом;
  - определение типа ACL-списка (входящий/исходящий);
  - определение соответствия трафика разрешающим или запрещающим условиям.

- ACL-список, применяемый как исходящий к интерфейсу, не действует для входящего трафика по тому же интерфейсу.

- Для каждого интерфейса маршрутизатор может иметь один ACL-список для одного направления по каждому сетевому протоколу. Для IP-протокола, один интерфейс может иметь один входящий ACL-список и один исходящий ACL-список одновременно.

Диапазон адресов в списках контроля доступа

- В простых ACL-списках указывается только один разрешенный или запрещенный адрес. Для блокирования нескольких адресов или диапазонов адресов необходимо несколько инструкций или групповая маска.

- Групповая маска определяет, сколько бит входящего IP-адреса соответствуют сравниваемому адресу.

Групповая маска, разрешающая одиночный узел:

```
172.16.22.87 0.0.0.0
host 172.22.8.17
```

Групповая маска, разрешающая диапазон узлов сети /24:

```
172.16.22.0 0.0.0.255
```

Групповая маска, разрешающая все узлы сети /16:

```
172.16.0.0 0.0.255.255
```

Групповая маска, разрешающая все узлы сети /8:

```
10.0.0.0 0.255.255.255
```

```
R1(config)#access-list 1 permit  192.168.1.0  0.0.0.255
```

	Десятичный эквивалент	Двоичный эквивалент
Адрес сравнения:	192.168.1.0	11000000.10101000.00000001.00000000
Групповая маска:	0.0.0.255	00000000.00000000.00000000.11111111
Биты адреса сравнения для сопоставления:	192.168.1.X	11000000.10101000.00000001.XXXXXXXX
Адрес входящего пакета:	192.168.1.27	11000000.10101000.00000001.00011011

Если эти биты совпадают, пакет разрешается данным ACL-списком

IP-адрес входящего пакета совпадает с адресом сравнения и битами групповой маски

Параметры host и any

- Для фильтрации одного, определенного узла, используйте групповую маску 0.0.0.0 после IP-адреса или параметр **host** перед IP-адресом.

  R1(config)#access-list 9 deny 192.168.15.99 0.0.0.0

  Соответствует следующему:

  R1(config)#access-list 9 deny host 192.168.15.99

- Для фильтрации всех узлов используйте групповую маску 255.255.255.255. Другим способом фильтрации всех узлов является использование параметра **any**.

  R1(config)#access-list 9 permit 0.0.0.0 255.255.255.255

  Соответствует следующему:

  R1(config)#access-list 9 permit any

Фильтрация трафика сети, разбитой на подсети

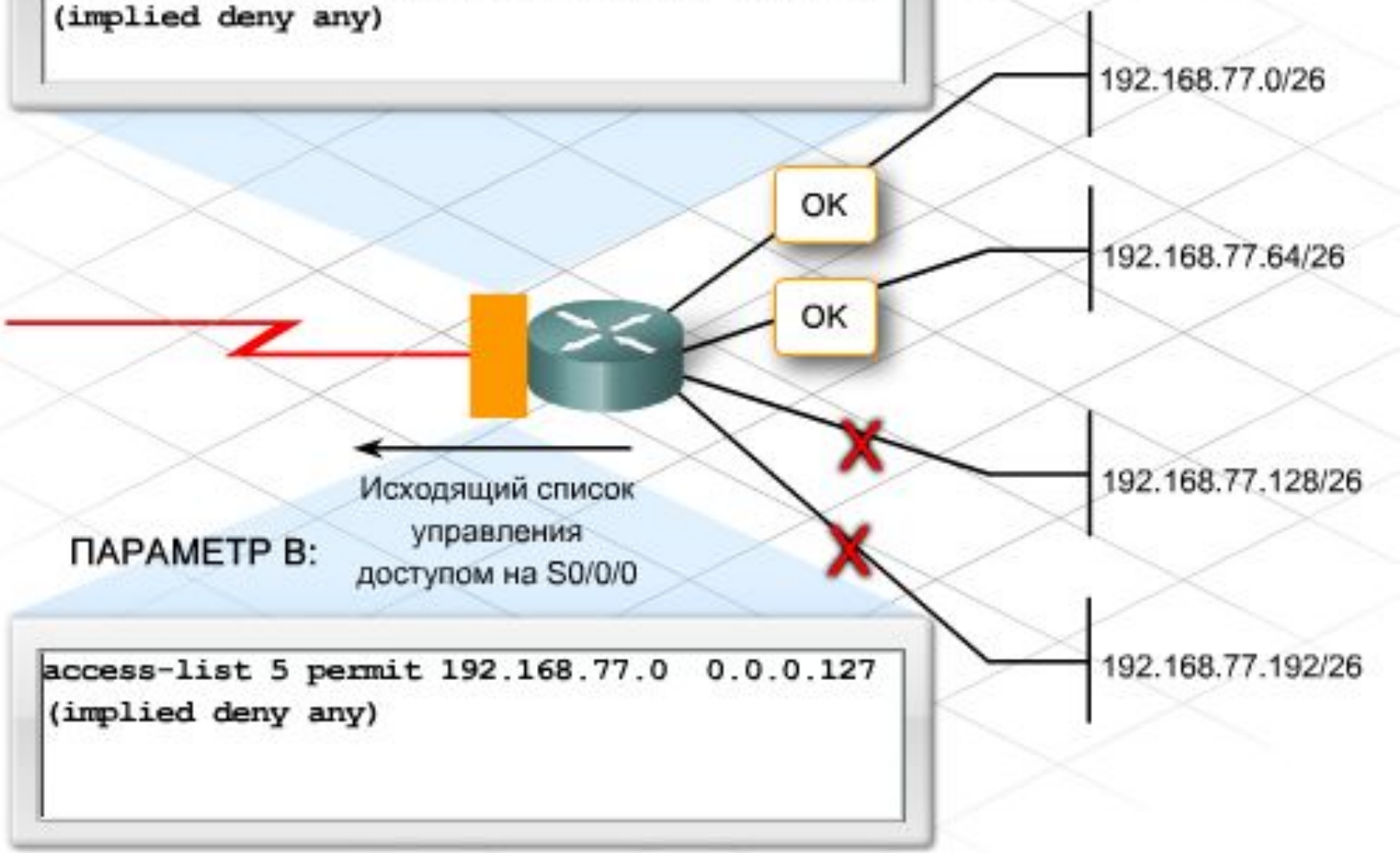
- Сеть 192.168.77.0 с маской подсети 255.255.255.192 или /26 образует следующие четыре подсети:
  - 192.168.77.0/26
  - 192.168.77.64/26
  - 192.168.77.128/26
  - 192.168.77.192/26

- Чтобы разрешить трафик с первых двух из этих подсетей, используйте следующие две инструкции ACL-списка:
  - **access-list 55 permit 192.168.77.0 0.0.0.63**
  - **access-list 55 permit 192.168.77.64 0.0.0.63**

- Первые две сети в сумме образуют 192.168.77.0/25. В результате вычитания суммированной маски подсети 255.255.255.128 из значений 255 маски получается групповая маска 0.0.0.127. Использование этой маски позволяет объединить эти две подсети в одной инструкции ACL-списка вместо двух.
  - **access-list 5 permit 192.168.77.0 0.0.0.127**

ПАРАМЕТР A:

```
access-list 55 permit 192.168.77.0  0.0.0.63
access-list 55 permit 192.168.77.64 0.0.0.63
(implied deny any)
```



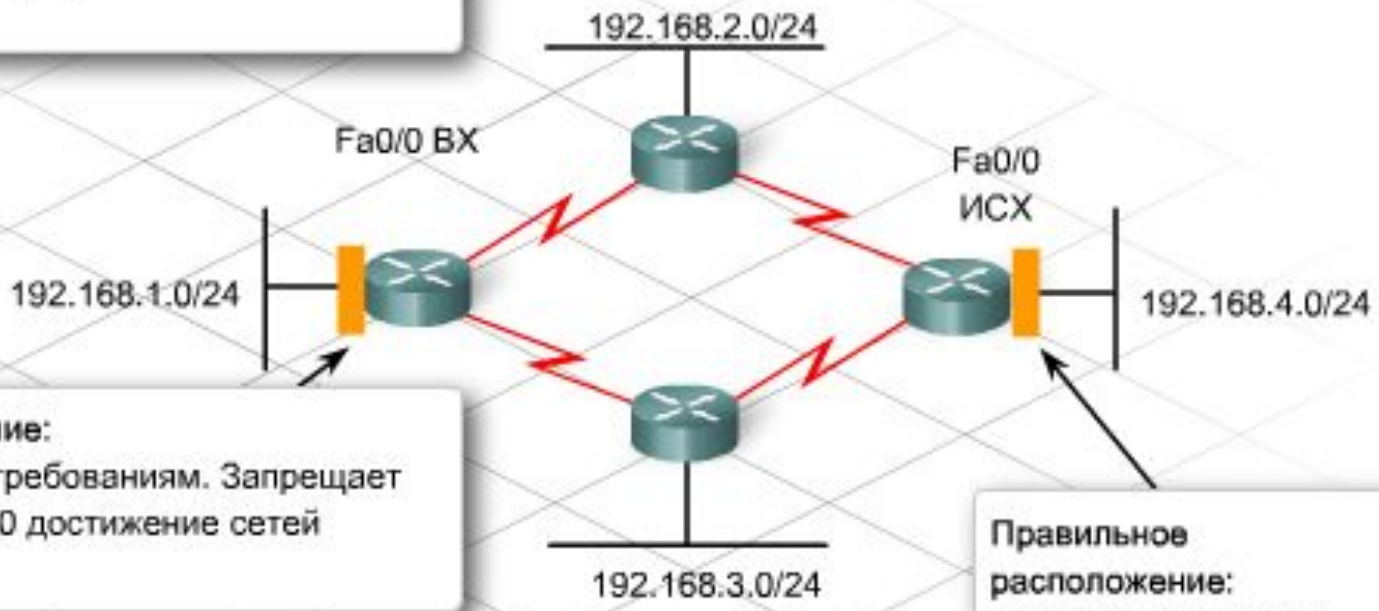
ПАРАМЕТР B:

```
access-list 5 permit 192.168.77.0  0.0.0.127
(implied deny any)
```

Планирование списка контроля доступа

- Этап планирования включает следующие действия:
  - Определение требований к фильтрации трафика.
  - Выбор типа ACL-списка, наилучшим образом отвечающего требованиям:
    - важно размещать стандартные ACL-списки как можно ближе к конечному узлу;
    - важно разместить расширенный ACL-список ближе к исходному адресу.
  - Определение маршрутизатора и интерфейса, для которого будет использоваться ACL-список.
  - Выбор направления фильтрации трафика.

Требования:
запретите трафику из сети 192.168.1.0 вход в сеть 192.168.4.0. Разрешите трафику 192.168.1.0 достижение других сетей.

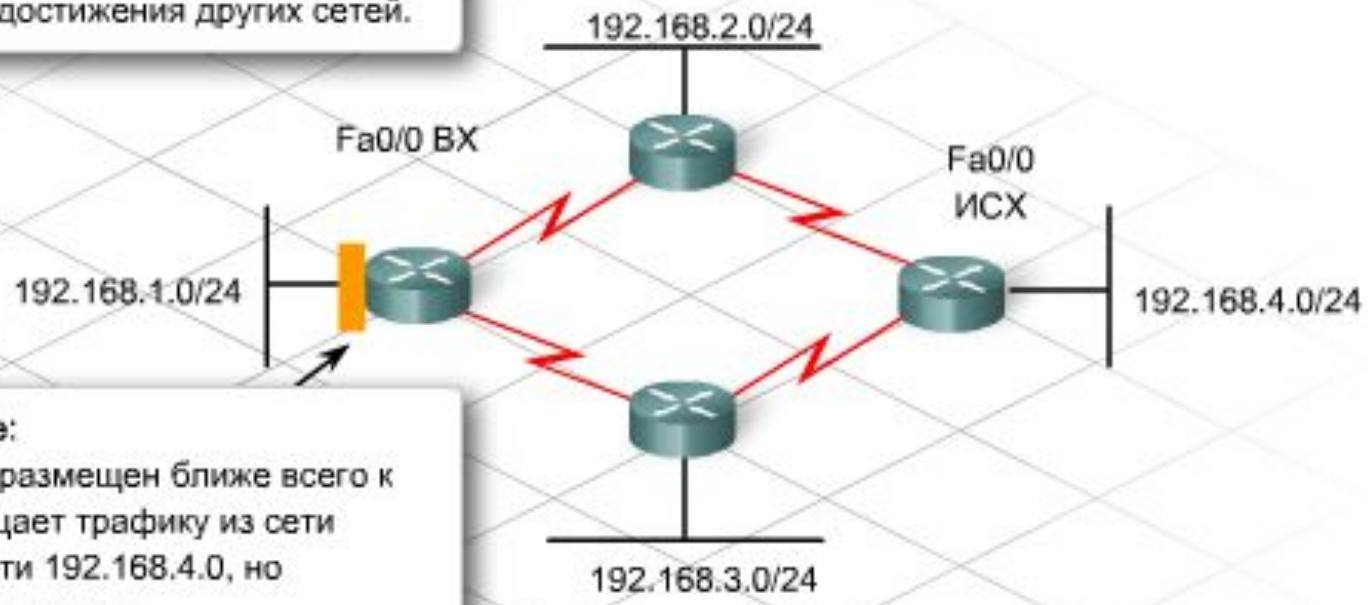


Неправильное расположение:
соответствует некоторым требованиям. Запрещает трафику из сети 192.168.1.0 достижение сетей 192.168.2.0 и 192.168.3.0.

Правильное расположение:
соответствует всем требованиям.

```
ACL
access-list 9 deny 192.168.1.0  0.0.0.255
access-list 9 permit  any
```

Требования:
используйте расширенный ACL-список для запрещения трафику из сети 192.168.1.0 входа в сеть 192.168.4.0 и разрешения достижения других сетей.



Правильное расположение:
расширенный ACL-список размещен ближе всего к источнику, который запрещает трафику из сети 192.168.1.0 достижение сети 192.168.4.0, но разрешает ему вход в другие сети.

```
ACL
access-list 109 deny ip 192.168.1.0  0.0.0.255   192.168.4.0  0.0.0.255
access-list 109 permit ip any any
```

Направление фильтрации трафика

- **Входящий трафик** – это трафик, поступающий в интерфейс маршрутизатора извне. Маршрутизатор сравнивает входящий пакет с ACL-списком перед поиском целевой сети в таблице маршрутизации. Пакеты, отбрасываемые в этой точке, позволяют исключить излишние операции поиска маршрутизатора.

