6. Виртуальные сети

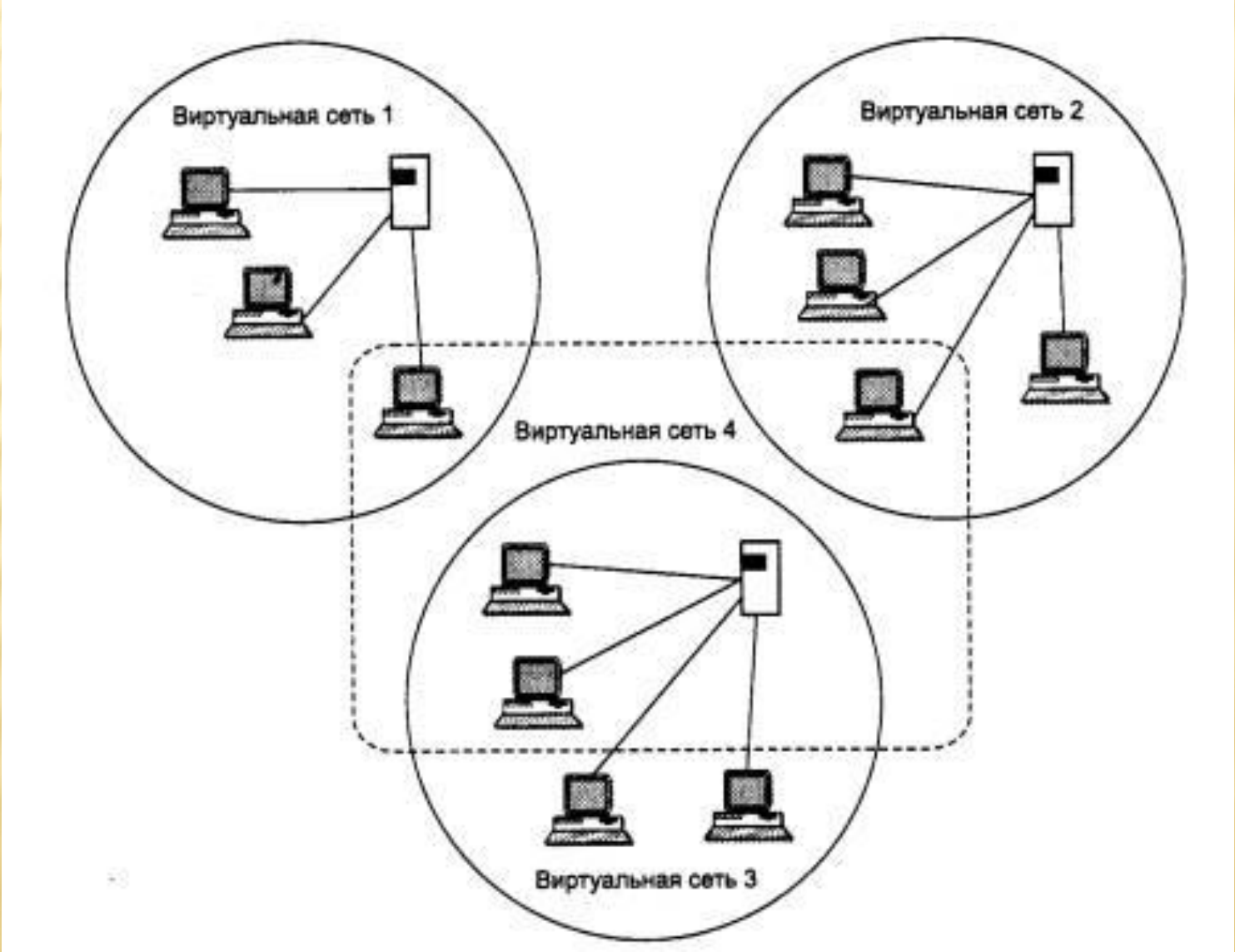
Газизов Тимур Тальгатович,
к.т.н., доцент кафедры информатики ТГПУ

