# Основы компьютерных сетей. 7. Углубленное изучение сетевых технологий.

access list

wildcard

Технологии VLAN (802.1Q).

# План занятия:

- access list
- wildcard
- VLAN 802.1Q

# Что такое access list?

Access list (или ACL - Access Control List) - это набор правил, который определяет, какие типы сетевого трафика разрешены или запрещены на устройстве сетевого оборудования, таком как маршрутизатор или коммутатор.

Access list используются для контроля доступа к сетевым ресурсам, например, они могут определять, какие узлы могут подключаться к сети, какие порты могут быть использованы для определенных типов трафика, и так далее.

Access list могут быть применены на разных уровнях сети. Например, они могут работать на уровне интерфейса устройства, на уровне маршрутизатора или на уровне виртуальной частной сети (VPN).

# Access list бывают двух типов

**1.Стандартные Access list** - они основаны на источнике IP-адреса. Такие списки правил позволяют или блокируют трафик на основе источника, например, можно разрешить или запретить определенные IP-адреса.

**2.Расширенные Access list** - они могут включать критерии, такие как источник, назначение, порт и протокол. Это более гибкий вид Access list, позволяющий более детально управлять трафиком.

Access list - важный инструмент в сетевой безопасности, позволяющий ограничивать доступ к сетевым ресурсам и защищать их от несанкционированного доступа.

# Что такое wildcard?

"wildcard" (дословно: "джокер") обозначает специальный символ, который используется для задания шаблонов при сопоставлении адресов IP или портов.

В стандартных и расширенных Access Control Lists (ACLs) для маршрутизаторов и коммутаторов Cisco, wildcard-маска используется для указания диапазона адресов, на которые применяются правила.

Это позволяет гибко определять диапазоны адресов и разрешать или блокировать трафик в соответствии с этими шаблонами.

# Что такое wildcard?

Примеры wildcard-масок в IPv4:

- **0.0.0.0** - соответствует любому адресу.
- **255.255.255.255** - соответствует конкретному адресу.
- **0.0.0.255** - соответствует всем адресам в последнем октете сети.
- **0.0.255.255** - соответствует всем адресам в последних двух октетах сети.

# Что такое wildcard?

Например, если у вас есть правило в Access Control List, которое имеет следующий формат:

```
permit 192.168.1.0 0.0.0.255
```

Это означает, что разрешен весь трафик с адресами в диапазоне от 192.168.1.0 до 192.168.1.255.

Часто wildcard называют “обратной маской”, но это не совсем корректно.

# VLAN

VLAN (Virtual Local Area Network) - это логический сегмент сети, который позволяет разделить физическую сеть на несколько логических групп. Внешне устройства в разных VLAN'ах могут выглядеть как будто они подключены к разным физическим сетям, хотя физическое соединение остается общим.

Вот несколько ключевых характеристик VLAN:

