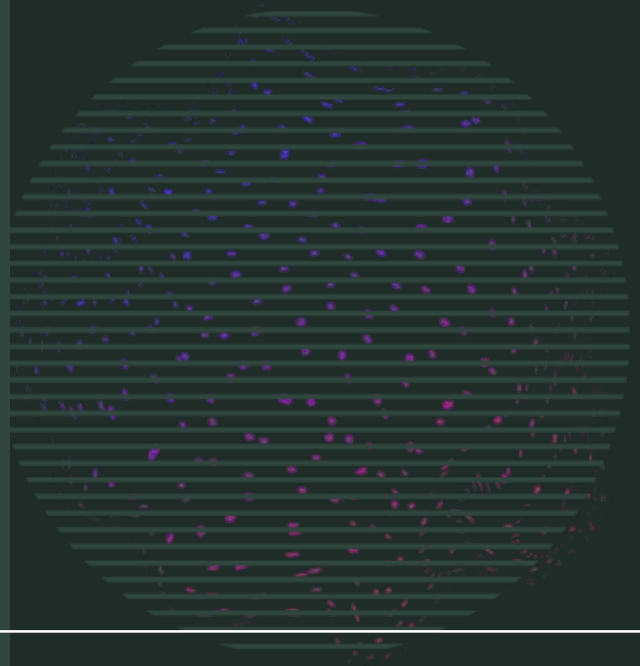
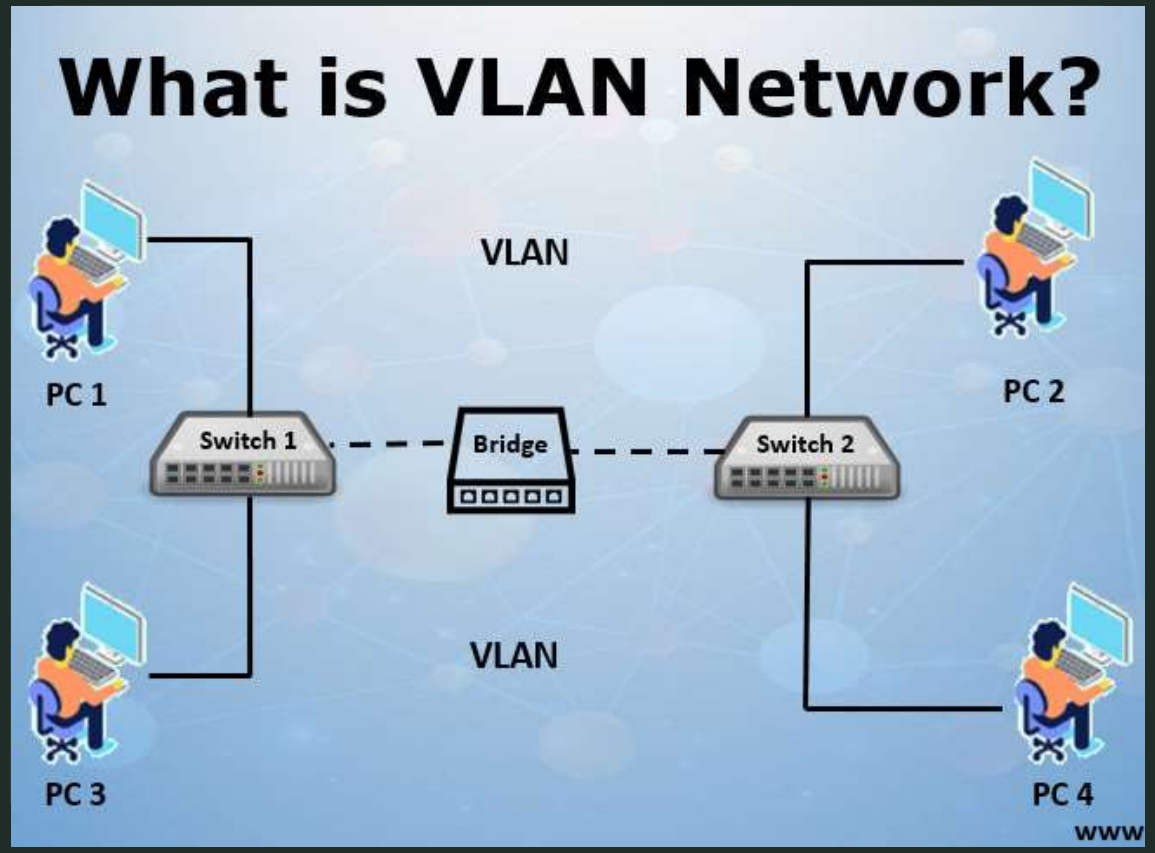
Виртуальные локальные сети(VLAN)