ИНФОРМАЦИОННЫЕ СЕТИ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

ВИРТУАЛЬНАЯ СЕТЬ

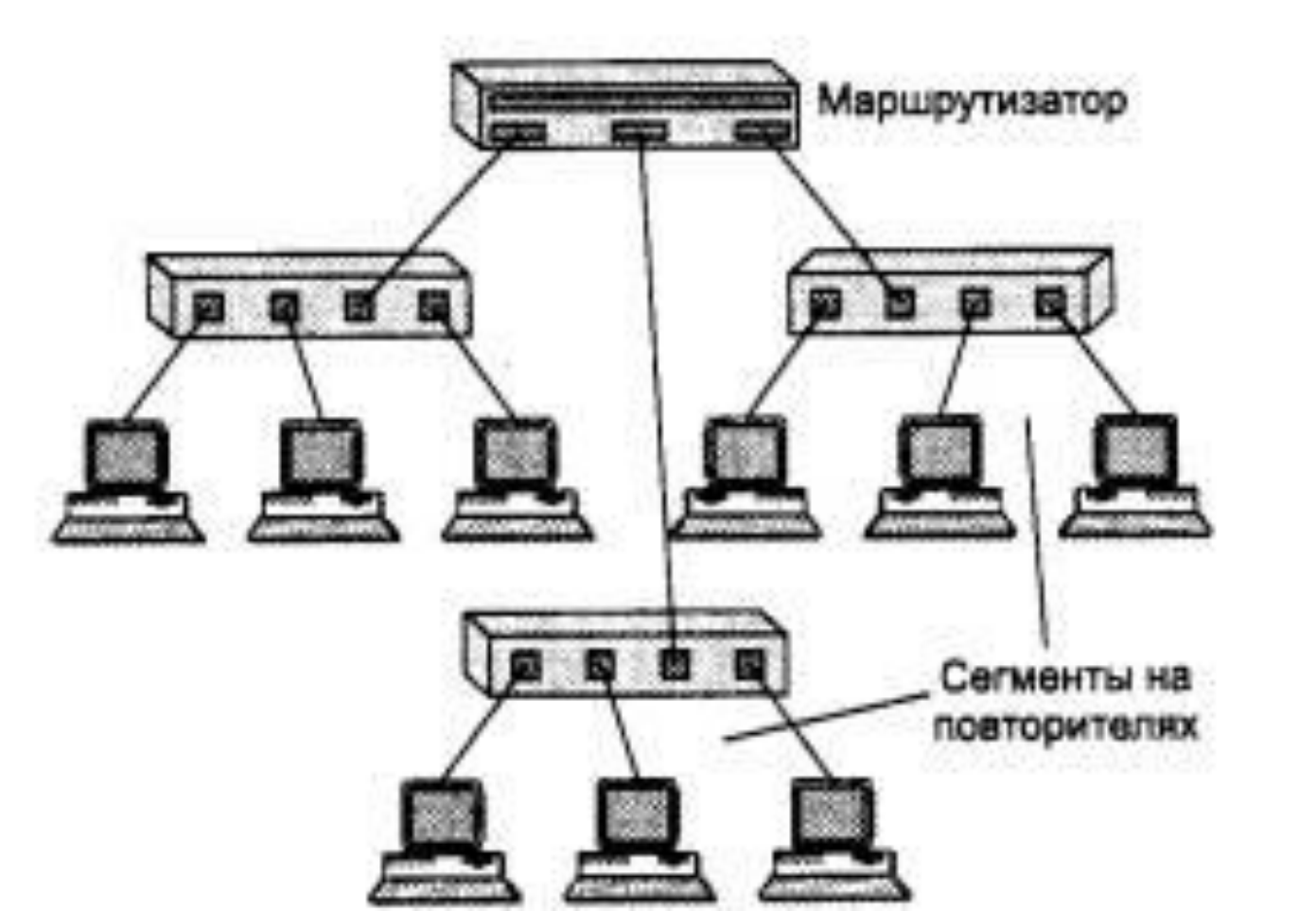
- группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети
- облегчении процесса создания изолированных сетей
- Связь сетей через маршрутизаторы: гибкая основа для построения крупной сети