- **Исходящий трафик** проходит через маршрутизатор по интерфейсу. Для исходящего пакета маршрутизатор уже осуществил поиск по таблице маршрутизации и переключил пакет на правильный интерфейс. Пакет сравнивается с ACL-списком непосредственно перед выходом из маршрутизатора.

Создание ACL-списка

- Синтаксис стандартного ACL-списка следующий:
  access-list [номер-списка-доступа] [deny|permit] [исходный адрес] [исходная-групповая маска][log]

- Поскольку каждый пакет сравнивается с инструкцией ACL-списка до нахождения совпадения, порядок размещения инструкций в ACL-списке может влиять на создаваемое запаздывание.

- Для описания функции каждого раздела или инструкции ACL-списка используйте команду **remark**:
  access-list [номер списка] remark [текст]

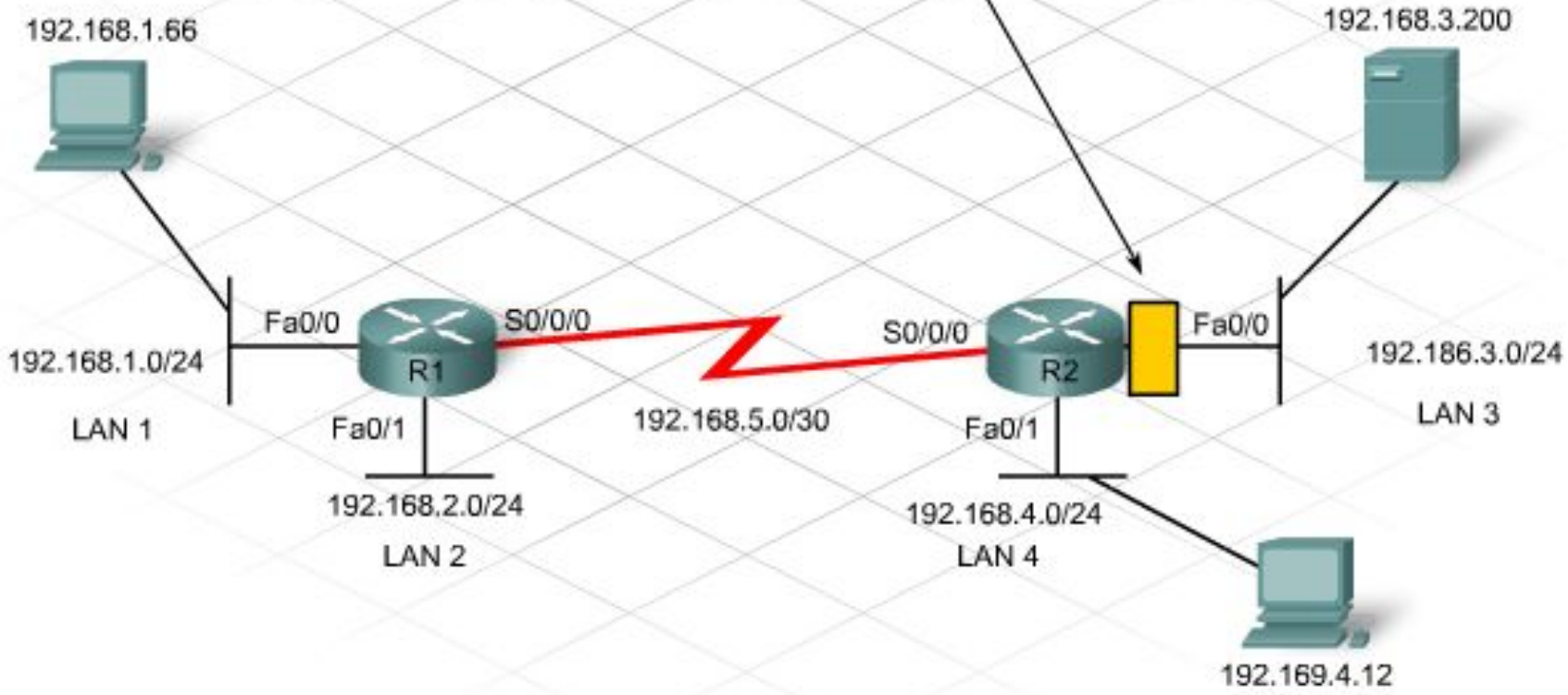
- Для удаления ACL-списка используйте следующую команду:
  no access-list [номер списка]

- Из стандартного или расширенного ACL-списка нельзя удалить одну строку. Вместо этого ACL-список удаляется полностью и его необходимо заменить.

```
R2(config)#access-list 3 remark Access to departmental server
R2(config)#access-list 3 deny host 192.168.4.12
R2(config)#access-list 3 permit 192.168.4.0 0.0.0.255
R2(config)#access-list 3 permit 192.168.1.66
```

Конкретные

Общие



Применение ACL-списка

- Присвойте ACL-список одному или более интерфейсам, указав входящий или исходящий трафик. Применяйте стандартный ACL-список как можно ближе к конечному адресу.

  R2(config-if)#ip access-group номер списка доступа [in | out]

- Следующие команды позволяют поместить список доступа access-list 5 для интерфейса Fa0/0 маршрутизатора R2 с фильтрацией входящего трафика:

  R2(config)#interface fastethernet 0/0

  R2(config-if)#ip access-group 5 in

- По умолчанию в ACL-списке к интерфейсу применяется **out** направление.

- Чтобы удалить ACL-список из интерфейса без изменения самого ACL-списка, используйте команду **no ip access-group interface**.

Проверка списка контроля доступа

- **show ip interface** – эта команда выводит сведения об IP-интерфейсе с указанием любых присвоенных ACL-списков.

- **show access-list [номер списка доступа]** – эта команда позволяет вывести содержимое всех ACL-списков маршрутизатора. Эта команда также выводит на экран число совпадений по каждой разрешающей или запрещающей инструкции с момента применения ACL-списка. Чтобы вывести определенный список, добавьте имя ACL-списка или номер в качестве параметра команды.

- **show running-config** – эта команда выводит на экран все настроенные ACL-списки маршрутизатора, даже если они в данный момент не применены к интерфейсу.

Настройка нумерованных расширенных ACL-списков

- Для расширенных ACL-списков используется номер списка доступа из диапазонов от 100 до 199 и от 2000 до 2699. Правила, действующие для стандартных ACL-списков, также действительны для расширенных ACL-списков:
  - в одном ACL-списке следует указывать несколько инструкций;
  - каждая инструкции должна иметь один и тот же номер ACL-списка;
  - для представления IP-адресов следует использовать ключевые слова host или any.

- Основным отличием синтаксиса расширенного ACL-списка является необходимость указывать протокол после условия разрешения или запрещения. Это может быть IP-протокол с указанием всего IP-трафика или определением фильтрации определенного IP-протокола, такого как TCP, UDP, ICMP и OSPF.

Пример

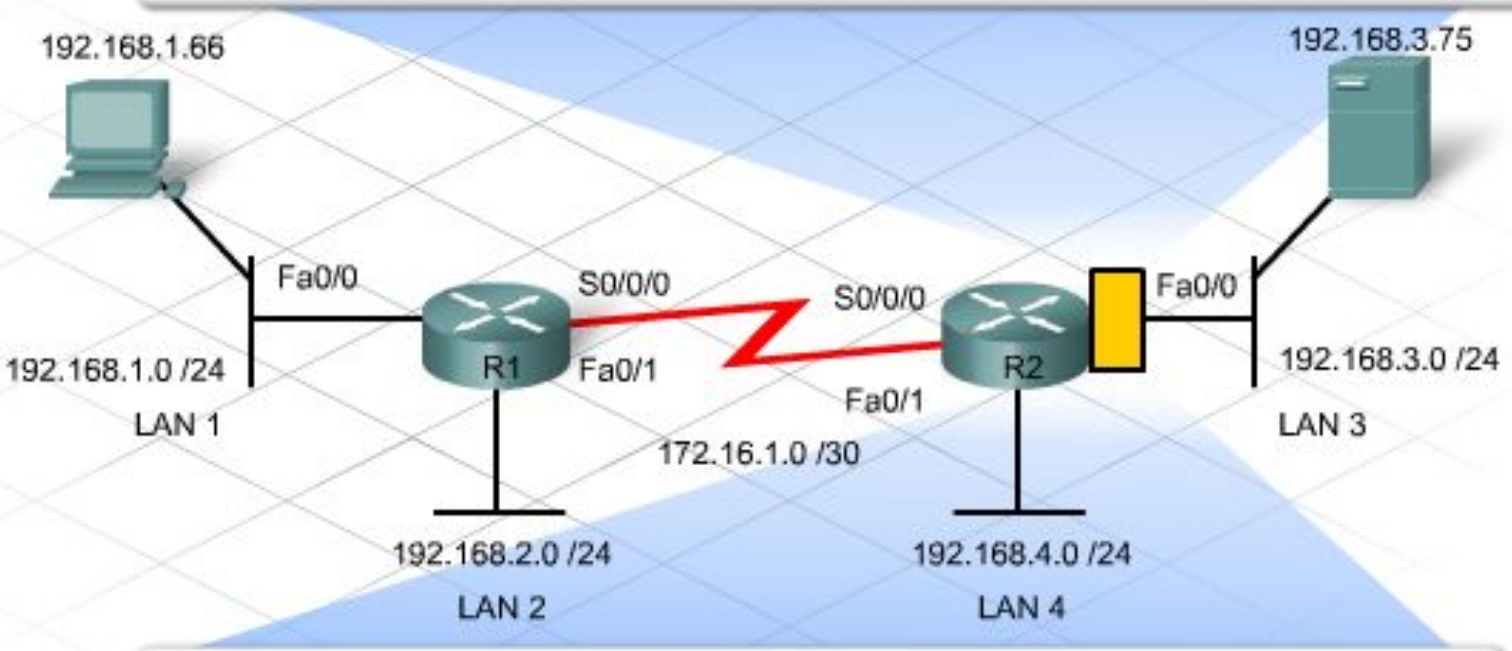
- Например, в компании есть сервер с адресом 192.168.3.75. Установлены следующие требования:
  - разрешать доступ к узлам в локальной сети 192.168.2.0;
  - разрешать доступ к узлу 192.168.1.66;
  - блокировать доступ к узлам в локальной сети 192.168.4.0;
  - разрешать доступ к остальным адресам в компании.

- В качестве вариантов уменьшения числа инструкций и сокращения нагрузки на обработку маршрутизатором можно привести следующие:
  - необходимо обеспечить выявление проходного трафика большого объема и запрет блокируемого трафика в начальных инструкциях по ACL-списку;
  - объединение нескольких разрешающих и запрещающих инструкций в одну инструкцию при помощи диапазонов;
  - старайтесь блокировать доступ определенной группы вместо того, чтобы разрешать его другой группе из большего числа пользователей.

Вариант A:

```
R2(config)#access-list 103 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.75
R2(config)#access-list 103 permit ip host 192.168.1.66 host 192.168.3.75
R2(config)#access-list 103 deny ip 192.168.4.0 0.0.0.255 host 192.168.3.75
R2(config)#access-list 103 permit ip any any

R2(config)#interface fa0/0
R2(config-if)#ip access-group 103 out
```



Вариант B:

```
R2(config)#access-list 103 deny 192.168.4.0 0.0.0.255 host 192.168.3.75
R2(config)#access-list 103 permit ip any any

R2(config)#interface fa0/0
R2(config-if)#ip access-group 103 out
```

Настройка именованных ACL-списков

- Для создания именованного ACL-списка используется следующая команда:

  ip access-list {standard | extended} name

- Именованный ACL-список применяется к интерфейсу аналогичным применению стандартного и расширенного ACL-списка образом.

```
R1(config)#ip access-list extended SALES-ONLY
R1(config-ext-nacl)#permit ip 192.168.1.66 0.0.0.0 any
R1(config-ext-nacl)#permit ip 192.168.1.77 0.0.0.0 any

R1(config)#interface fa0/0
R1(config-if)#ip access-group SALES-ONLY in
```