Мансуров Адель 09-231

Содержание



•Введение.
•Основы VLAN.
•Типы VLAN.
•Технологии и протоколы, связанные с VLAN.
•Настройка VLAN на оборудовании.
•Маршрутизация между VLAN.
•Безопасность в VLAN.
•Лучшие практики проектирования VLAN.
•Совеременные тенденции и будущее развитие VLAN
•Реальные примеры использования VLAN.
•Заключение.
•Тест.



Введение. Что такое VLAN

Определение VLAN:
Логическое разделение сети на уровне 2 модели OSI для изоляции устройств и оптимизации работы сети.

История:

•Появление технологии для сокращения широковещательного трафика.

•Стандарт IEEE 802.1Q (1998): основа для работы VLAN.

Актуальность:

•Управление сложными сетями.

•Повышение безопасности.

•Оптимизация трафика.

•Масштабируемость и интеграция с SDN.

Модель OSI

•Что такое модель OSI?

- Эталонная семиуровневая модель взаимодействия сетевых устройств.

•Семь уровней:

- Physical (кабели, сигналы), Data Link (MAC, VLAN), Network (IP), Transport (TCP, UDP), Session, Presentation, Application.

•Роль в VLAN:

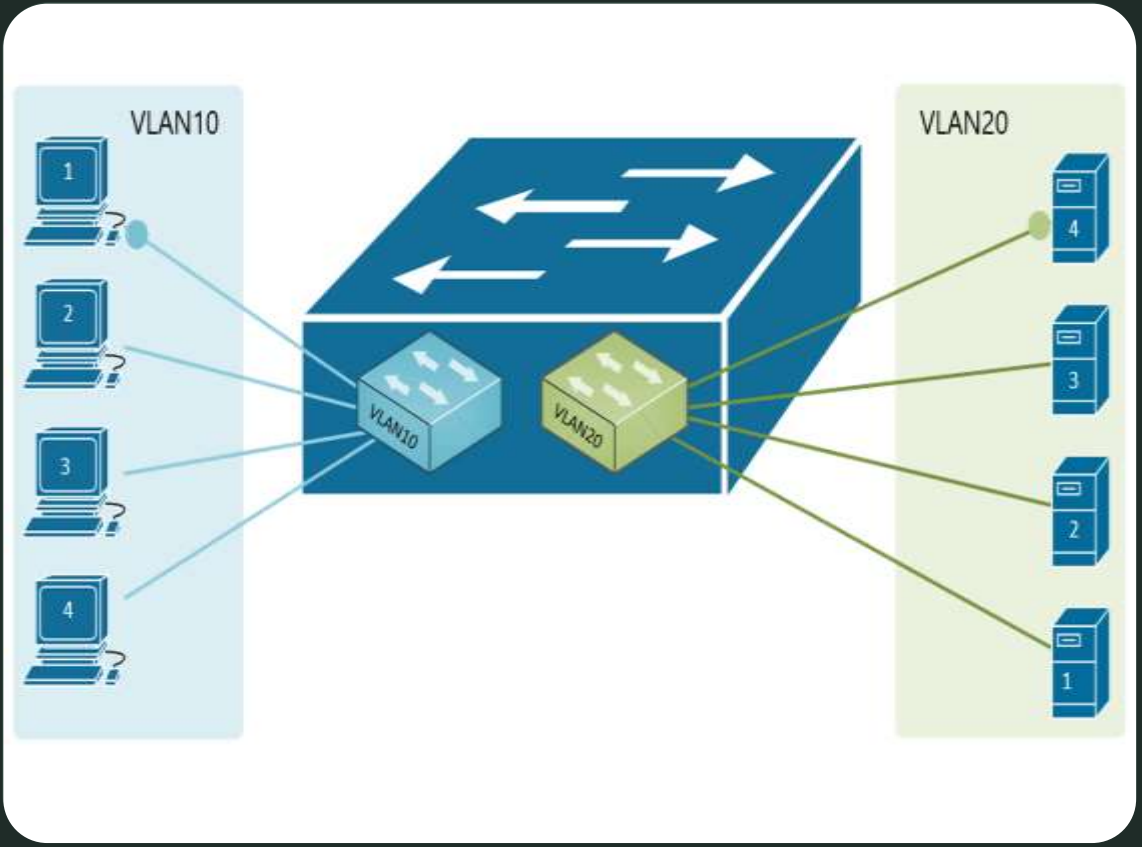
- VLAN работают на уровне 2 (Data Link).
- Между VLAN маршрутизация происходит на уровне 3 (Network).