ПРИМЕР ВИРТУАЛЬНЫХ СЕТЕЙ



ИНТЕРСЕТЬ

- Сеть построенная на повторителях



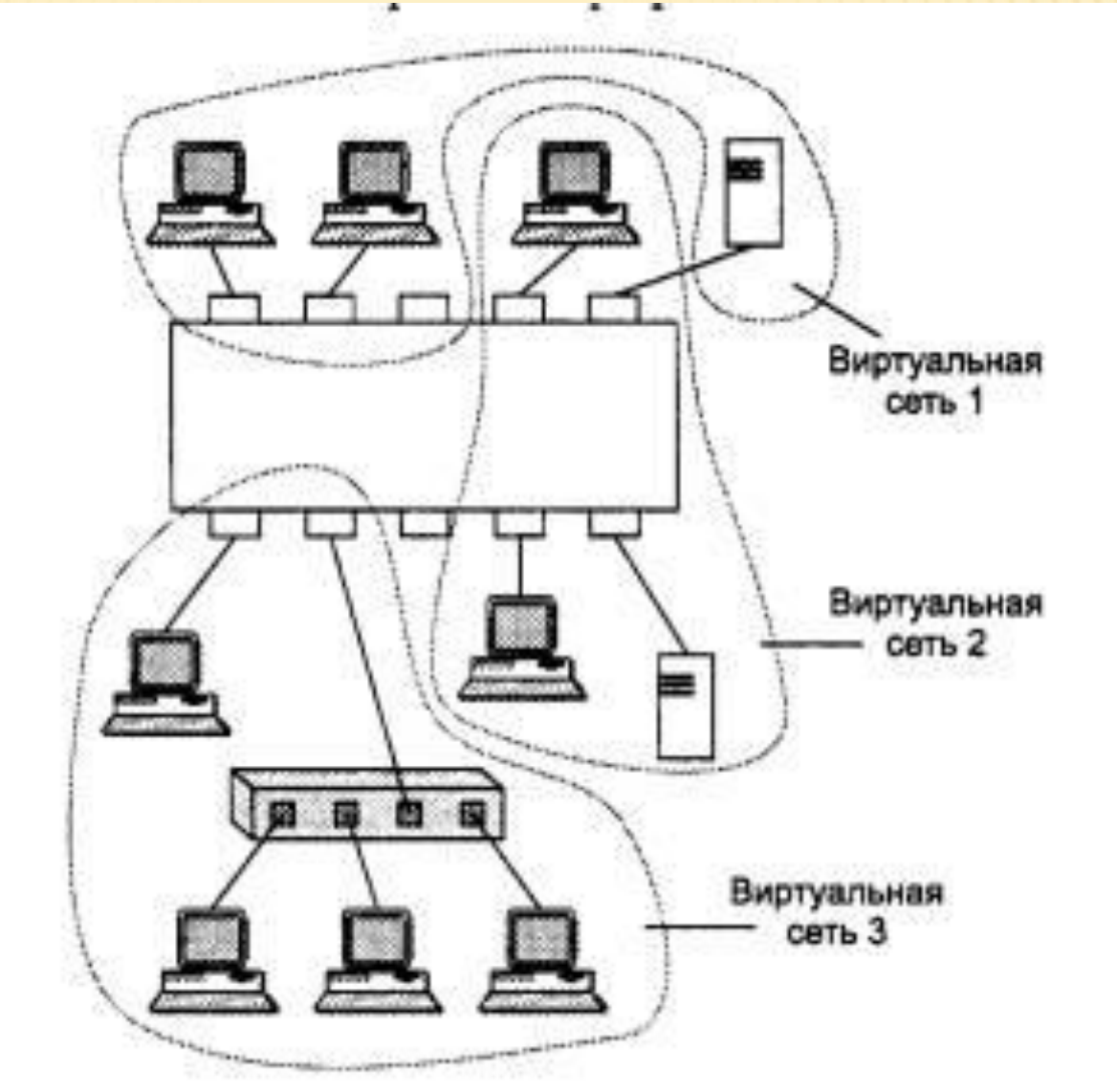
ВИРТУАЛЬНЫЕ СЕТИ В КОММУТАТОРАХ

- повышение производительности в каждой из виртуальных сетей, так как коммутатор передает кадры в такой сети только узлу назначения;
- изоляция сетей друг от друга для управления правами доступа пользователей и создания защитных барьеров на пути широковещательных штормов.
- Использование сетевого уровня – коммутаторы 3-его уровня

СТАНДАРТИЗАЦИЯ

- каждый крупный производитель коммутаторов разработал свою технологию виртуальных сетей
- 1998: стандарт IEEE 802.1Q
- механизм группирования: кадр, пришедший от порта, принадлежащего, например, виртуальной сети 1, никогда не будет передан порту, который не принадлежит этой виртуальной сети