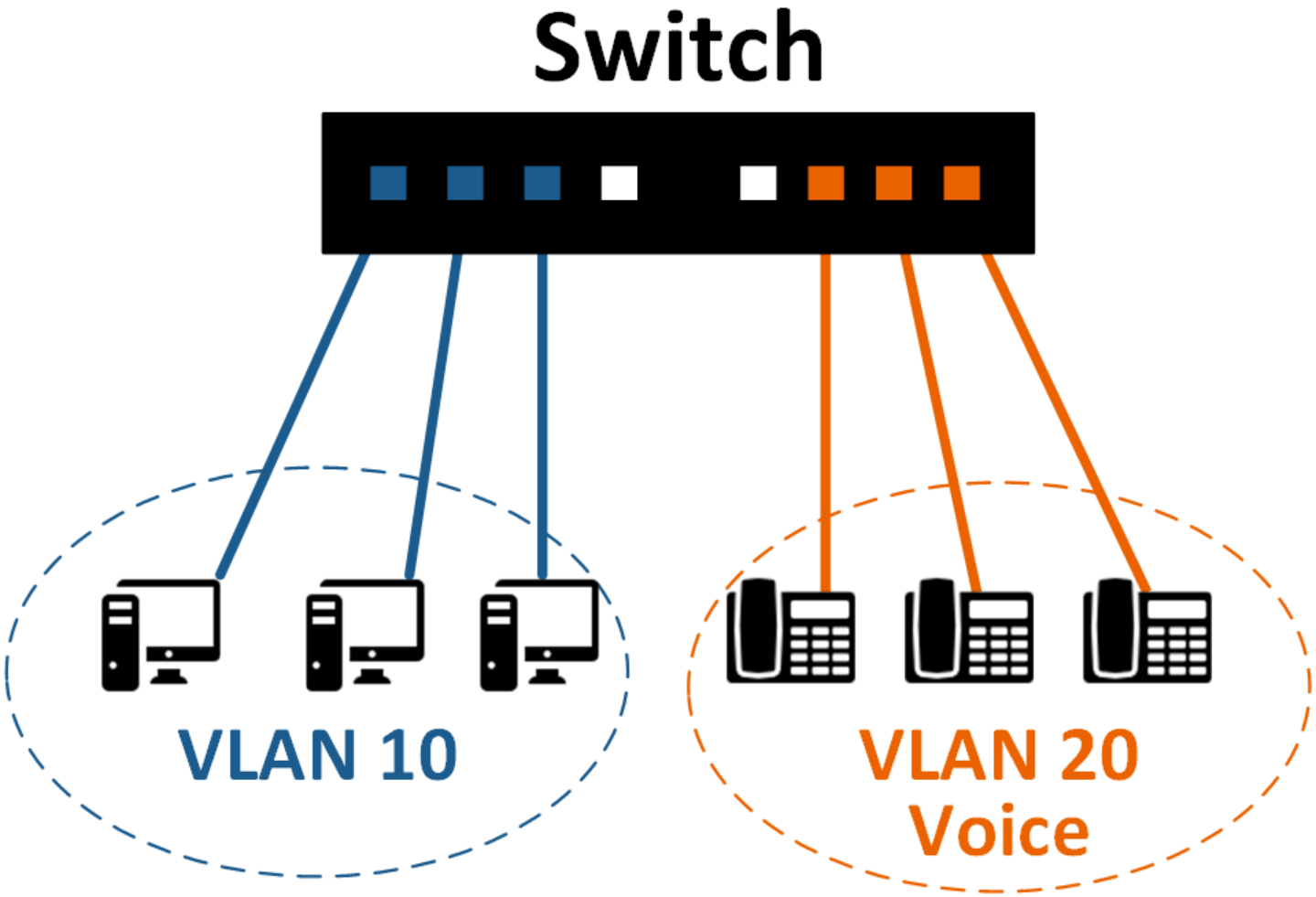
1. **Изоляция трафика**: Устройства в одном VLAN не видят трафик из других VLAN без соответствующих настроек маршрутизации.
2. **Безопасность и управление**: VLAN позволяют управлять доступом к ресурсам и улучшают безопасность сети, так как они разделяют сеть на отдельные сегменты.
3. **Эффективное использование пропускной способности**: VLAN могут быть использованы для разделения трафика на небольшие группы, что может уменьшить конфликты и улучшить производительность сети.
4. **Улучшение управляемости сети**: Администраторы смогут гибко управлять трафиком, группировать устройства и применять политики безопасности.