•Зачем нужна OSI?

- Стандартизация, упрощение проектирования сетей, диагностика проблем.

Основы VLAN

- **Модель OSI и VLAN:**
  - Работают на уровне 2 OSI (канальный уровень).
  - Связь с уровнем 3 для маршрутизации между VLAN.
- **Принципы логической сегментации:**
  - Разделение сети без физического изменения.
  - Ограничение широковещательного трафика внутри VLAN.
  - Типы портов: Access и Trunk.
- **Сравнение с физической сегментацией:**
  - VLAN дешевле, гибче и масштабируемее.
  - Изоляция данных с минимальными затратами на оборудование.



Data и Default VLAN

Data VLAN:

•Логическое разделение пользователей и трафика.

•Улучшение безопасности и QoS.

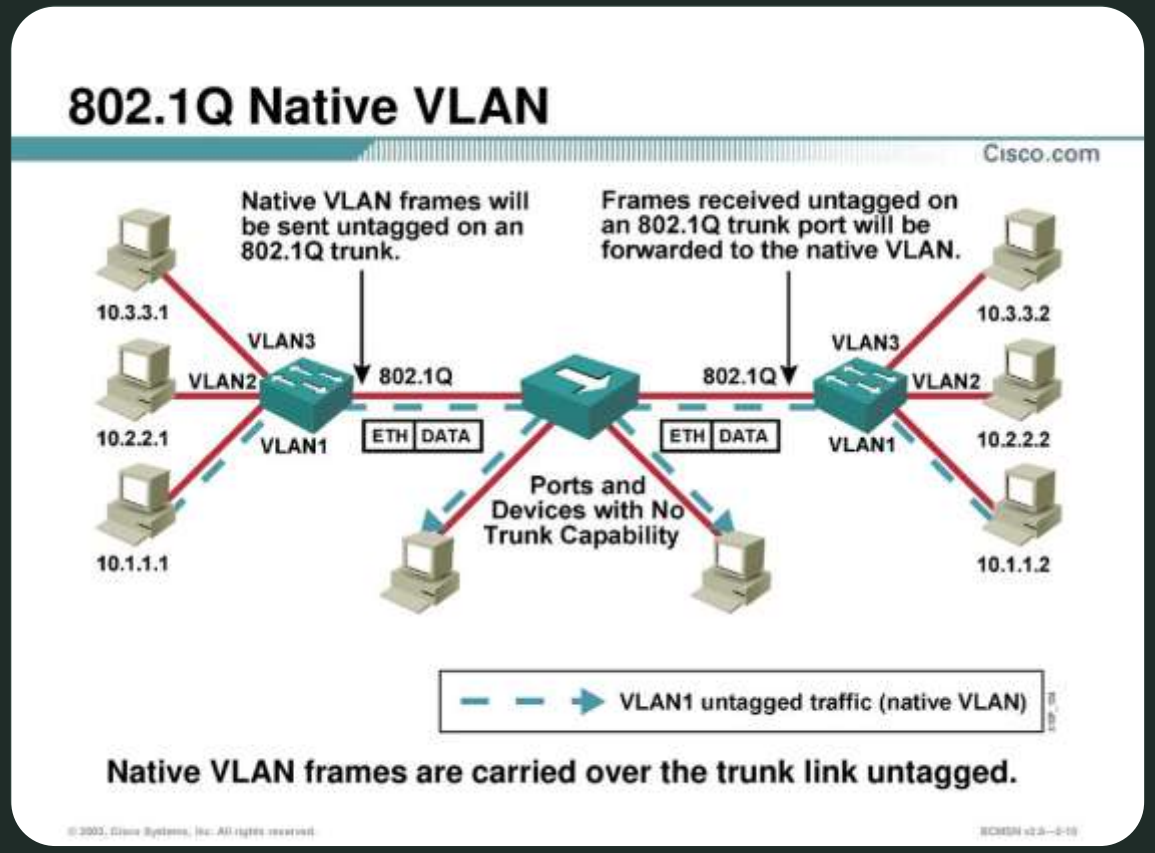
•Пример: VLAN 10 для IT, VLAN 20 для бухгалтерии.