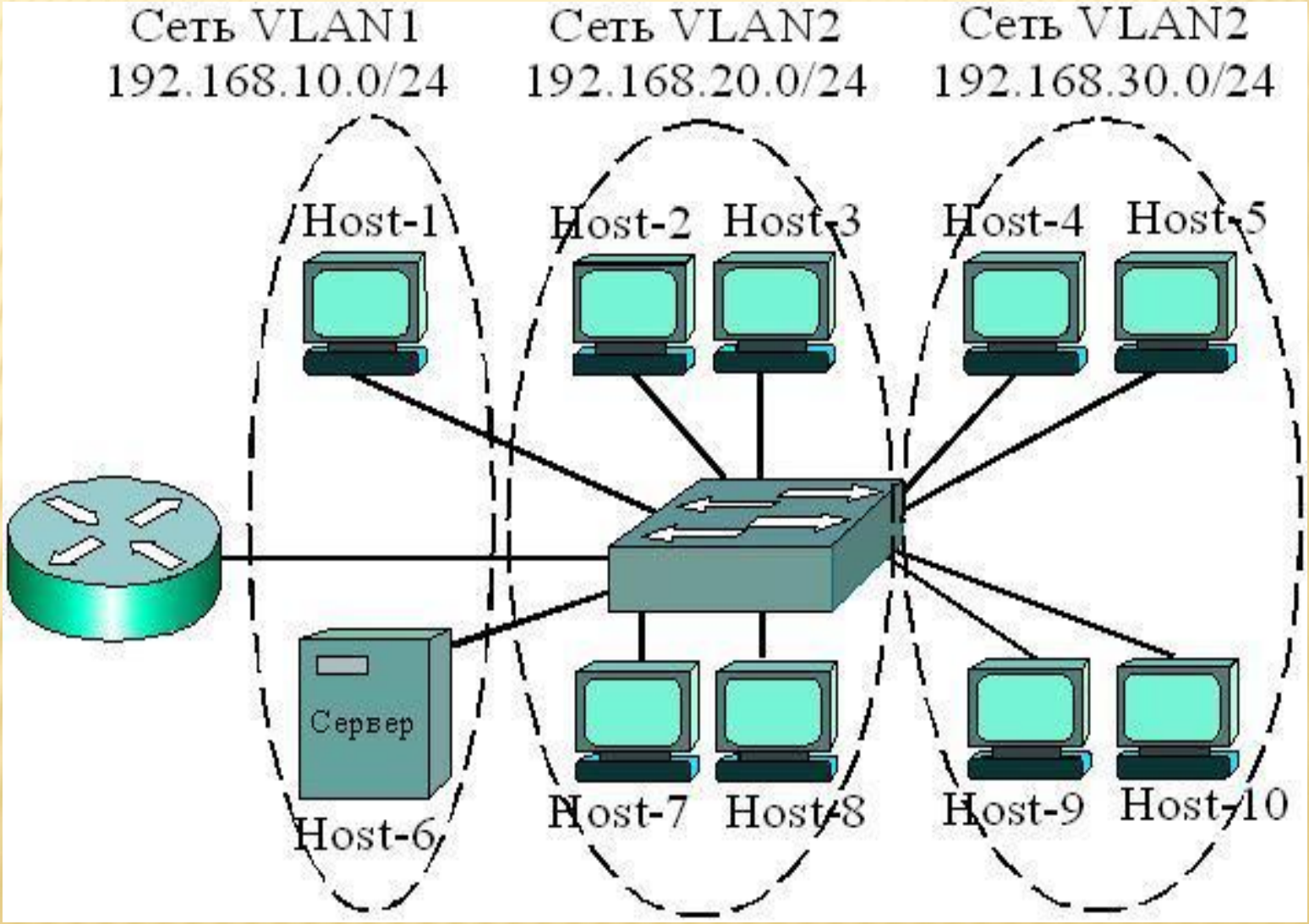
ВИРТУАЛЬНЫЕ СЕТИ



VLAN

- **Виртуальные сети** созданы, чтобы реализовать сегментацию сети на коммутаторах.
- логическое объединение групп станций сети, является одним из основных методов защиты информации в сетях на коммутаторах
- группировка по функциональным особенностям работы, независимо от физического местоположения пользователей
- обмен данными происходит только между устройствами, находящимися в одной VLAN
- обмен данными между различными VLAN производится **только через маршрутизаторы**