# VLAN

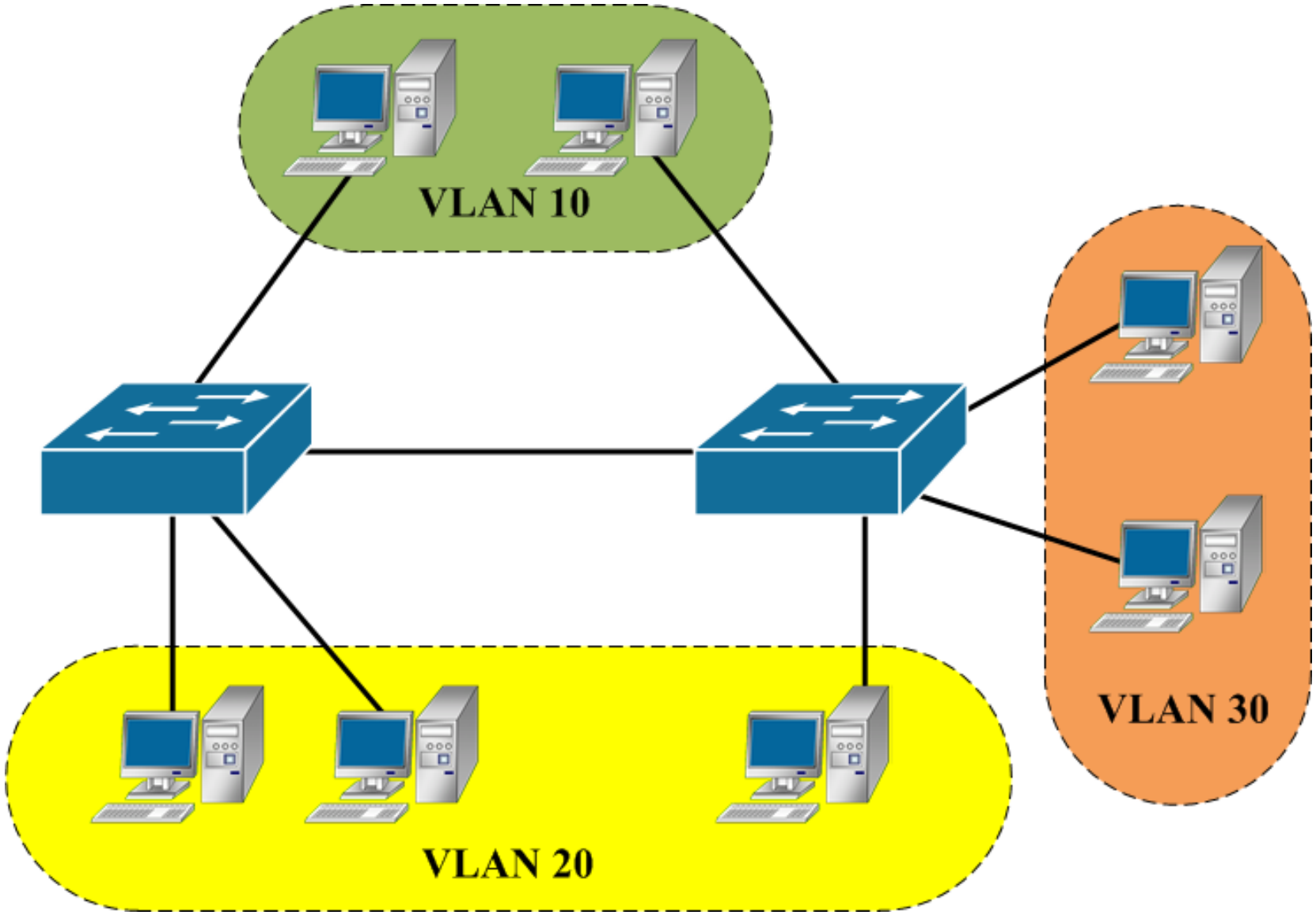
Примеры использования VLAN включают группировку устройств по отделам (например, финансы, маркетинг, IT), разделение голосового и данных трафика для улучшения качества VoIP, а также сегментацию для уменьшения влияния некоторых видов трафика на другие.

Для работы с VLAN требуется сетевое оборудование, поддерживающее эту технологию, например, управляемые коммутаторы.