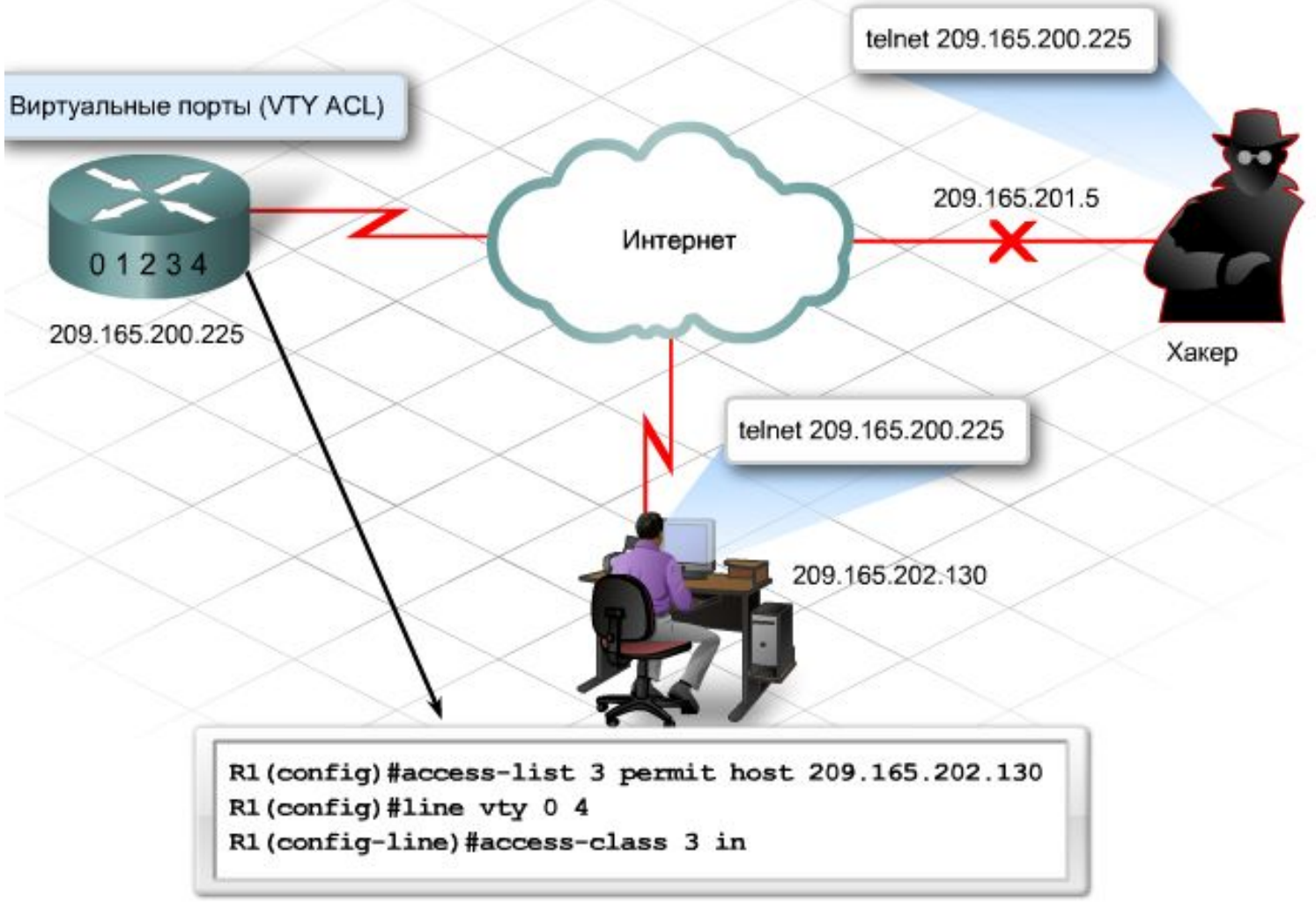
Редактирование списка контроля доступа

- В текущих версиях IOS для редактирования нумерованных и именованных ACL-списков используется команда ip access-list. ACL-список выводится со строками с нумерацией 10, 20, 30 и так далее. Для просмотра номеров строк используется следующая команда:

  show access-lists

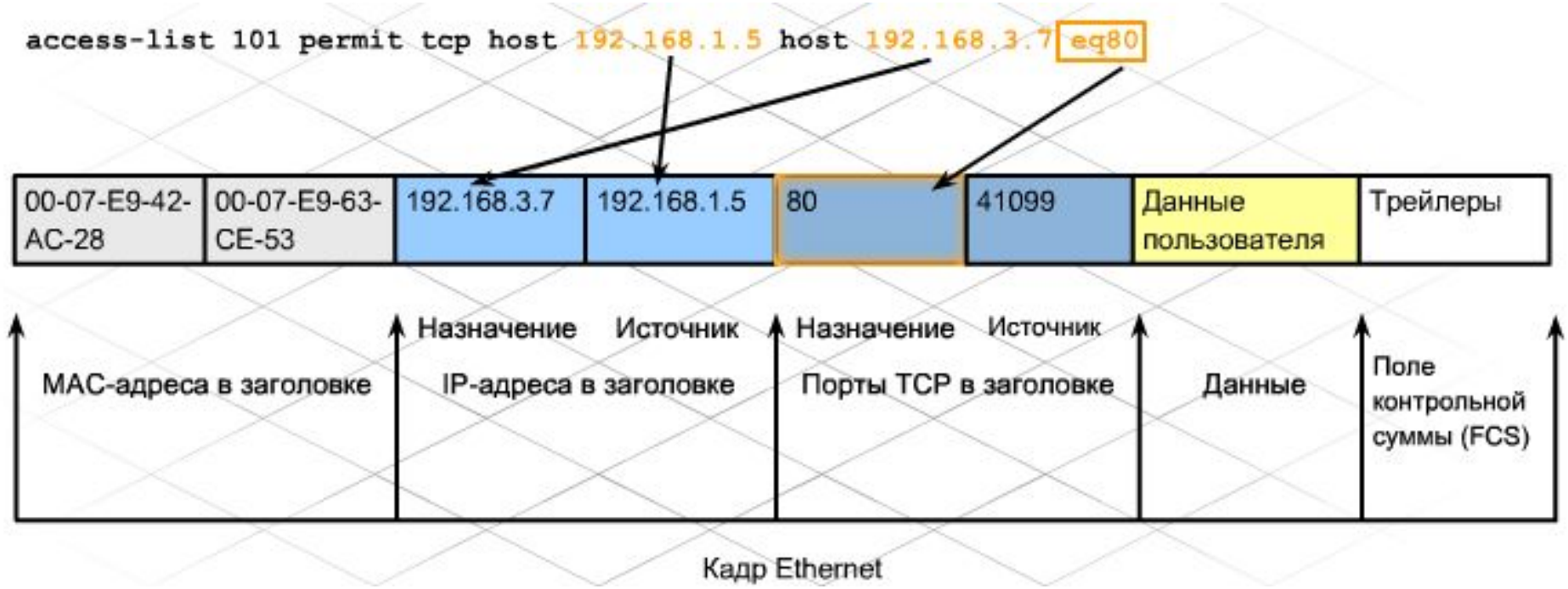
- Чтобы изменить существующую строку, выполните следующие действия:
  - удалите строку при помощи команды no line number;
  - повторно добавьте эту же строку с ее номером;
  - чтобы вставить новую строку между существующими строками 20 и 30, проделайте следующее:
  - используйте инструкцию new ACL с начальным номером между номерами существующих строк, например, 25.

Настройка доступа к VTY маршрутизатору



Настройка фильтрации определенных видов портов

- Расширенные ACL-списки также используются для фильтрации по номерам конечных портов.
- Помимо указания номеров портов, необходимо определить условие, прежде чем произойдет совпадение с инструкцией. Чаще всего используются следующие аббревиатуры:
  - eq - равно;
  - gt - больше;
  - lt - меньше.



Настройка списков для поддержания установленного трафика

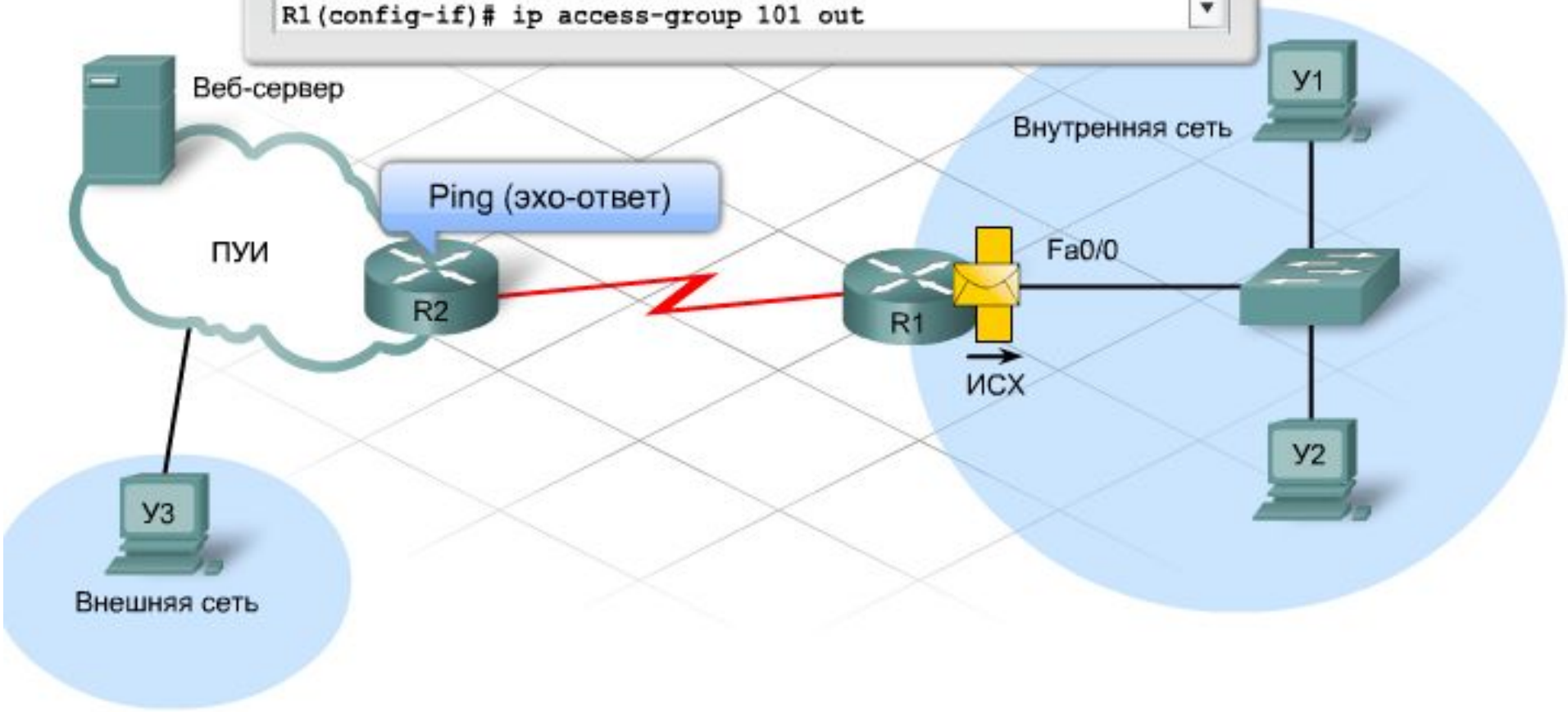
- Можно создать отдельную инструкцию, разрешающую внутренним пользователям устанавливать TCP-сеанс с внешними ресурсами. После трехстороннего подтверждения TCP и установления подключения все пакеты, передаваемые между двумя устройствами, будут разрешены. Для этого необходимо использовать следующее ключевое слово: **established**.

access-list 101 permit tcp any any established

Настройка списков для поддержания установленного трафика

```
R1(config)#access-list 101 permit tcp any any established
R1(config)#access-list 101 permit icmp any any echo-reply
R1(config)#access-list 101 permit icmp any any unreachable
R1(config)#access-list 101 deny any any

R1(config)# interface fa0/0
R1(config-if)# ip access-group 101 out
```



Влияние NAT и PAT на размещение списка

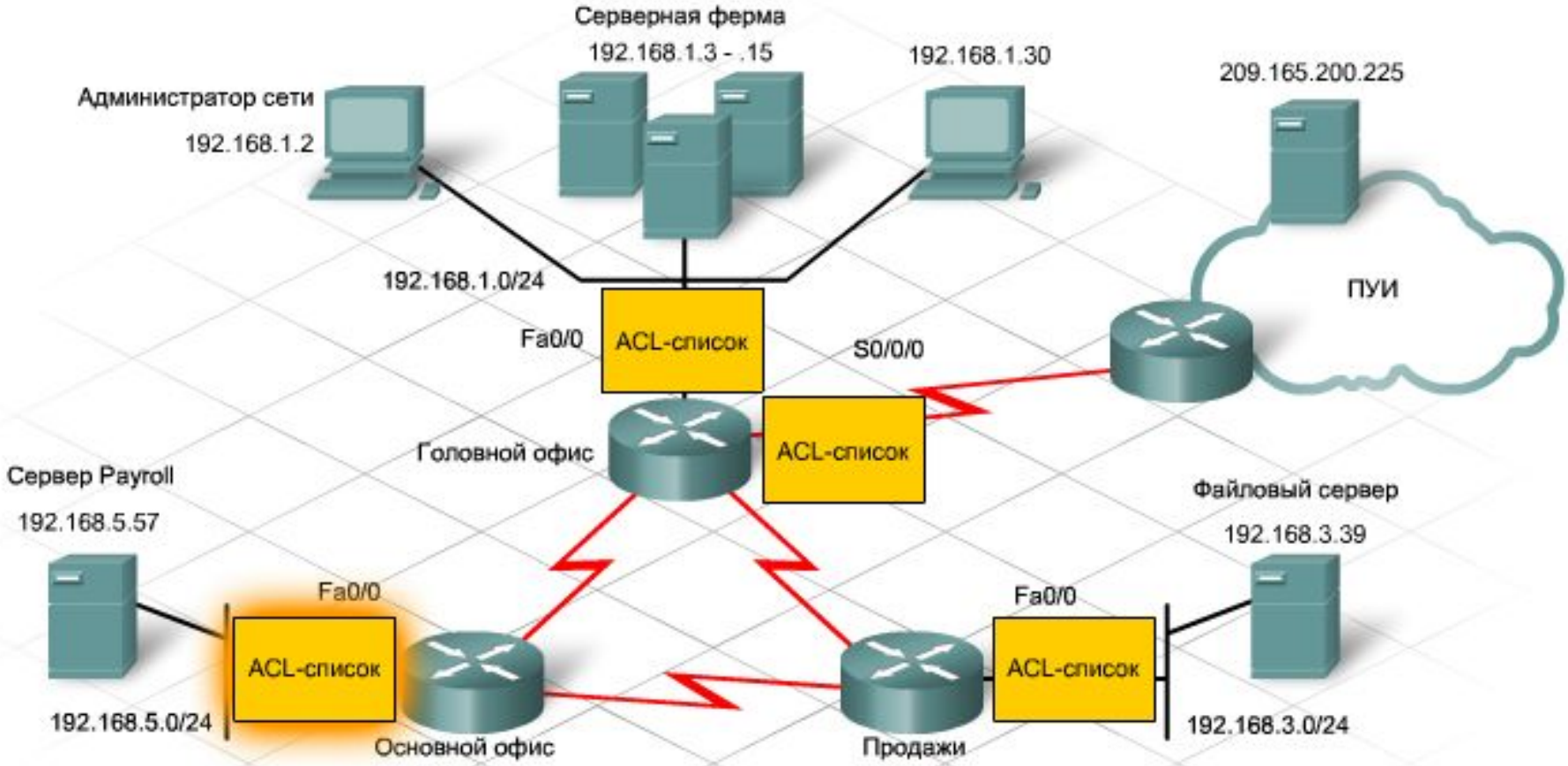
- При поступлении входящего пакета в NAT за пределами интерфейса, маршрутизатор выполняет следующее:
  - применяется входящий ACL-список;
  - конечный адрес преобразовывается из внешнего во внутренний или из глобального в локальный;
  - происходит маршрутизация пакета.

- При поступлении исходящего пакета через NAT за пределами интерфейса, маршрутизатор выполняет следующее:
  - исходный адрес преобразовывается из внутреннего во внешний или из локального в глобальный;
  - применяется исходящий ACL-список.