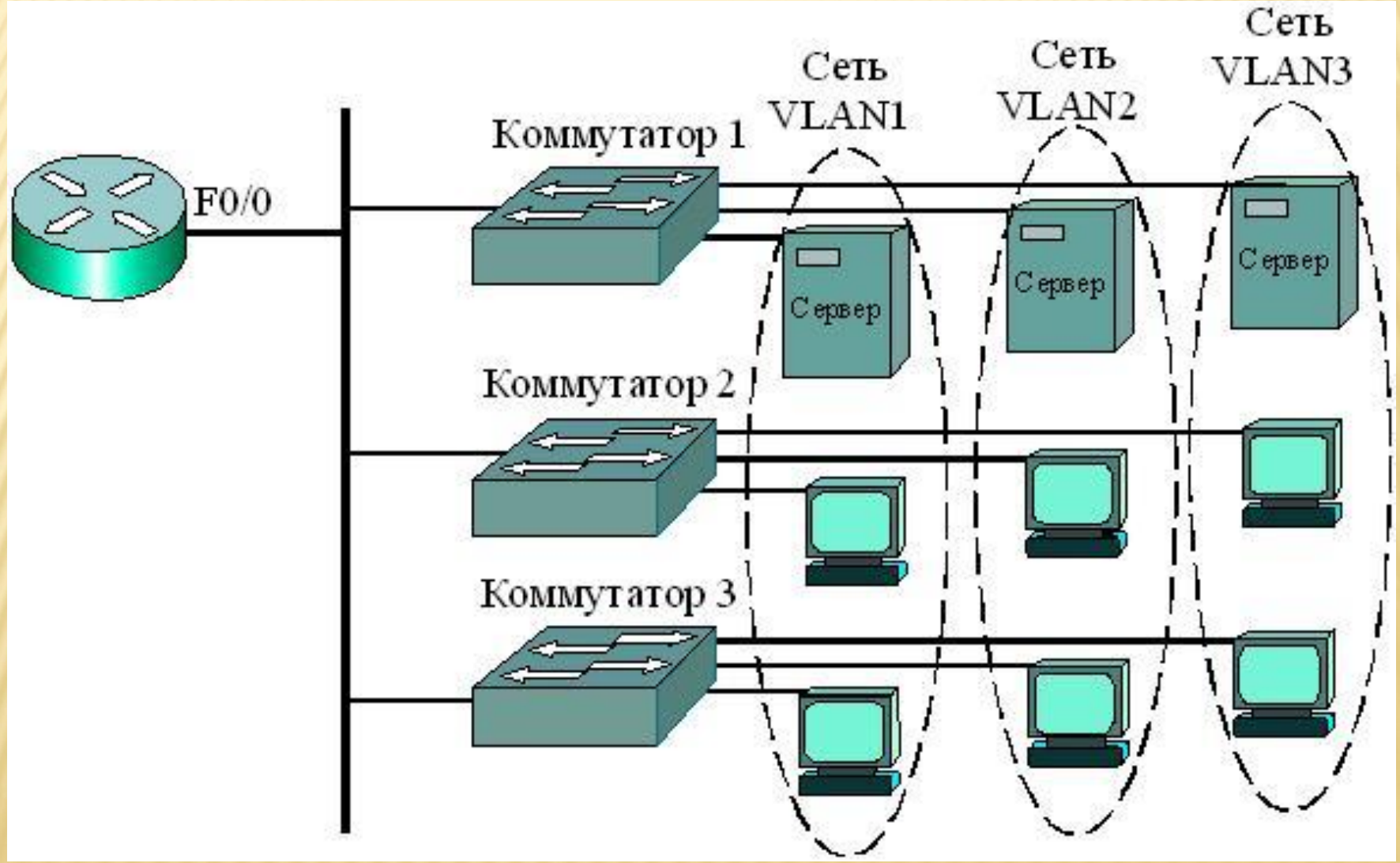
ПРИМЕР НЕСКОЛЬКИХ VLAN



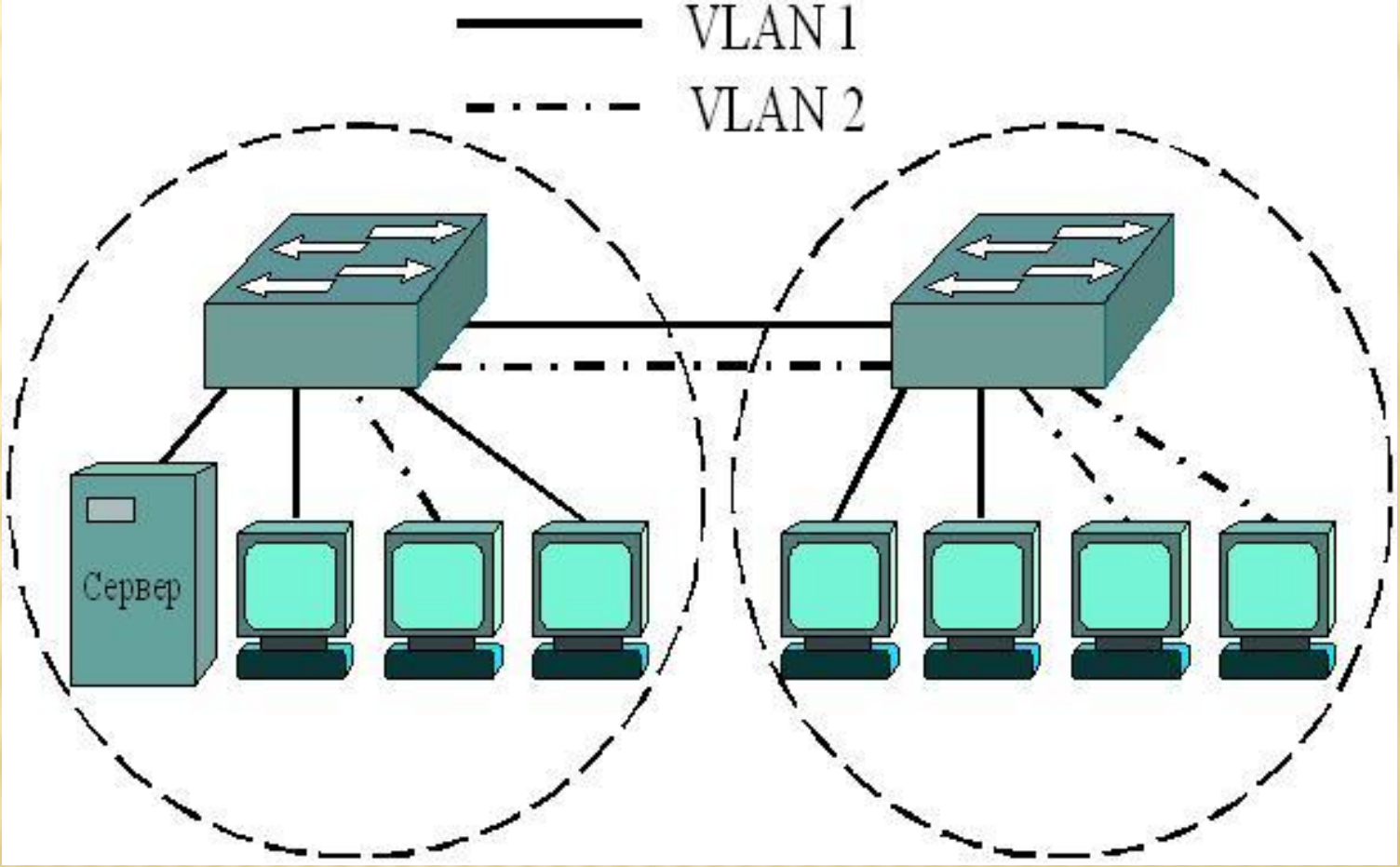
ПРИМЕР

- сеть VLAN является широковещательным доменом, созданным одним или более коммутаторами. На рисунке три виртуальных сети VLAN созданы одним маршрутизатором и тремя коммутаторами. При этом существуют три отдельных широковещательных домена (сеть VLAN 1, сеть VLAN 2, сеть VLAN 3). Маршрутизатор управляет трафиком между сетями VLAN, используя маршрутизацию Уровня 3

ТРИ ВИРТУАЛЬНЫХ СЕТИ VLAN



СЕТЬ НА НЕСКОЛЬКИХ КОММУТАТОРАХ



ТЕГ: **ИДЕНТИФИКАТОР КАДРА**

- кадры данных могут быть получены коммутатором от любого устройства, присоединенного к любой виртуальной сети, при обмене данными между коммутаторами в заголовок кадра добавляется **уникальный идентификатор кадра – тег (tag)**
- **Тег** определяет VLAN каждого пакета