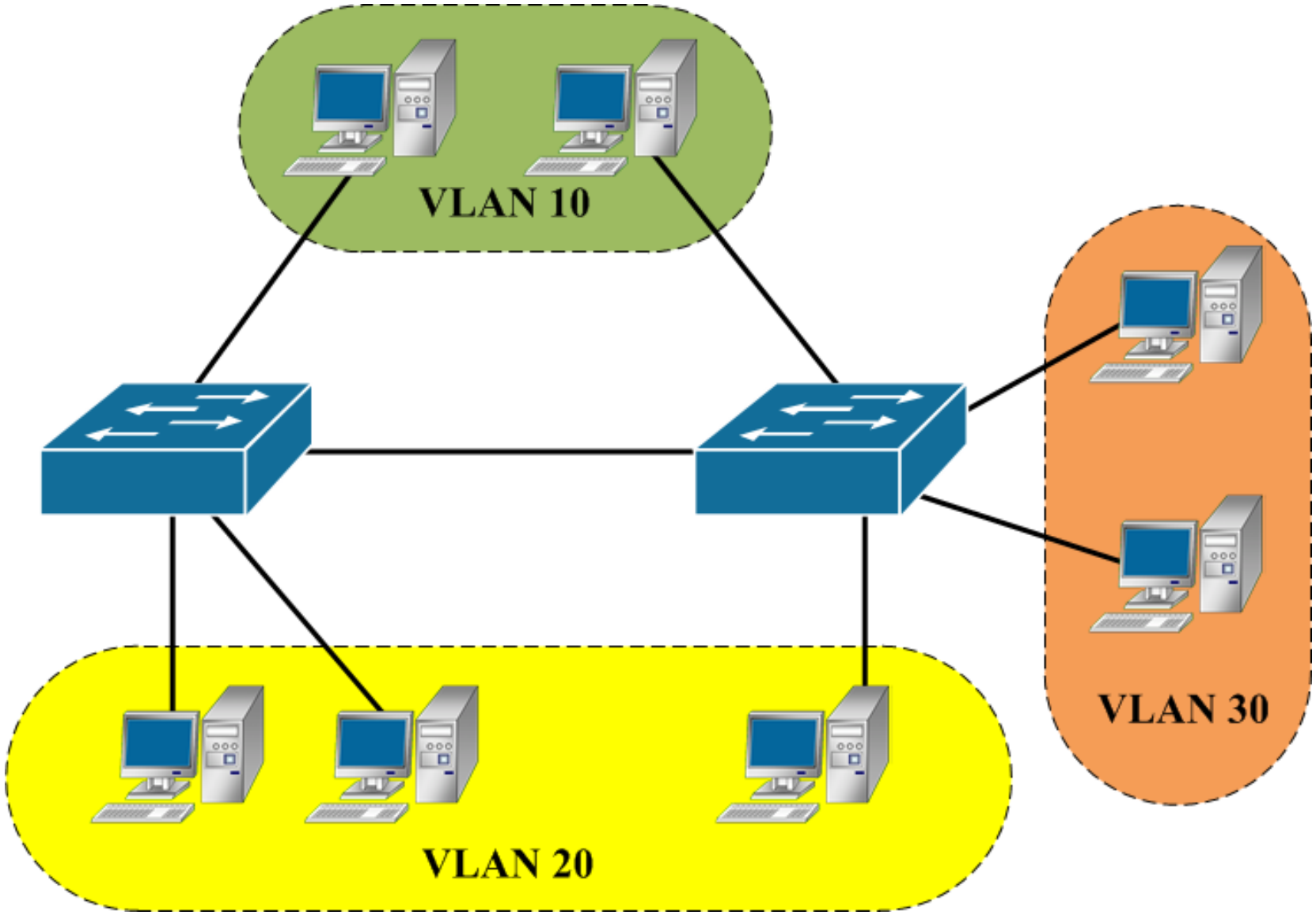
# VLAN



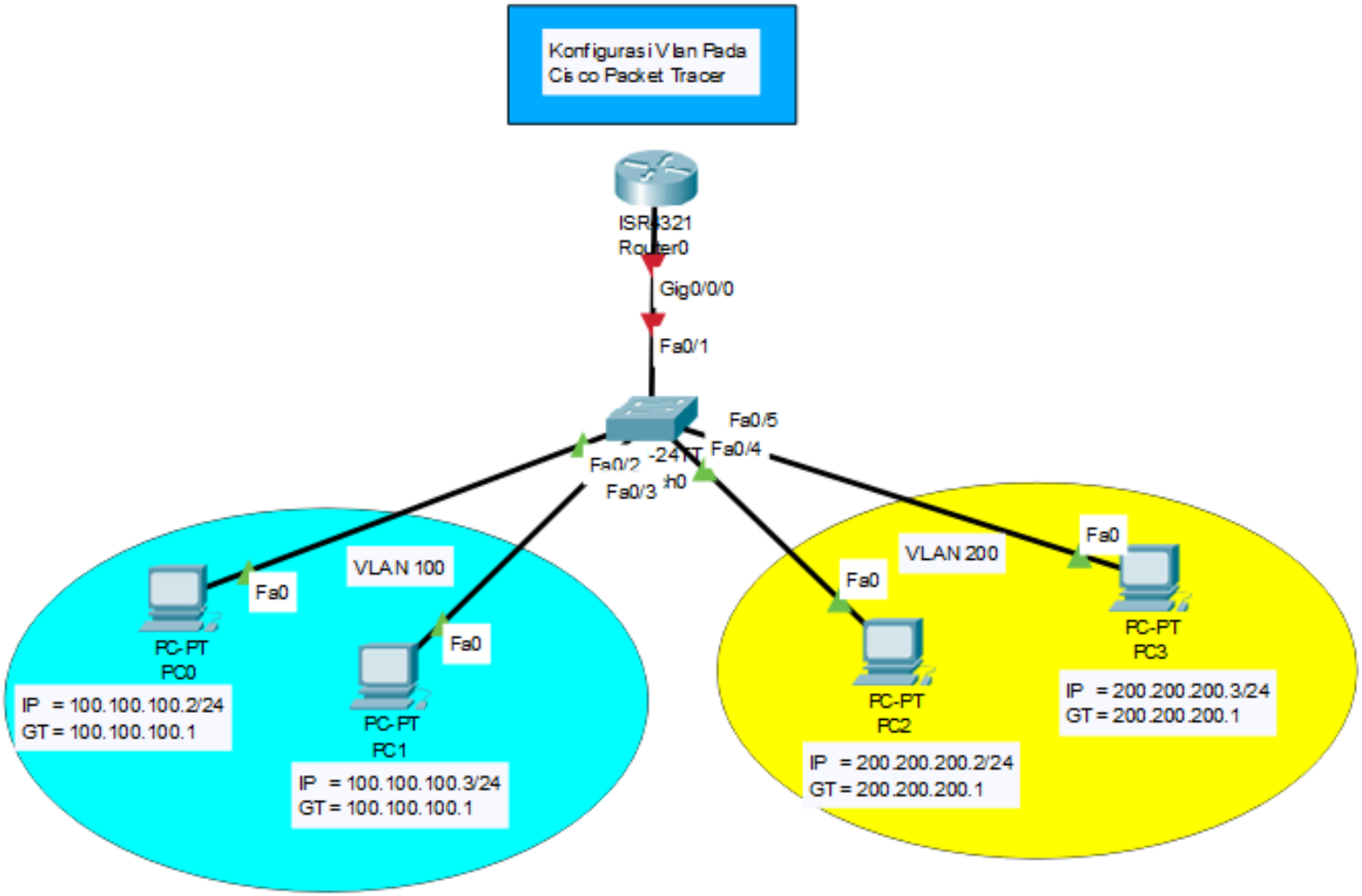
# VLAN



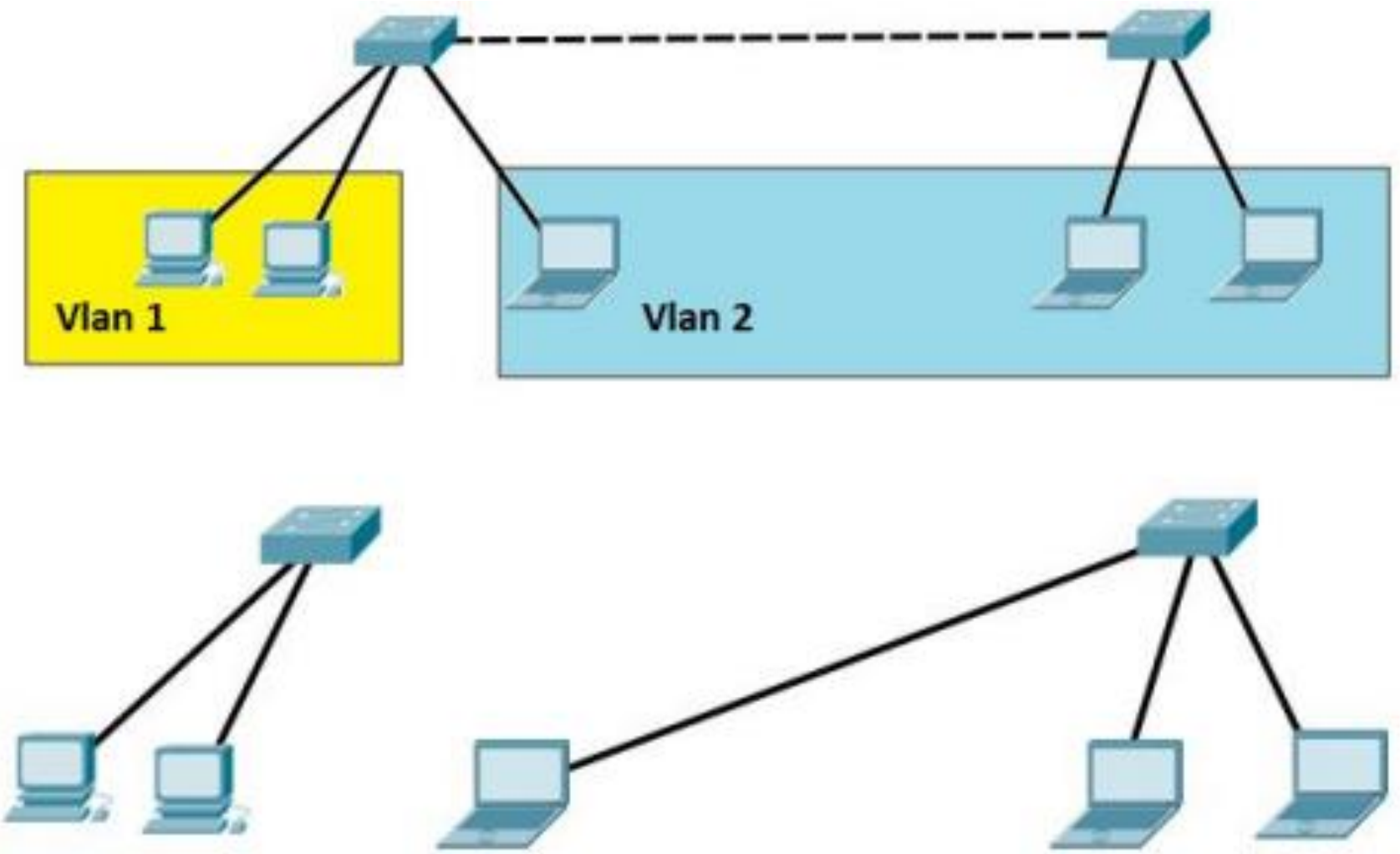
# VLAN



# VLAN


Konfigurasi Vlan Pada
Cisco Packet Tracer
ISR4321
Router0
Gig0/0/0
Fa0/1
Fa0/5
Fa0/4
Fa0/2
Fa0/3
VLAN 100
Fa0
PC-PT
PC0
IP = 100.100.100.2/24
GT = 100.100.100.1
Fa0
PC-PT
PC1
IP = 100.100.100.3/24
GT = 100.100.100.1
VLAN 200
Fa0
PC-PT
PC2
IP = 200.200.200.2/24
GT = 200.200.200.1
Fa0
PC-PT
PC3
IP = 200.200.200.3/24
GT = 200.200.200.1

# VLAN



# VLAN

Количество VLAN, которые могут быть настроены на одном коммутаторе, зависит от нескольких факторов, включая модель и тип коммутатора, а также используемый стандарт VLAN.

В стандарте 802.1Q (который является самым распространенным протоколом для работы с VLAN), теоретически можно создать до 4096 VLAN'ов, однако не все они могут быть использованы практически из-за ограничений.

На практике, многие коммутаторы имеют ограничения на количество активных VLAN. К примеру, некоторые младшие или более дешевые модели коммутаторов могут поддерживать менее 100 активных VLAN.

“Из коробки” все порты коммутатора находятся в VLAN 1.

# VLAN

При проектировании сети нужно решить сколько нужно VLAN и какие компьютеры в них будут, например количество VLAN может совпадать с количеством отделов в организации.

# VLAN инкапсуляция

VLAN инкапсуляция относится к процессу добавления VLAN-тегов к сетевым кадрам внутри локальной сети.

Это позволяет коммутаторам и другому сетевому оборудованию различать и маршрутизировать трафик между различными VLAN.