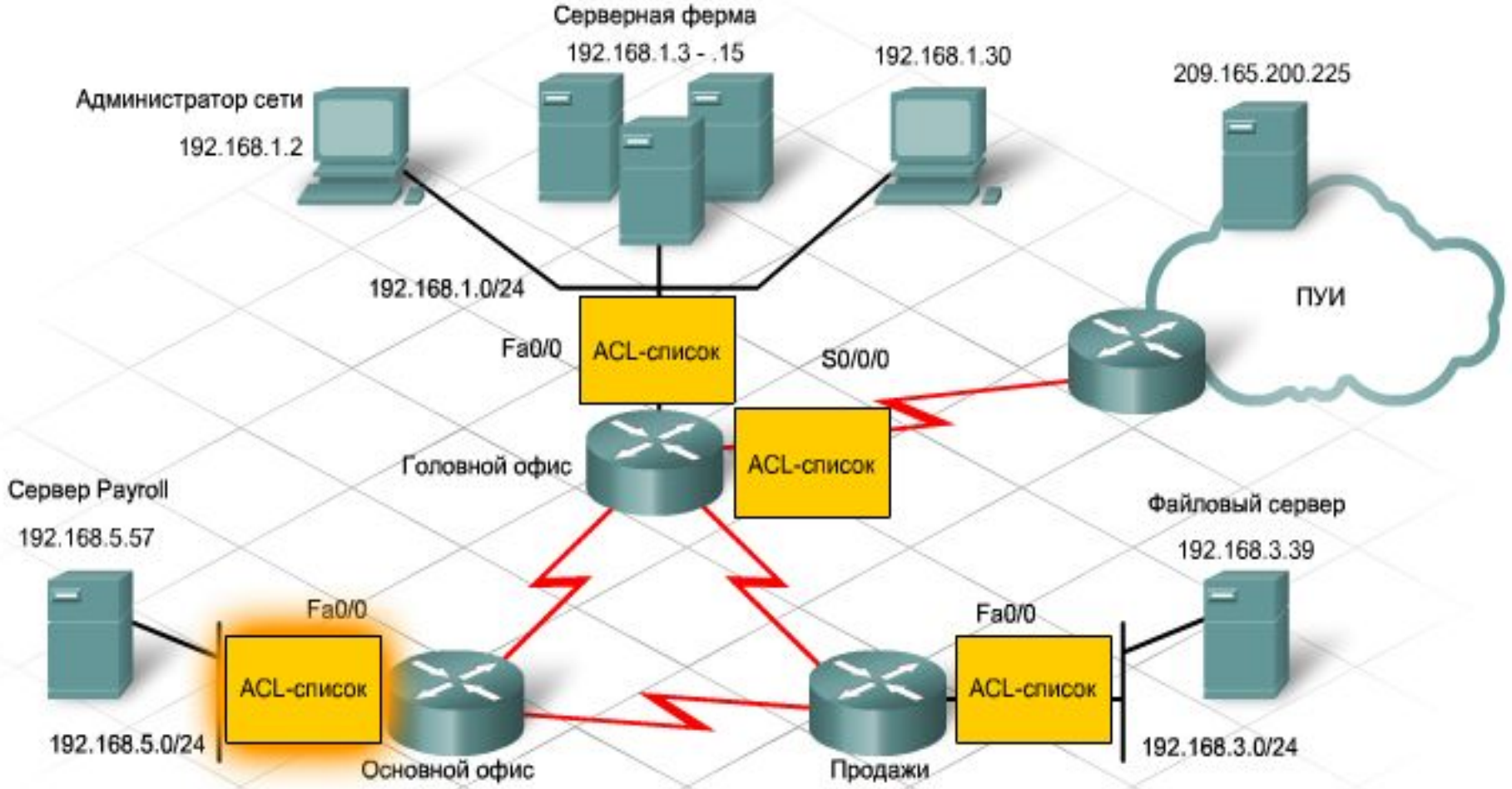
Анализ списков и их размещение

- Администраторы должны проверить ACL-список, строка за строкой, и ответить на следующие вопросы:
  - Какой службе инструкция запрещает доступ?
  - Исходный и конечный адрес.
  - Какие номера портов блокируются?
  - Что произойдет, если ACL-список перенести на другой интерфейс?
  - Что произойдет, если фильтровать трафик по ACL-списку в другом направлении?
  - Заключается ли проблема в NAT?

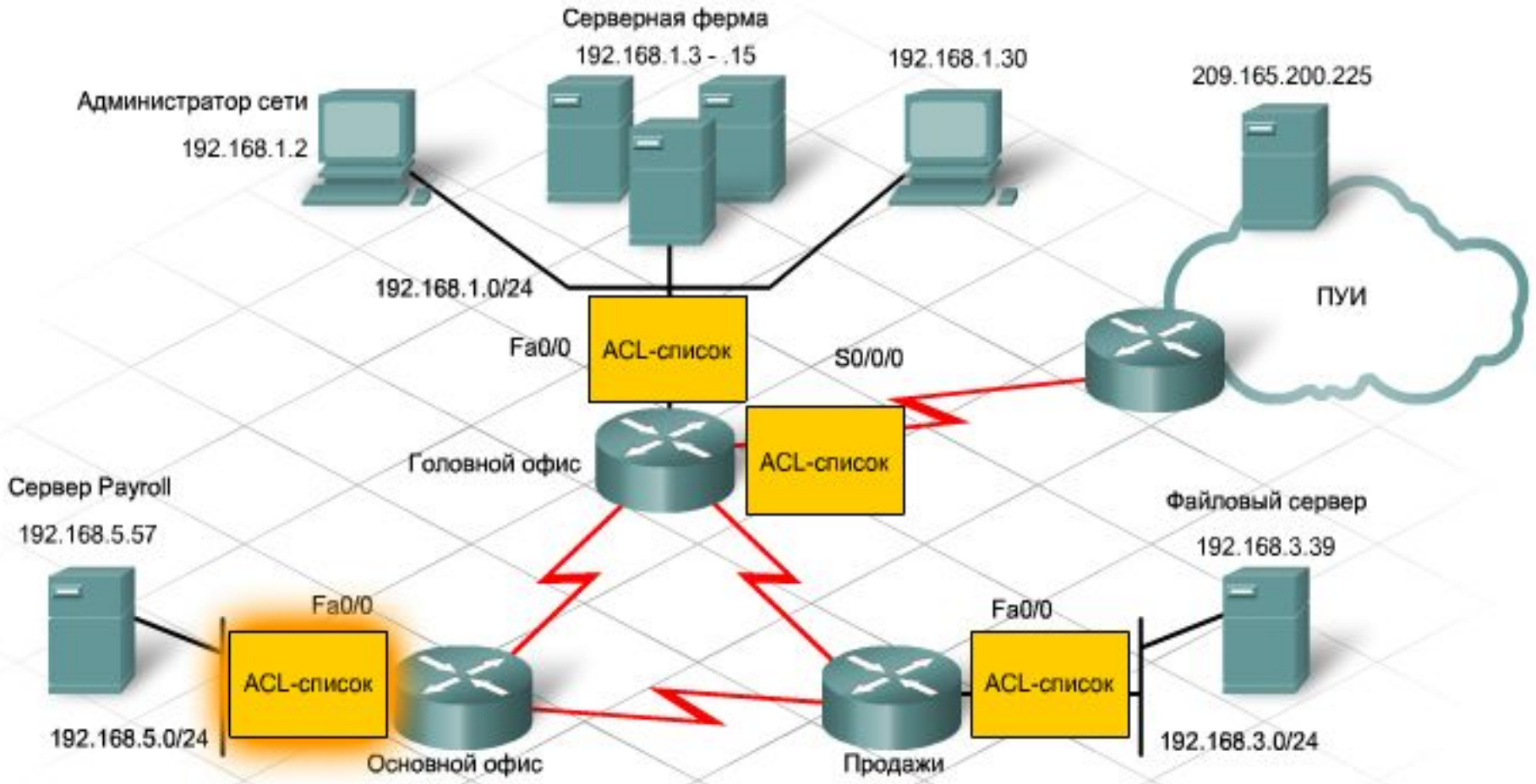
- При оценке расширенного ACL-списка важно помнить о следующих ключевых моментах:
  - ключевое слово tcp разрешает или запрещает протоколы, такие как FTP, HTTP, Telnet и т.д.;
  - ключевая фраза permit ip используется для разрешения всего IP-трафика, включая протоколы TCP, UDP и ICMP.



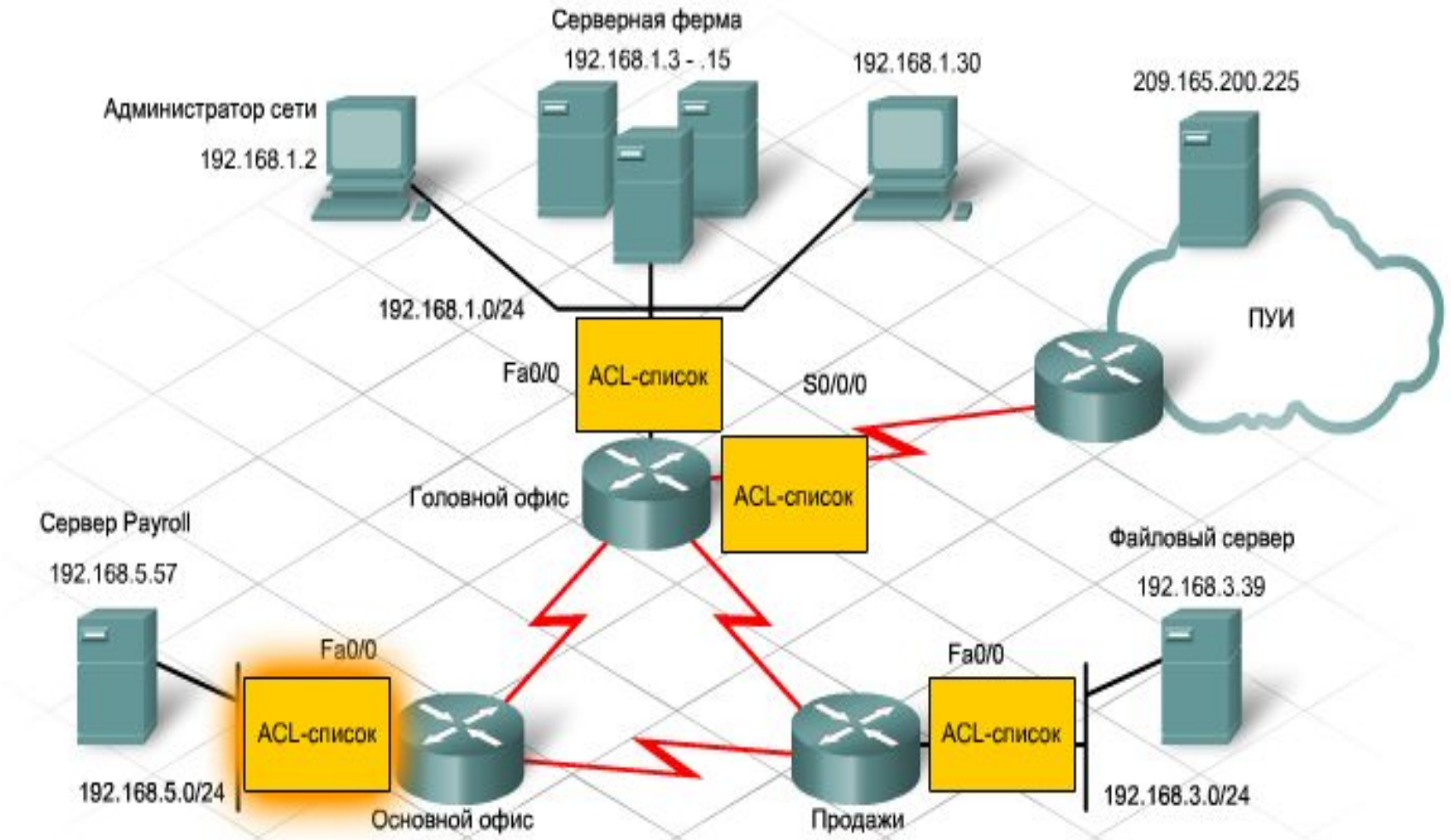
Основной офис — расширенный ACL-список 111 – входящий интерфейс Fa0/0	
Access-list 111 permit ip host 192.168.5.57 any	Разрешает серверу Payroll доступ к любому адресу
Access-list 111 permit udp 192.168.5.0 0.0.0.255 any eq 53	Разрешает всем пользователям в этой сети доступ к удаленной DNS
Access-list 111 permit tcp 192.168.5.0 0.0.0.255 any eq 80	Разрешает всем пользователям в этой сети доступ к веб-службам



Головной офис — расширенный ACL-список 100 – входящий интерфейс Fa0/0	
Access-list 100 permit ip 192.168.1.0 0.0.0.15 any	Разрешает полный доступ ферме серверов и администратору сети
Access-list 100 deny tcp 192.168.1.0 0.0.0.255 eq 23	Запрещает доступ по Telnet пользователям ПК
Access-list 100 permit ip any any	Разрешает весь остальной трафик



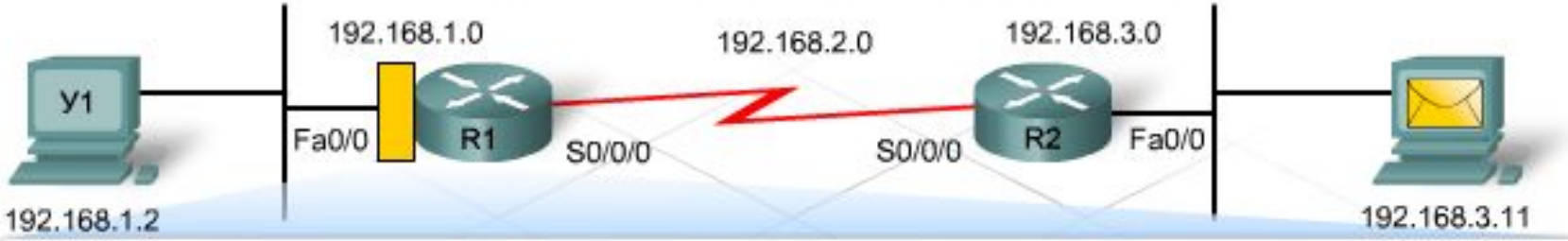
Головной офис — расширенный ACL-список 105 – входящий интерфейс S0/0/0	
Access-list 105 permit icmp any any echo-reply	Разрешает возвращение из Интернета эхо-ответов
Access-list 105 permit icmp any any unreachable	Разрешает возвращение из Интернета сообщений об ошибках
Access-list 105 permit tcp any any established	Разрешает установленные сеансы TCP из Интернета