ФОРМАТ ТЕГА

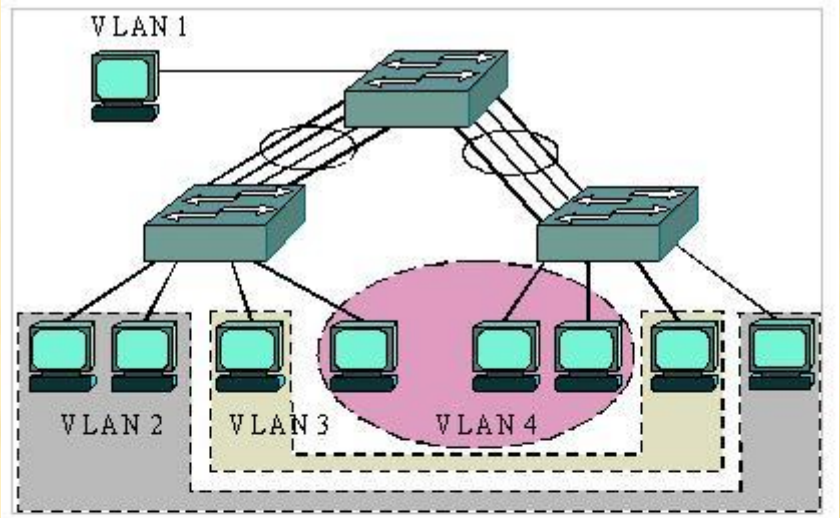
- 12 бит используются для адресации (4096 виртуальных сетей)
- 3 бита – 8 уровней приоритета
- 1 бит – тип сети (Token Ring)

Таблица 16.1. Формат тега виртуальной сети		
3 бита	1 бит	12 бит
Приоритет	CFI	VLAN ID

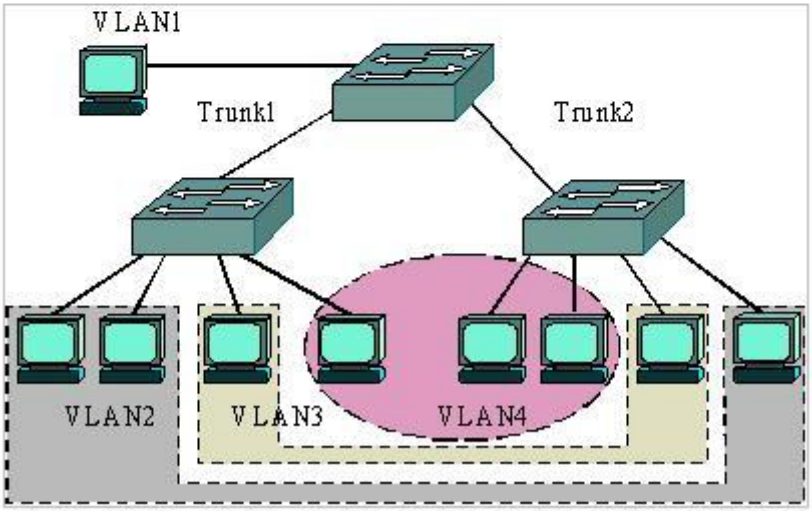
ТРАНКОВЫЕ СОЕДИНЕНИЯ

- для соединения нескольких коммутаторов между собой задействуют несколько физических портов
- **транк (trunk) - один агрегированный логический канал**
- транковые соединения используются и для подключения маршрутизатора к коммутатору
- Пропускная способность агрегированного логического канала равна сумме пропускных способностей физических каналов

ИСПОЛЬЗОВАНИЕ ТРАНКОВ



а)



б)

КОНФИГУРИРОВАНИЕ ВИРТУАЛЬНЫХ СЕТЕЙ

- Создание виртуальных сетей может производиться двумя способами:
  - в режиме глобального конфигурирования;
  - из привилегированного режима конфигурирования по команде vlan database.
- Состояние виртуальных сетей и интерфейсов коммутатора Cisco Catalyst серии 2950-24 с именем Sw_A можно посмотреть по следующей команде:
  - Sw_A#sh vlan brief

КРАТКИЕ ИТОГИ

- Сеть VLAN состоит из узлов, объединенных единственным широковещательным доменом, который образован приписанными к виртуальной сети портами коммутатора. Широковещательные передачи снижают безопасность информации.
- Трафик между VLAN обеспечивается маршрутизацией, т. е. общение между узлами разных виртуальных сетей происходит только через маршрутизатор.
- При обмене данными между коммутаторами в заголовок добавляется уникальный идентификатор кадра – тег (tag) виртуальной сети, который определяет членство VLAN каждого пакета.