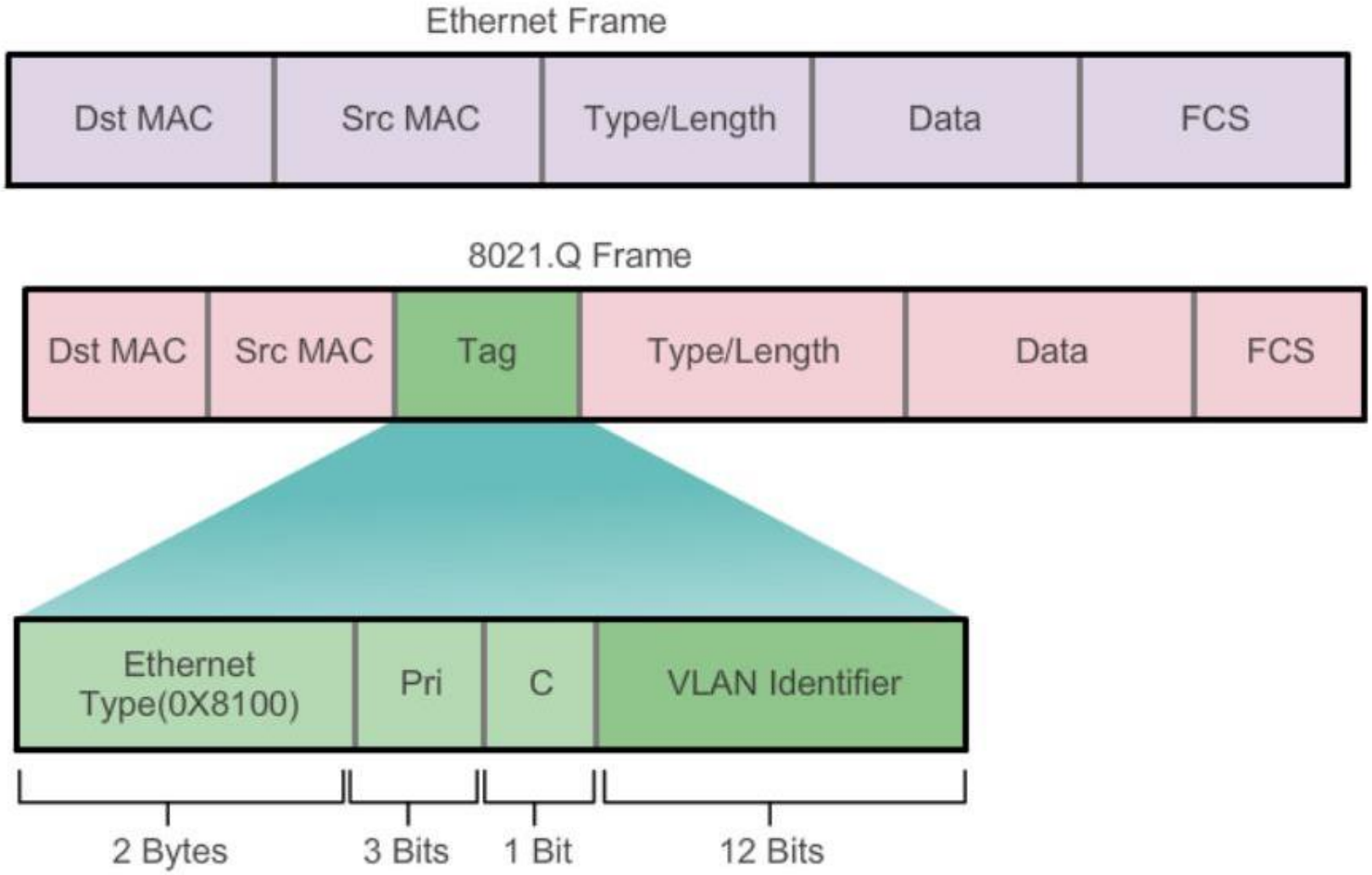
**802.1Q(dot1q)**:

Это наиболее распространенный стандарт для VLAN инкапсуляции.

В этом стандарте 4 байта (32 бита) добавляются в заголовок Ethernet кадра.

Один из этих байтов представляет собой VLAN тег, который содержит идентификатор VLAN (VLAN ID) и информацию о приоритете трафика (QoS).

# VLAN инкапсуляция



# Роли интерфейсов коммутаторов

На коммутаторах существует несколько типов интерфейсов, каждый из которых выполняет свою специфическую роль в сетевом окружении. Вот некоторые из основных ролей интерфейсов на коммутаторе:

**1.Access Port (Доступный порт)(Ethernet)**:

1. Роль: Обычно подключается к конечным устройствам, таким как компьютеры, принтеры или IP-телефоны.
2. Характеристики: Один VLAN может быть назначен к Access порту. Кадры, поступающие с этого порта, не имеют VLAN-тега и считаются принадлежащими к назначенному VLAN.

**2.Trunk Port (Магистральный порт)(dot1q)**:

1. Роль: Обычно соединяется с другими коммутаторами или маршрутизаторами для передачи трафика между VLAN.
2. Характеристики: Поддерживает передачу кадров с VLAN-тегами. Может быть назначено несколько VLAN на один Trunk порт.

# Роли интерфейсов коммутаторов

**3.Hybrid Port (Гибридный порт)**:

1. Роль: Комбинация свойств Access и Trunk порта. Используется для подключения к устройствам, которые могут быть как конечными устройствами, так и другими коммутаторами.
2. Характеристики: Позволяет как передачу кадров с VLAN-тегами, так и работу в одном VLAN (аналогично Access порту).

**4.Port-channel (EtherChannel)**:

1. Роль: Группа физических интерфейсов, объединенных в одну логическую связь для повышения пропускной способности и увеличения отказоустойчивости.
2. Характеристики: Обычно используется для агрегации каналов между коммутаторами.

**5.SVI (Switch Virtual Interface)**:

1. Роль: Интерфейс, представляющий виртуальный интерфейс коммутатора для удаленного управления и конфигурации, а также для пересылки трафика к управляющему приложению.
2. Характеристики: Может быть назначен IP-адрес и работать на уровне сетевого уровня (Layer 3).