Продажи — расширенный ACL-список 122 – входящий интерфейс Fa0/0	
Access-list 122 deny ip 192.168.3.0 0.0.0.255 host 192.168.5.57	Запрещает доступ из этой сети к серверу Payroll
Access-list 122 permit udp 192.168.3.0 0.0.0.255 any range 20 21	Разрешает всем пользователям в этой сети доступ к данным FTP и управлению сеансом FTP
Access-list 122 permit udp 192.168.3.0 0.0.0.255 any eq 53	Разрешает всем пользователям в этой сети доступ к удаленной DNS
Access-list 122 permit tcp 192.168.3.0 0.0.0.255 any eq 80	Разрешает всем пользователям в этой сети доступ к веб-службам

Ведние журнала для проверки работоспособности списка

Источник	Назначение	
192.168.1.2	192.168.3.20	ICMP-протокол




```
R1(config)#no access-list 123
R1(config)#access-list 123 deny tcp host 192.168.1.2  host 192.168.3.11 eq 23 log
R1(config)#access-list 123 permit ip 192.168.1.0  0.0.0.255  any log
R1(config)#access-list 123 deny ip any any log
R1(config)#end
R1#

*Sep  9 20:02:11.979: %SEC-6-IPACCESSLOGP: list 123 permitted udp 192.168.1.2(2138)
192.168.3.11(30),  1 packet
R1#
*Sep  9 20:02:53.067: %SEC-6-IPACCESSLOGP: list 123 denied tcp 192.168.1.2(1141)
192.168.3.11(23), 1 packet
R1#
*Sep  9 20:03:48.279: %SEC-6-IPACCESSLOGDP: list 123 permitted icmp 192.168.1.2
192.168.3.20 (8/0), 1 packet
```

Ведение журнала

- Ведение журнала включается для отдельных инструкций ACL-списка. Чтобы задействовать эту возможность, добавьте параметр log в конец каждой инструкции ACL-списка, по которой необходимо вести учет.
- Ведение журнала в консоли требует больше памяти, которая бывает ограниченной. Вместо этого рекомендуется настроить маршрутизатор на отправку сообщений журнала на внешний сервер. Такие сообщения носят название syslog и могут просматриваться пользователем в реальном времени или позднее.
- Сообщения подразделяются на типы в зависимости от семи уровней серьезности: от уровня 0, представляющего критическое состояние или неработоспособность системы, до уровня 7, обозначающего информационные сообщения, например содержащие отладочную информацию.

Ведение журнала

- При ведении журнала ACL-списка, создается информационное сообщение со следующими сведениями:
  - номер ACL-списка;
  - разрешенный или запрещенный пакет;
  - исходный и конечный адреса;
  - число пакетов.

- Отключить ведение журнала можно при помощи следующей команды:

  no logging console

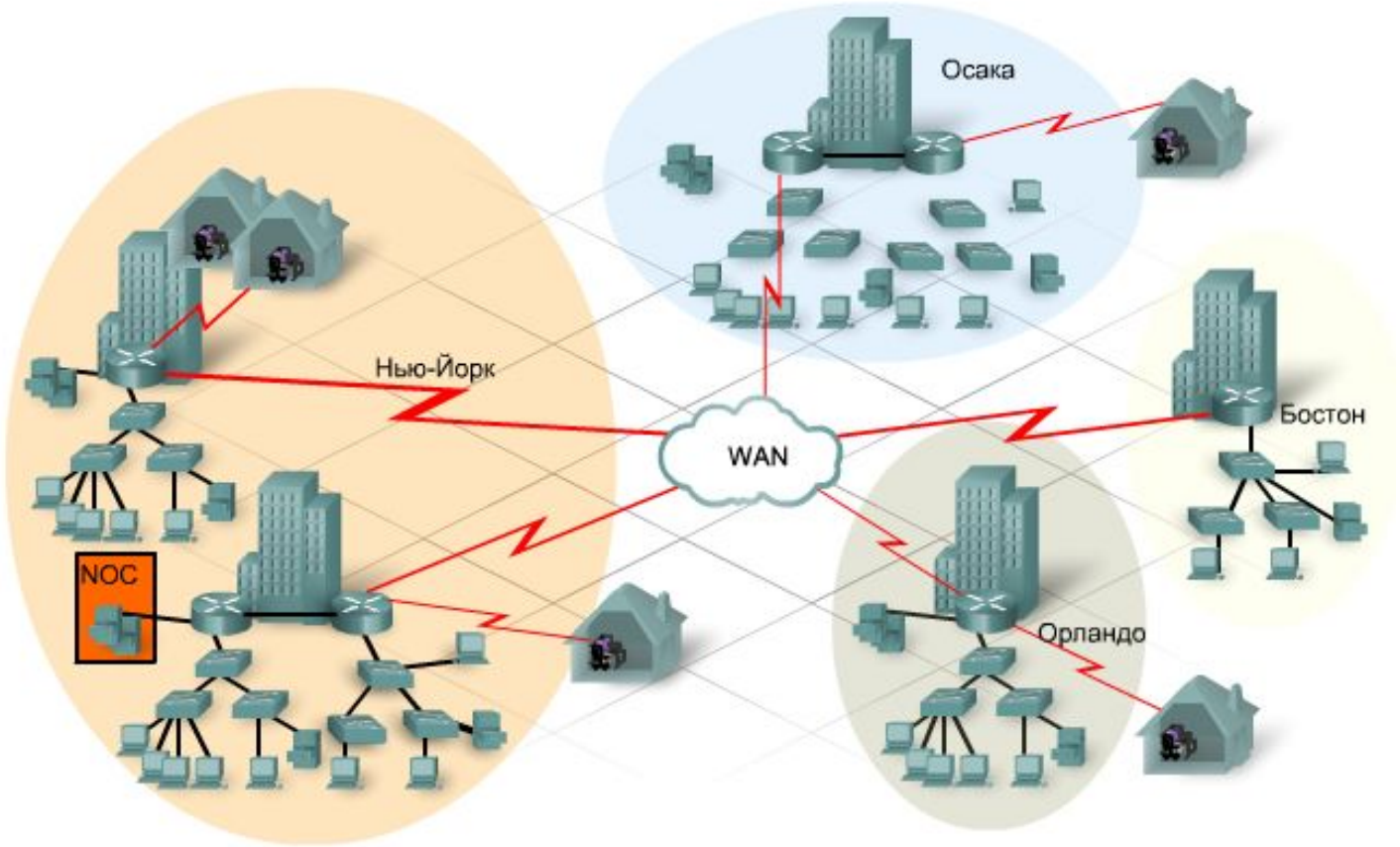
- Для полного отключения отладки следует использовать следующую команду:

  undebug all

- Чтобы отключить определенную отладку, например ip packet, потребуется следующая команда: **no debug ip packet**

Устройства сети WAN и технологии

- Расширение компании требует перехода от локальной сети (LAN) к использованию глобальной сети (WAN)
- Внутри локальной сети всеми кабельными соединениями, устройствами и службами администратор сети управляет на месте. Большинство организаций приобретают службы глобальной сети у поставщиков услуг WAN
- Наиболее распространенная технология локальной сети (LAN) — Ethernet. Технологии сети WAN заключаются в последовательной передаче данных

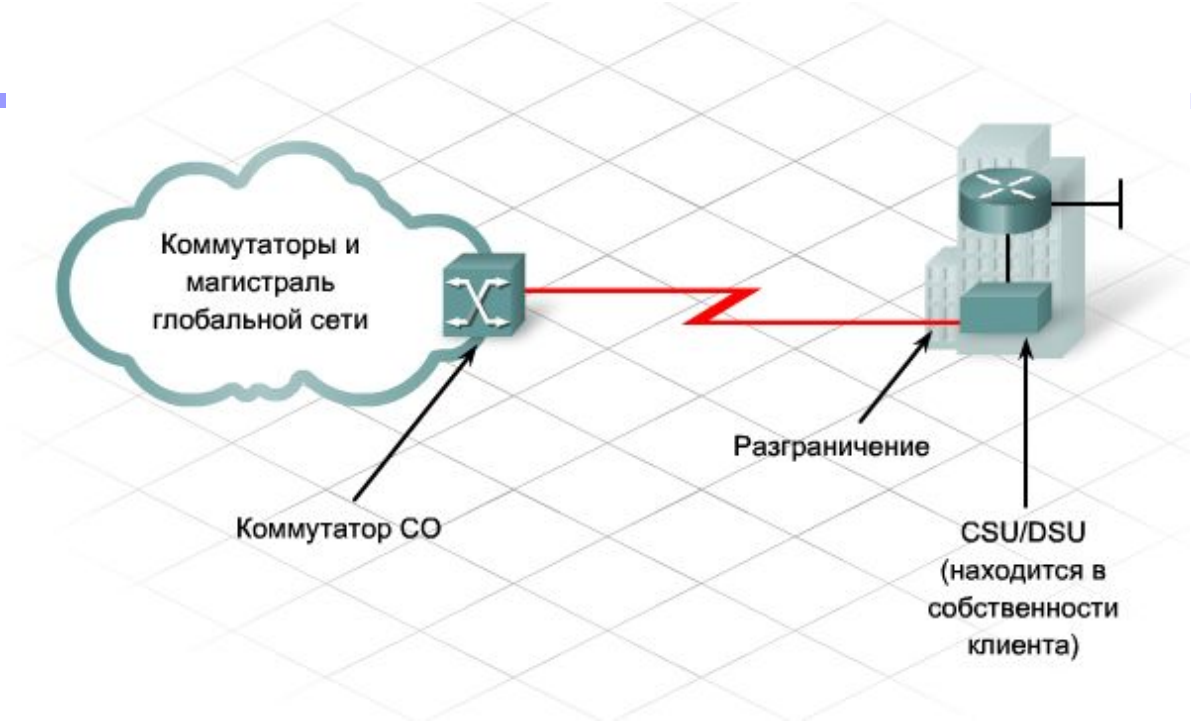


Устройства сети WAN и технологии

- Для обработки данных с целью передачи их по сети WAN с помощью цифровых каналов требуется
  - устройство обработки канала (**CSU**);
  - устройство обработки данных (**DSU**).
- При использовании аналогового соединения требуется модем.

- Точкой, в которой управление соединением и ответственность за него переходит от пользователя к поставщику услуг, является интерфейс сетевого окончания или **точка разграничения** (demarc — архитектура распределенного управления сетью масштаба предприятия).

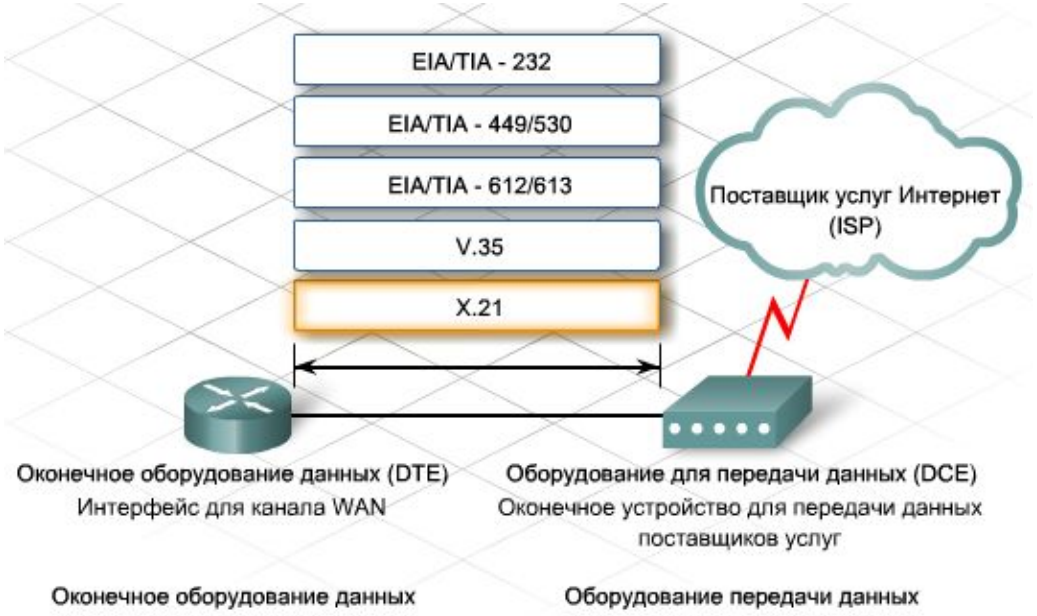
- Размещенное на стороне пользователя оборудование, независимо от его владельца, поставщики услуг называют телекоммуникационным оборудованием клиента (CPE).



- Центральным офисом является место, в котором находится оборудование поставщика услуг, обеспечивающее соединения для клиента.
- Для физического подключения телекоммуникационного оборудования клиента к маршрутизатору или коммутатору сети WAN в центральном офисе используется медный или оптоволоконный кабель – такое соединение называется местной линией связи или "последней милей". Со стороны пользователя, это соединение называется первой милей

Устройства сети WAN и технологии

- Устройство CSU/DSU является оборудованием передачи данных (**DCE**)
  - управляют скоростью передачи данных в местную линию
  - обеспечивают передачу сигнала синхронизации на маршрутизатор
- Маршрутизатор, отправляющий данные на оборудование передачи данных, называется оконечным оборудованием данных (**DTE**)



X.21

- Стандарт ITU-T для синхронной передачи цифровой информации
- Использует 15-контактный D-образный разъем.