Default VLAN:

•VLAN по умолчанию (обычно VLAN 1).

•Используется для служебного трафика (STP, CDP).

•Не рекомендуется для рабочих данных из-за рисков безопасности.



Management и Native VLAN

Management VLAN:

•VLAN для управления устройствами (SSH, SNMP).

•Пример: VLAN 100 для изоляции административного трафика.

Native VLAN:

•Обрабатывает нетегированный трафик на Trunk-портах.

•Рекомендуется использовать номера, отличные от VLAN 1, для защиты.

Voice, Security и Private VLAN

Voice VLAN:

•Минимизация задержек и потерь для VoIP.

•Пример: VLAN 150 для IP-телефонов.

Security VLAN:

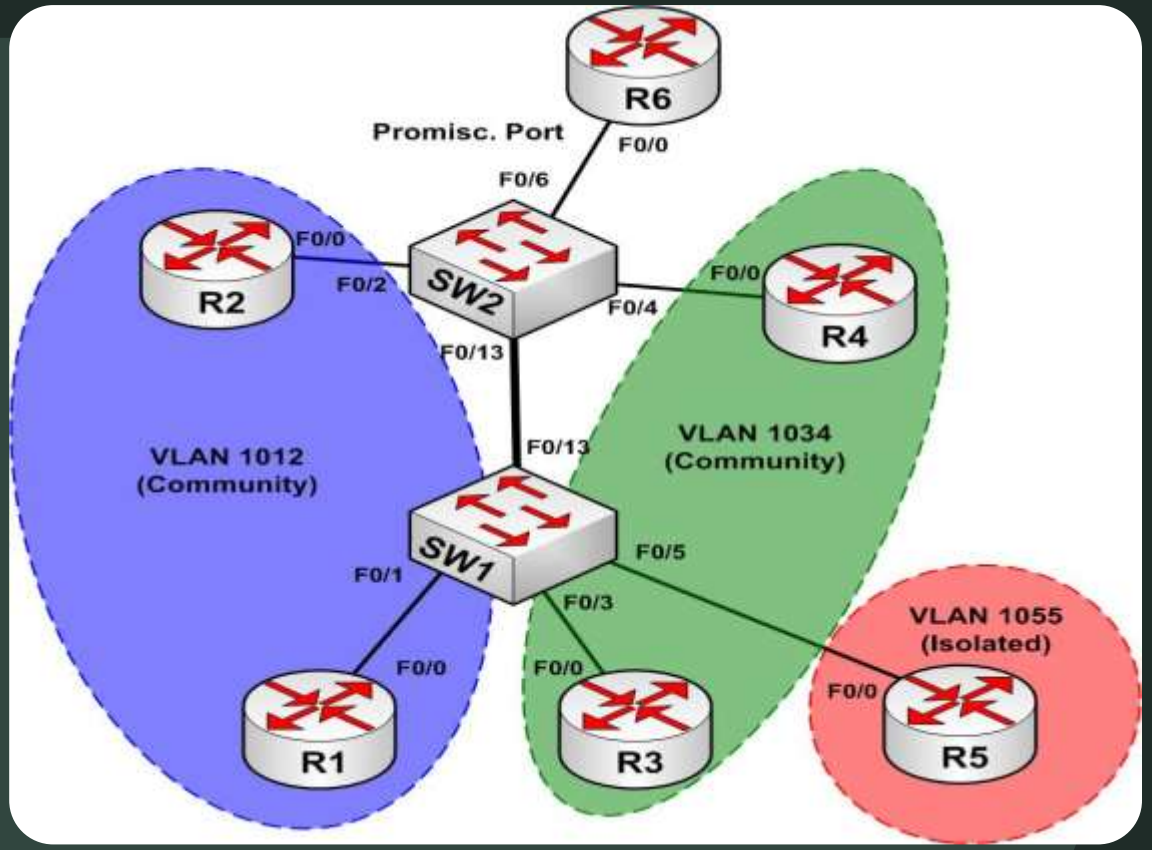
•Изоляция критически важных данных.

•Пример: VLAN 200 для финансовых серверов.

Private VLAN:

•Изоляция устройств внутри VLAN.

•Пример: Isolated и Community VLAN в дата-центрах.



IEEE 802.1Q и Trunking

•**IEEE 802.1Q:**

•Добавляет тег VLAN к Ethernet-кадру.

•Поля: TPID, PCP, CFI, VLAN ID.

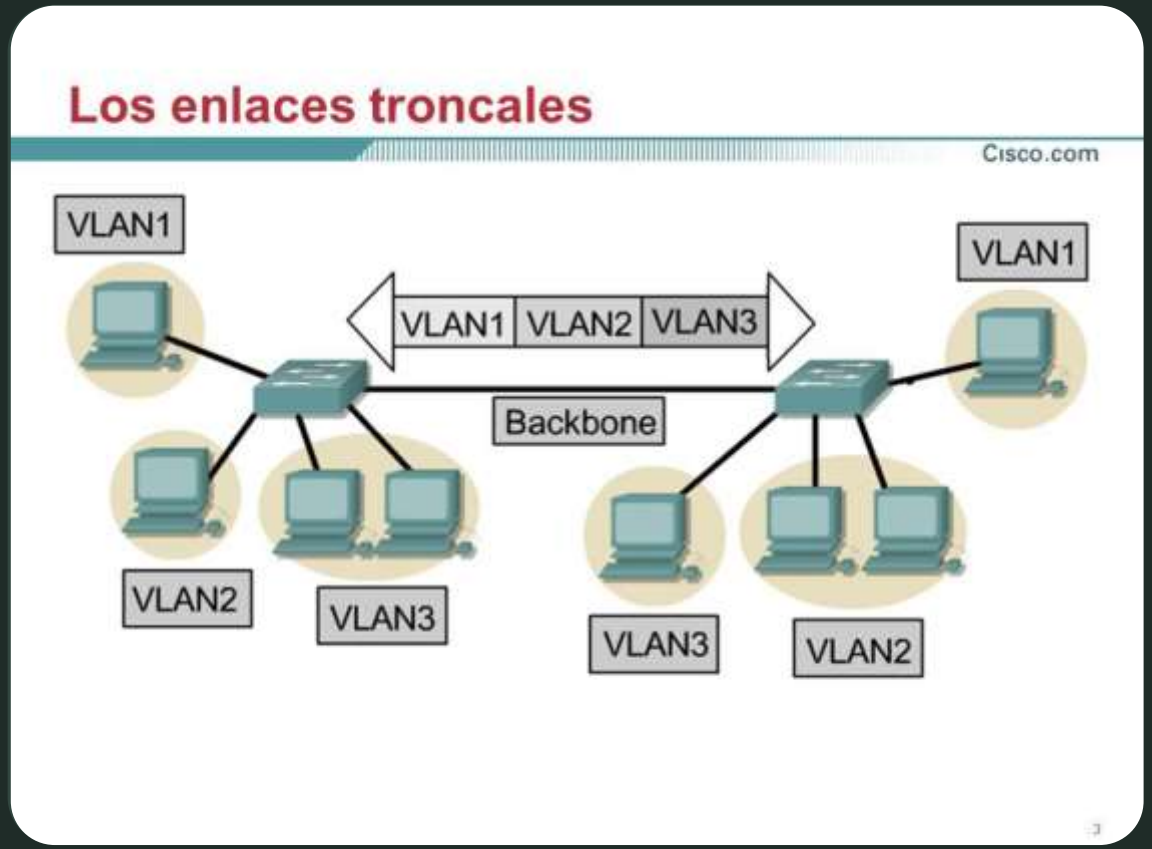
•Поддерживает до 4094 VLAN.