# Субинтерфейсы роутера

Субинтерфейсы (Subinterfaces) - это логические интерфейсы, создаваемые на физическом интерфейсе маршрутизатора. Они позволяют одному физическому интерфейсу работать с несколькими VLAN или подсетями, что делает их важными для реализации маршрутизации между виртуальными сетями в сетях с использованием технологий VLAN и 802.1Q тегирования.

Основные характеристики субинтерфейсов:

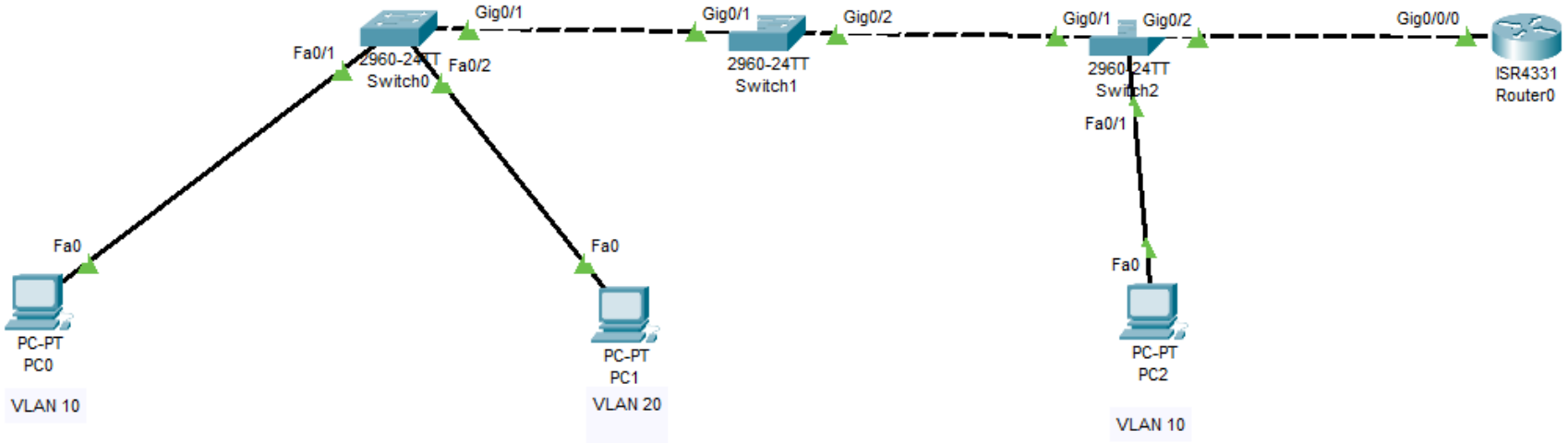
1. **Идентификация субинтерфейса**: Каждый субинтерфейс имеет свой собственный уникальный номер или идентификатор (например, FastEthernet0/0.1, FastEthernet0/0.2 и т.д.).
2. **Принадлежность к VLAN**: Каждый субинтерфейс может быть назначен определенному VLAN, что позволяет маршрутизатору обрабатывать трафик, связанный с этим VLAN.
3. **Назначение IP-адреса**: Субинтерфейсам можно назначать IP-адреса, что позволяет им работать на уровне сетевого уровня (Layer 3) и обеспечивать маршрутизацию между VLAN.
4. **Использование 802.1Q тегов**: Субинтерфейсы часто используются совместно с 802.1Q тегированием для разделения трафика между VLAN.

# Пример использования субинтерфейсов:

Предположим, у вас есть один физический интерфейс на маршрутизаторе, который подключен к коммутатору, и вы хотите, чтобы он обрабатывал трафик из двух разных VLAN: VLAN 10 и VLAN 20. Вы можете создать два субинтерфейса (например, FastEthernet0/0.10 и FastEthernet0/0.20) и назначить им соответствующие VLAN и IP-адреса.

Использование субинтерфейсов позволяет эффективно управлять трафиком между разными VLAN и обеспечивать маршрутизацию в виртуальных сетях.

# Практика


Gig0/1
Gig0/1
Gig0/2
Gig0/1
Gig0/2
Gig0/0/0
Fa0/1
2960-24TT
Switch0
Fa0/2
2960-24TT
Switch1
2960-24TT
Switch2
ISR4331
Router0
Fa0/1
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
VLAN 10
VLAN 20
VLAN 10