V.35

- Стандарт ITU-T для синхронной передачи данных между сетевым устройством доступа и сетью с пакетной коммутацией со скоростью до 48 Кбит/сек
- Использует 34-контактный прямоугольный разъем

EIA/TIA - 612/613

- Обеспечивает доступ к сервисам на скорости до 52 Мбит/сек, использует 60-контактный D-образный разъем

EIA/TIA - 449/530

- Более быстрая (до 2 Мбит/сек) версия EIA/TIA-232
- Использует 36-контактный D-образный разъем, может применяться для более длинных кабелей.
- Также называется RS-422 и RS-423

EIA/TIA - 232

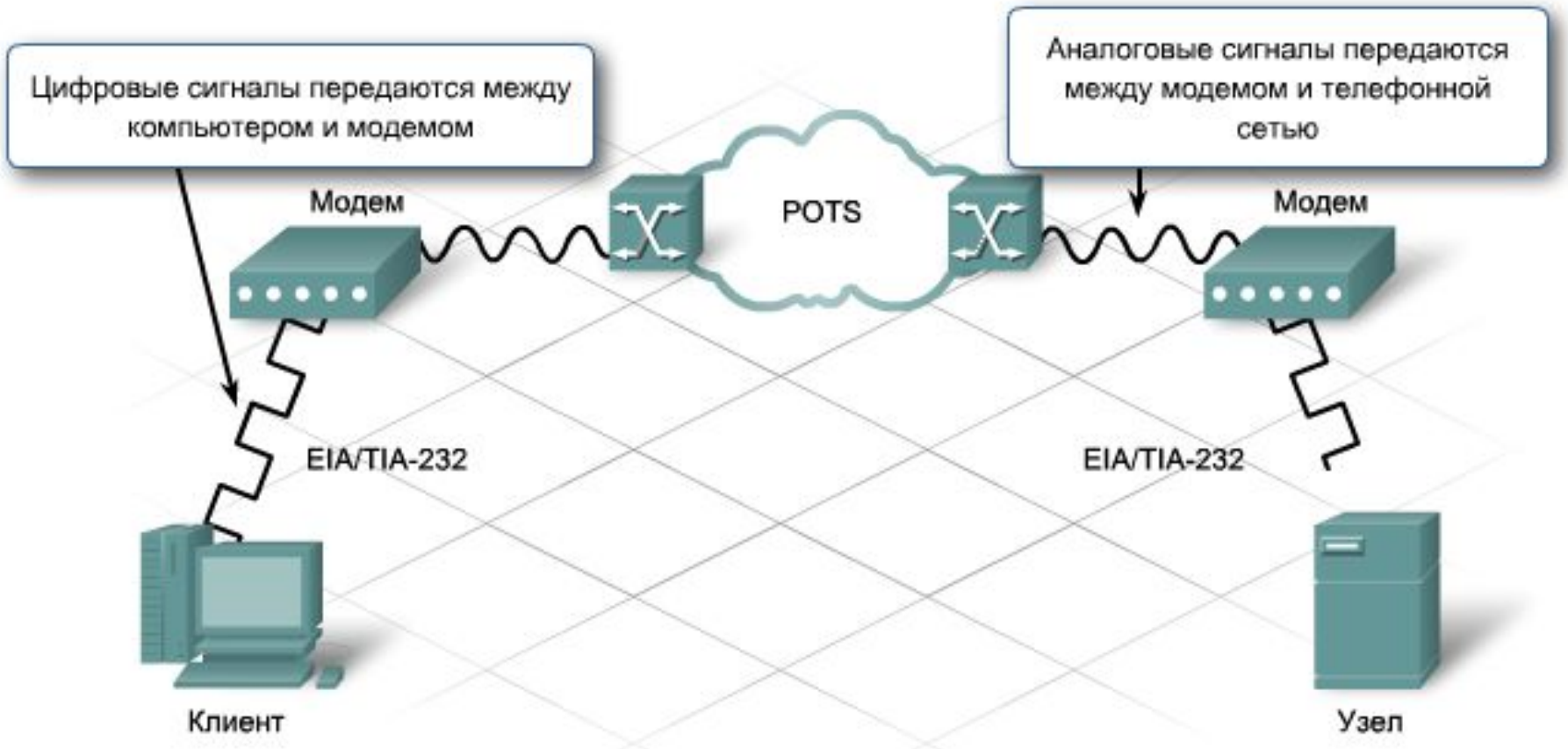
- Допускает скорость передачи сигналов до 64 Кбит/сек на короткие расстояния, использует 25-контактный D-образный разъем
- Ранее назывался стандартом RS-232
- Эквивалентен спецификации ITU-T V.24

Тип канала	Стандарт сигнала	Скорость передачи данных
56	DS0	56 Кбит/сек
64	DS0	64 Кбит/сек
T1	DS1	1,544 Мбит/сек
E1	ZM	2,048 Мбит/сек
E3	M3	34,064 Мбит/сек
J1	Y1	2,048 Мбит/сек
T3	DS3	44,736 Мбит/сек
OC-1	SONET	51,84 Мбит/сек
OC-3	SONET	155,54 Мбит/сек
OC-9	SONET	466,56 Мбит/сек
OC-12	SONET	622,08 Мбит/сек
OC-18	SONET	933,12 Мбит/сек
OC-24	SONET	1244,16 Мбит/сек
OC-36	SONET	1866,24 Мбит/сек
OC-48	SONET	2488,32 Мбит/сек

Стандарты сети WAN

- Стандарты WAN описывают характеристики физического и канального уровня передачи данных.
- Стандарты WAN канального уровня включают такие параметры, как:
  - физическая адресация;
  - управление потоком;
  - тип инкапсуляции;
  - порядок прохождения данных по каналу сети WAN.
- Примеры протоколов сети WAN для уровня 2:
  - процедура доступа к каналу для передачи кадров (протокол LAPF);
  - высокоуровневое управление каналом данных (протокол HDLC);
  - протокол "точка-точка" (протокол PPP).

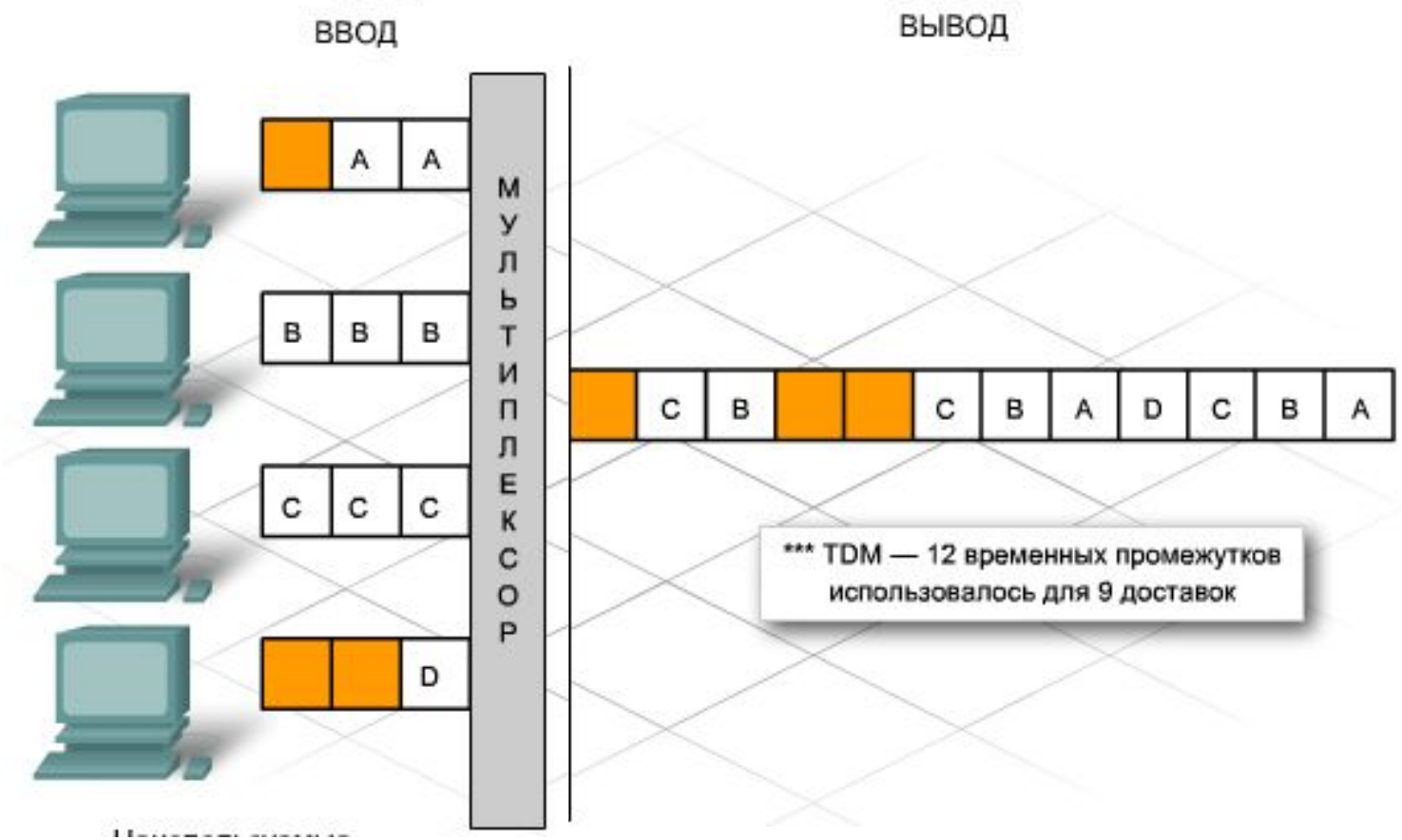
Доступ к сети WAN



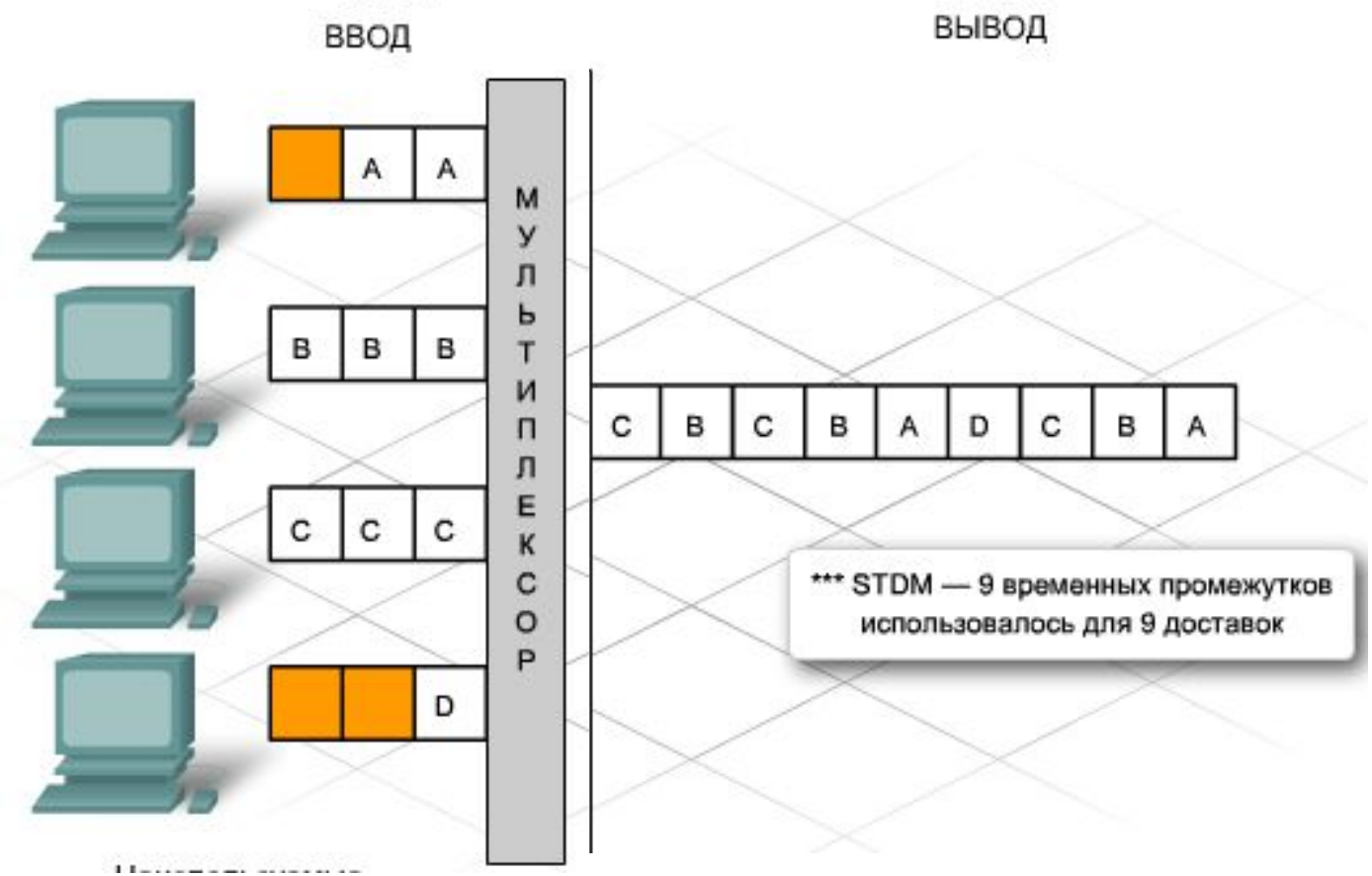
Доступ к сети WAN

- Существует две технологии, когда для данных из нескольких каналов может быть выделена полоса пропускания по одному кабелю на основе времени:
  - мультиплексирование с разделением времени (TDM);
  - статическое мультиплексирование с разделением времени (STDM).
- При мультиплексировании TDM полоса пропускания выделяется на основе предварительно назначенных временных интервалов. Каждый временной промежуток представляет период, в течение которого сеанс связи полностью использует физическую среду передачи данных.
- STDM может отслеживать сеансы, для которых требуется дополнительная полоса пропускания