•**Trunking**:

•Позволяет передавать трафик из нескольких VLAN через один порт.

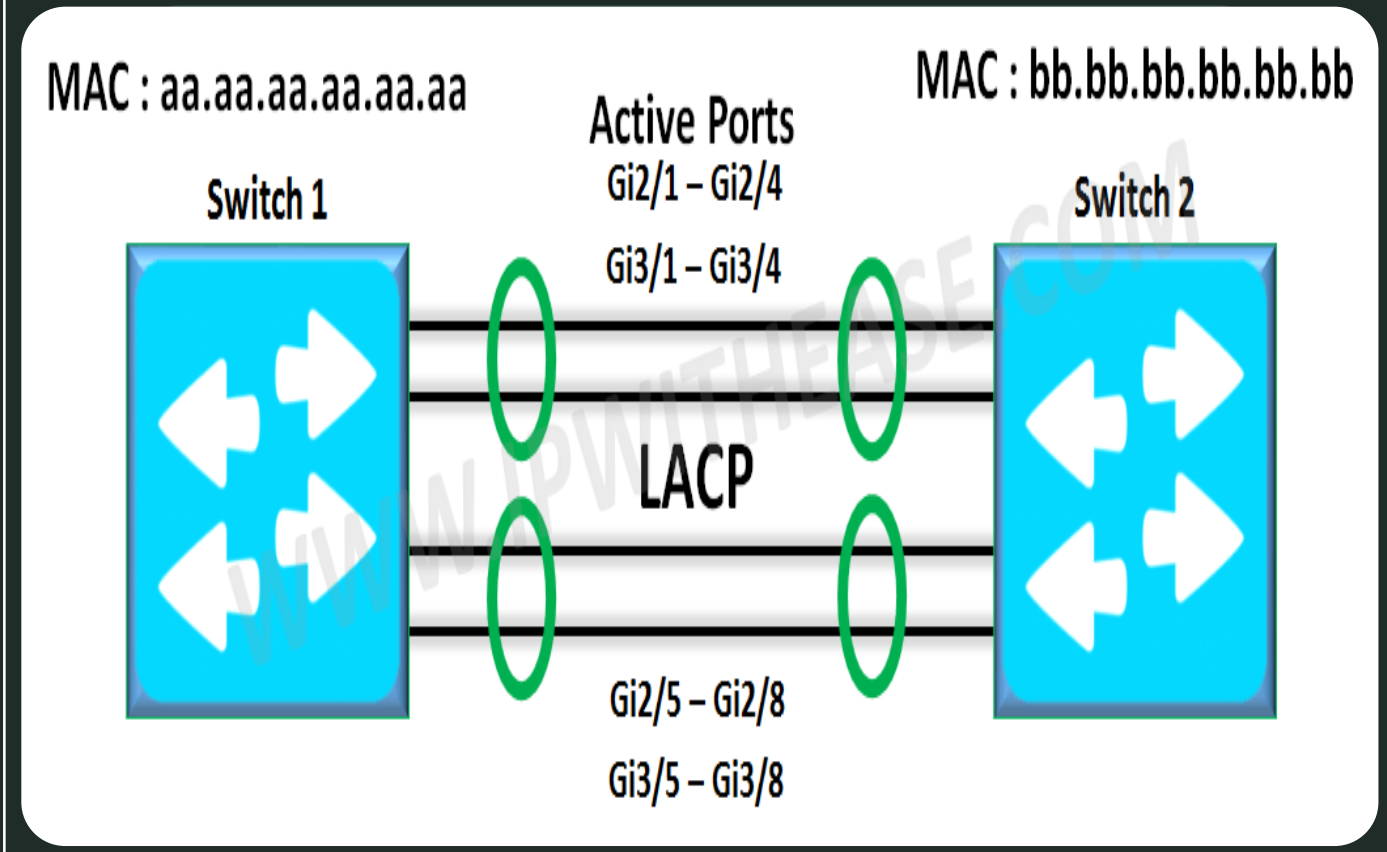
•Использует тегирование 802.1Q.