Мультиплексирование TDM

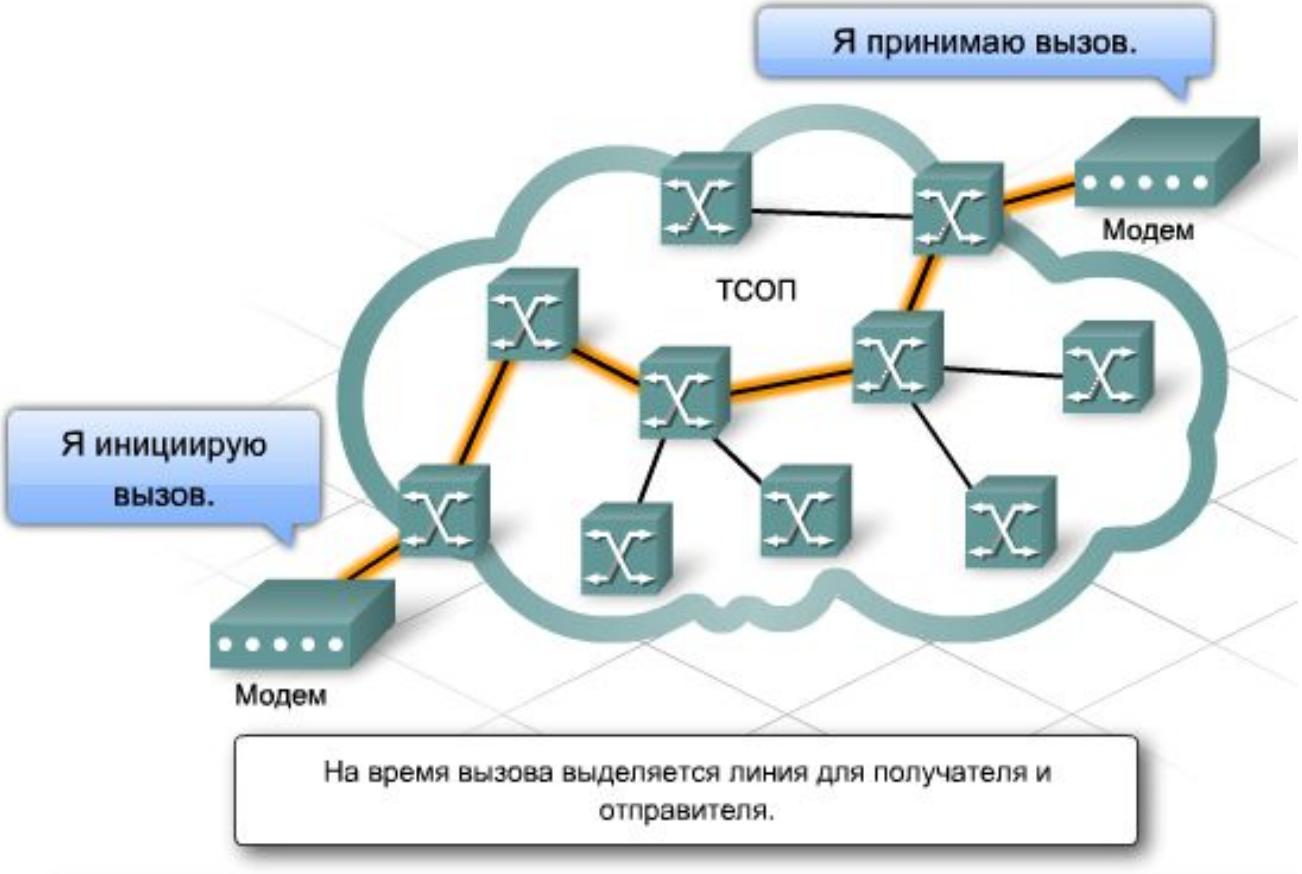


Мультиплексирование STDM



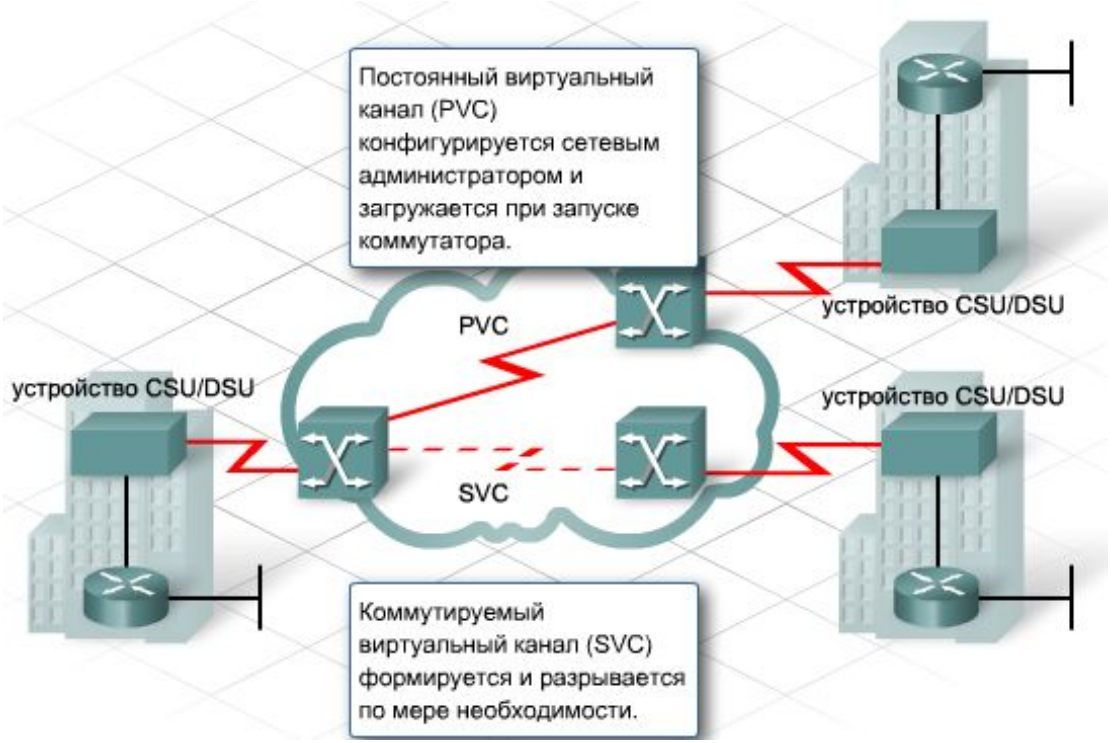
Коммутация каналов и пакетов

- Подключение предприятий к службам сети WAN осуществляется разными способами.
  - Выделенная арендуемая линия
  - Коммутация каналов
  - Пакетная коммутация
  - Коммутация ячеек



Коммутация каналов и пакетов

- При использовании технологии пакетной коммутации поставщик услуг устанавливает виртуальные каналы
  - Коммутируемый виртуальный канал (SVC) динамически устанавливается между двумя точками по запросам маршрутизаторов на передачу данных
  - Постоянный виртуальный канал (PVC) обеспечивает постоянную магистраль для пересылки данных между двумя точками

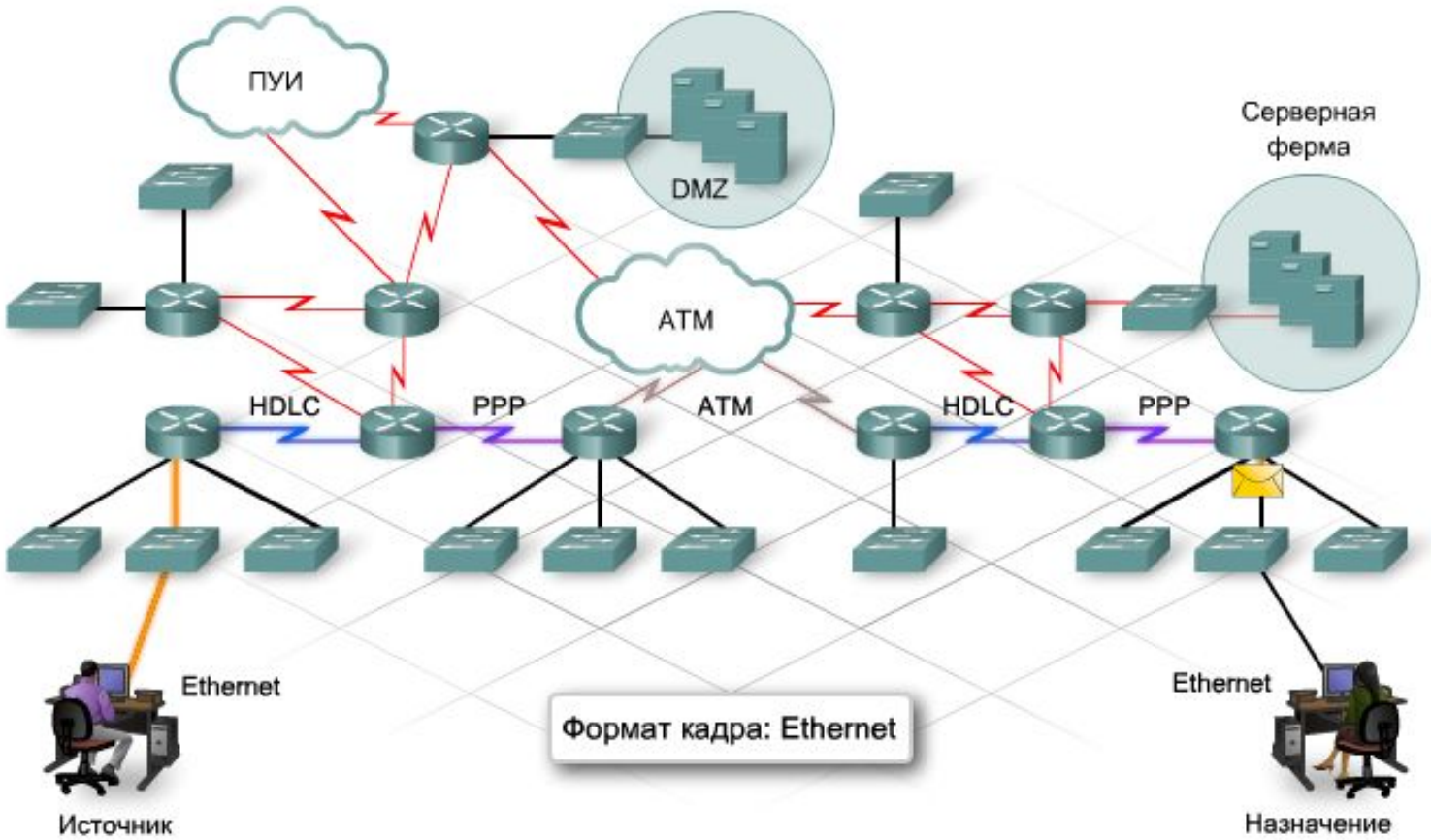


Технологии WAN «последняя миля» и «длинная дистанция»

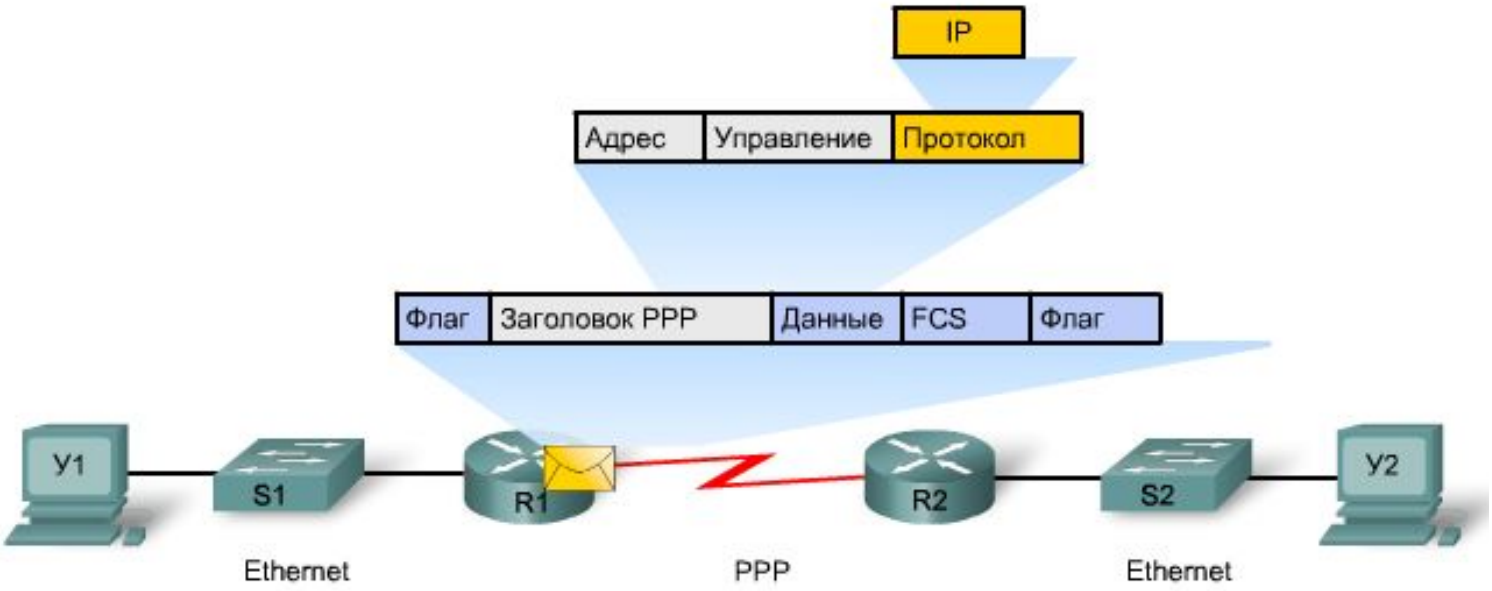
- Примеры технологий "последней мили":
  - аналоговый набор номера;
  - цифровая сеть с интегрированными услугами (ISDN);
  - выделенная линия;
  - кабельная связь;
  - цифровая абонентская линия (DSL);
  - Frame Relay;
  - беспроводная сеть.
- Существование различных технологий WAN позволяет поставщикам услуг надежно пересылать данные на большие расстояния. Некоторые из них включают стандарт ATM, спутниковую связь, Frame Relay и выделенные линии.
- Синхронная оптоволоконная сеть (SONET) и синхронная цифровая иерархия (SDH) – это стандарты, которые позволяют перемещать большие объемы данных на большие расстояния с помощью оптоволоконного кабеля.
- Одной из новейших разработок для сверхдлинных соединений является технология мультиплексирования по длине волны высокой плотности (DWDM).

Инкапсуляции Ethernet и WAN

- Инкапсуляция соответствует отдельному формату в зависимости от технологии, применяемой в сети
- Уровень 2 добавляет содержимое заголовка, которое соответствует типу физической передачи данных по сети
- При прохождении данных по сети инкапсуляция канального уровня может постоянно меняться, в то время как инкапсуляция сетевого уровня неизменна.



Инкапсуляции Ethernet и WAN



- Тип инкапсуляции должен совпадать в обеих конечных точках прямого соединения. Инкапсуляция канального уровня включает следующие поля:
  - **Flag** (флаг) - помечает начало и конец каждого кадра;
  - **Address** (адрес) - зависит от типа инкапсуляции; не требуется, если канал WAN является прямым соединением;
  - **Control** (управление) - используется для указания типа кадра;
  - **Protocol** (протокол) - используется для определения типа инкапсулированного протокола сетевого уровня; представлено не во всех инкапсуляциях сети WAN;
  - **Data** (данные) - используется как данные уровня 3 и датаграмма IP-сети;
  - **Frame check sequence** (FCS) (контрольная последовательность кадра) - обеспечивает механизм сверки, позволяющий убедиться, что кадр не был поврежден во время передачи.

HDLC и PPP

- Протокол HDLC использует синхронную последовательную передачу данных, при которой обеспечивается безошибочная связь между двумя точками
- HDLC определяет структуру кадров уровня 2, что позволяет управлять потоком и ошибками с помощью механизма подтверждения и определения размера окна

Кадр HDLC (открытый стандарт)

Флаг	Адрес	Управление	Сведения	FCS	Флаг
8 бит	8 бит	8 или 16 бит	Переменная длина, 0 или более бит, кратно 8	16 или 32 бита	8 бит

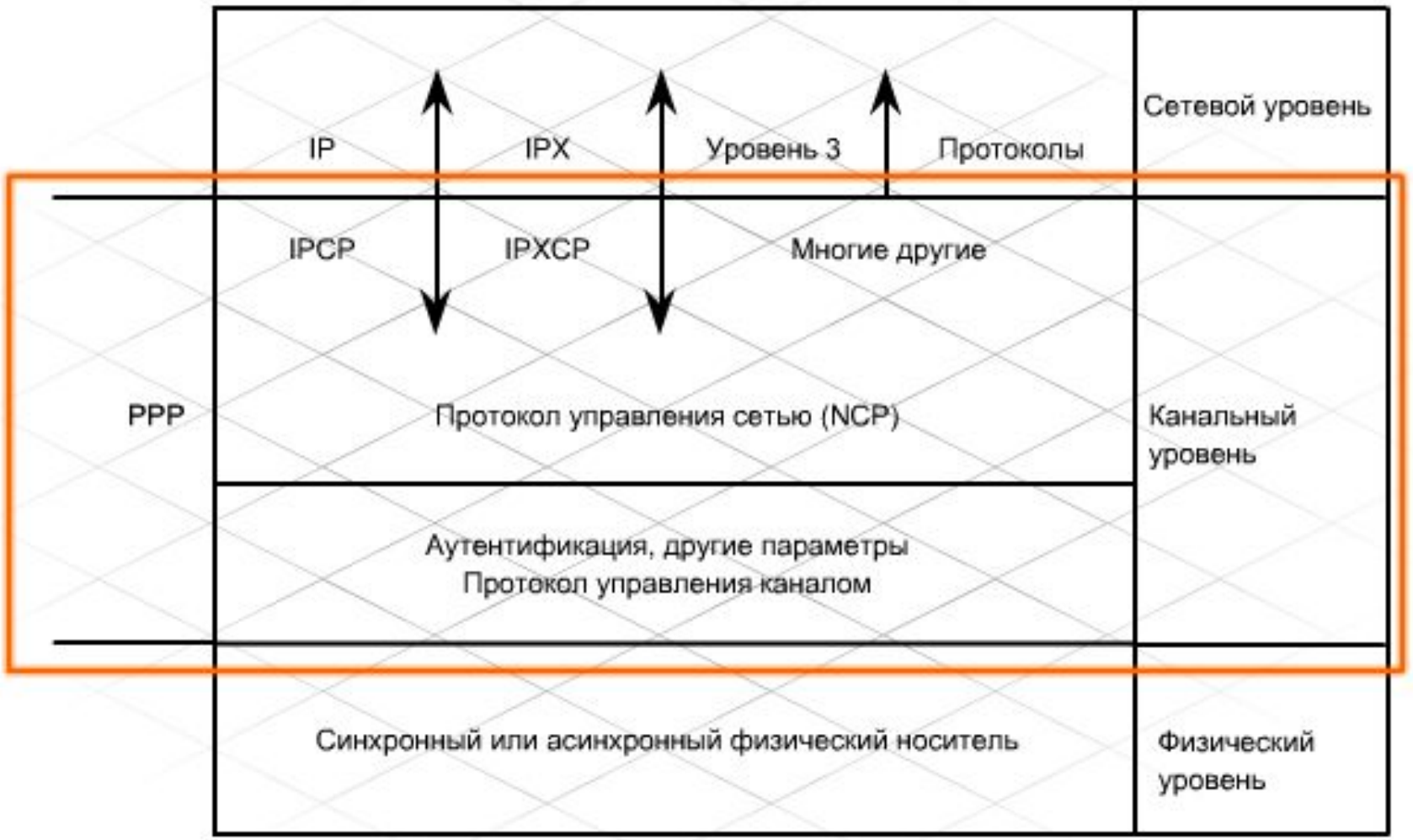
Кадр Cisco HDLC

Флаг	Адрес	Управление	Тип (код протокола)	Информация	FCS	Флаг
8 бит	8 бит	8 бит	16 бит	Переменная длина, 0 или более бит, кратно 8	16 бит	8 бит

HDLC и PPP

- PPP использует многоуровневую архитектуру для инкапсулирования и передачи датаграмм нескольких протоколов по прямому каналу
- Протокол PPP могут поддерживать следующие интерфейсы:
  - асинхронные последовательные подключения;
  - синхронные последовательные подключения;
  - высокоскоростной последовательный интерфейс (HSSI);
  - цифровая сеть с интегрированными услугами (ISDN).
- Стандарт PPP содержит два подпротокола:
  - Протокол управления каналом данных — отвечает за установку, поддержку и завершение передачи данных по прямому соединению.
  - Протокол управления сетью — обеспечивает взаимодействие с различными протоколами сетевого уровня.

HDLC и PPP


IP
IPX
Уровень 3
Протоколы
Сетевой уровень
IPCP
IPXCP
Многие другие
PPP
Протокол управления сетью (NCP)
Канальный уровень
Аутентификация, другие параметры
Протокол управления каналом
Синхронный или асинхронный физический носитель
Физический уровень

Протокол управления каналом

- Протокол PPP использует протокол управления каналом (LCP) для установления, поддержки, тестирования и завершения передачи данных по прямому соединению. Дополнительно, протокол управления каналом согласовывает и настраивает параметры канала сети WAN. Протокол LCP выполняет согласование следующих параметров:
  - аутентификация;
  - сжатие;
  - обнаружение ошибок;
  - группа каналов;
  - обратный PPP-вызов.

- Также протокол LCP:
  - обрабатывает различные размеры пакетов;
  - обнаруживает общие ошибки настроек;
  - определяет нормальную и сбойную работу канала.

Протокол управления сетью

- Протокол PPP использует компонент протокола управления сетью (NCP) для инкапсулирования нескольких протоколов сетевого уровня, чтобы они могли выполняться в тех же каналах связи

- Выполнение сеансов PPP проходит через три этапа:
  - установление соединения - PPP отправляет кадры по протоколу LCP для настройки и тестирования канала передачи данных. Кадры LCP содержат поле параметров настройки, которое выполняет согласование таких параметров, как максимальный размер передаваемого блока данных (MTU), сжатие и аутентификация соединения
  - аутентификация (необязательно) - включает защиту с помощью паролей для идентификации маршрутизаторов соединения
  - передача данных по протоколу сетевого уровня - PPP отправляет пакеты по протоколу управления сетью для выбора настройки одного или нескольких протоколов сетевого уровня, таких как IP или IPX

Настройка PPP

- **encapsulation ppp** - включает инкапсуляцию PPP для последовательного интерфейса
- **compress [предиктор| стекер]** - включает сжатие в интерфейсе с помощью предиктора или стекера
- **ppp multilink** - настраивает распределение нагрузки в нескольких каналах
- **show interfaces serial** – отображает инкапсуляцию и состояние протокола управление каналом
- **show controllers** – показывает состояние каналов интерфейса и подключен ли к нему кабель
- **debug serial interface** – проверяет приращение пакетов проверки на активность. Если приращения пакетов не происходит, возможно, в плате интерфейса или в сети существует проблема синхронизации
- **debug ppp** – предоставляет информацию о различных этапах процесса PPP, включая согласование и аутентификацию

Аутентификация PPP

- В канале PPP существует два возможных типа аутентификации:
  - протокол аутентификации по паролю (PAP)
  - протокол аутентификации по квитированию вызова (CHAP)

- Протокол PAP является простым методом проверки подлинности удаленного устройства. Для отправки своего имени пользователя и пароля PAP использует двухстороннее согласование. Вызываемое устройство проверяет имя вызывающего устройства и подтверждает, что отправленный и сохраненный в его базе данных пароль совпадает. Если пароли совпадают, аутентификация считается успешно выполненной.
- PAP повторно отправляет имя пользователя и пароль по каналу открытым текстом, пока не будет получено подтверждение или завершено соединение

Аутентификация PPP

- При выполнении протокола CHAP пароль не отправляется через канал. Аутентификация происходит в процессе начального установления соединения и во время его активного состояния.
- В протоколе CHAP используется трехэтапное квитирование.
  - PPP устанавливает этап соединения.
  - Локальный маршрутизатор отправляет сообщение запроса на удаленный маршрутизатор.
  - Удаленный маршрутизатор использует запрос и коллективный секретный пароль для генерирования односторонней хеш-функции.
  - Удаленный маршрутизатор отправляет одностороннюю хеш-функцию обратно на локальный маршрутизатор.
  - Локальный маршрутизатор сравнивает отклик с собственным расчетом, используя запрос и тот же коллективный секретный пароль.
  - Локальный маршрутизатор подтверждает аутентификацию, если значения совпадают.
  - Локальный маршрутизатор немедленно разрывает соединение, если значения не совпадают.

Аутентификация PPP

- **username имя password пароль** – команда глобальной настройки. Создает локальную базу данных, которая содержит имя и пароль удаленного устройства. Это имя должно точно и с учетом регистра совпадать с именем узла удаленного маршрутизатора.

- **ppp authentication {chap | chap pap | pap chap | pap}** - команда настройки интерфейса. Определяет тип аутентификации на каждом интерфейсе, например — PAP или CHAP.

- **ppp pap sent-username имя password пароль** – команда настройки интерфейса. Определяет комбинацию имени пользователя и пароля, которая будет отправлена на удаленный маршрутизатор

- Чтобы отобразить изменение последовательности проверки, используйте команду debug на обоих маршрутизаторах.

  debug ppp{authentication | packet | error | negotiation | chap }

  - Authentication - отображает последовательность изменения аутентификации
  - Packet - отображает отправленные и полученные пакеты PPP
  - Negotiation - отображает пакеты, переданные во время запуска PPP, где параметры PPP согласованы
  - Error – отображает ошибки и статистику протокола, связанные с соединением и согласованием PPP
  - Chap – отображает изменения пакетов CHAP

Обзор протокола FrameRelay

- Сети **Frame Relay** — это сети множественного доступа, такие же как Ethernet, но в которых не поддерживается передача трафика широковещательной рассылки. Frame Relay — это нешироковещательная сеть множественного доступа (NBMA).
- В протоколе Frame Relay используется технология коммутации пакетов с переменной длиной
- Маршрутизатор (DTE) подключается к сети поставщика услуг обычно по выделенной линии. При этом соединение проходит через коммутатор Frame Relay (DTE) к ближайшему местному серверу поставщика услуг. Такое соединение является каналом доступа
- Удаленный маршрутизатор на другом конце сети также является оконечным оборудованием передачи данных (DTE). Соединение между двумя оконечными устройствами передачи данных осуществляется по виртуальному каналу

Обзор протокола FrameRelay

- В сети NBMA каждому виртуальному каналу для идентификации требуется адрес уровня 2.
- В сети Frame Relay таким адресом является идентификатор канала связи (DLCI)
- Идентификатор DLCI определяет виртуальный канал, по которому будут переданы данные в точку назначения
- DLCI уровня 2 связан с адресом уровня 3 устройства на другом конце виртуального канала. Сопоставление DLCI и удаленного IP-адреса можно выполнять вручную или динамически с помощью процесса, называемого обратным переопределением адресов

Обзор протокола FrameRelay

- Интерфейс локального управления (LMI) является стандартом передачи сигналов между оконечным оборудованием передачи данных и коммутатором Frame Relay. Интерфейс локального управления отвечает за соединение и поддержку состояния между устройствами

- Сообщения LMI обеспечивают связь и синхронизацию между сетью и устройством пользователя

- Интерфейс локального управления предоставляет сведения о состоянии соединения по виртуальному каналу, которые отображаются в таблице сопоставлений Frame Relay:
  - ***Активное состояние*** - соединение активно, и маршрутизаторы могут обмениваться данными.
  - ***Неактивное состояние*** – локальное соединение с коммутатором Frame Relay выполняется, но удаленное соединение с коммутатором Frame Relay отсутствует.
  - ***Удаленное состояние*** – локальное соединение не получает сообщений интерфейса локального управления от коммутатора Frame Relay или отсутствует обслуживание между маршрутизатором телекоммуникационного оборудования клиента (CPE) и коммутатором Frame Relay

Обзор протокола FrameRelay

- Гарантированная скорость передачи (CIR) – определяет минимальную полосу пропускания, гарантированную поставщиком для передачи данных по виртуальному каналу
- Поставщик услуг вычисляет гарантированную скорость передачи как средний объем данных, передаваемых в какой-либо период времени.
  - Расчетный период времени является предельно допустимым временем
  - Число гарантированных битов внутри Tc является предельным пакетом
- Форсированная скорость передачи (EIR) является средним превышением скорости по сравнению с CIR, которое может поддерживать виртуальный канал при отсутствии перегрузки в сети
- Любое превышение битов сверх гарантированного пакета, вплоть до максимальной скорости, поддерживаемой каналом, называется форсированным пакетом

Обзор протокола FrameRelay

- Прямое извещение о насыщении (FECN) это поле с одним разрядом, для которого коммутатор может установить значение 1. Оно определяет оконечное оборудование данных, на котором ожидается перегрузка сети (чтобы задействовать процедуру устранения насыщения сети на принимающем устройстве).

- Явное предуведомление о перегрузке (BECN) – это поле с одним разрядом, которое при установке коммутатором значения 1 указывает, что ожидается перегрузка сети в обратном направлении.