•Важна настройка Native VLAN для обработки нетегированных кадров.



Протоколы VTP и GVRP, QinQ (802.1ad) — стекирование VLAN

- **GVRP:**
  - Стандартный протокол (IEEE 802.1Q).
  - Динамическая регистрация и удаление VLAN.
  - Используется в сетях с оборудованием разных производителей.
- **VTP:**
  - Проприетарный протокол Cisco.
  - Централизованное управление VLAN.
  - Режимы работы: Server, Client, Transparent.
  - Версии: VTPv1, VTPv2, VTPv3.



QinQ и LACP

•QinQ (802.1ad):

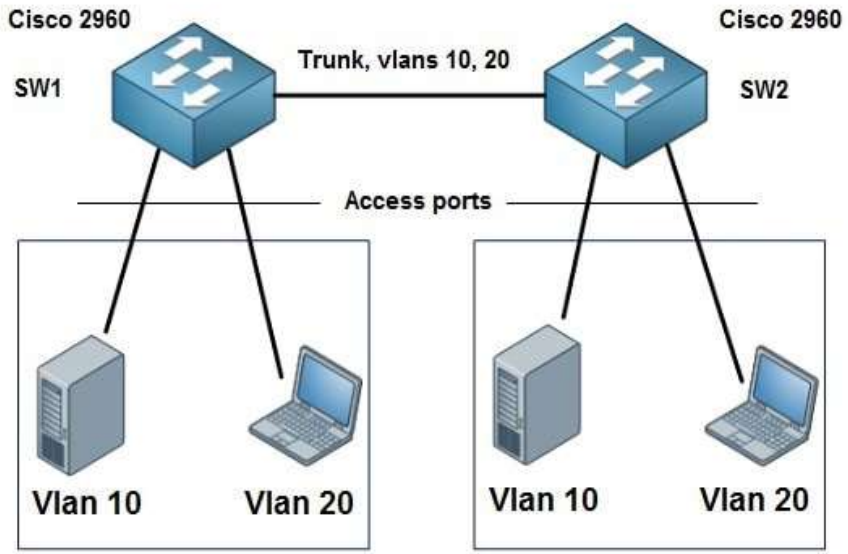
- Двойное тегирование для масштабируемости и изоляции.
- Теги: C-VLAN (внутренний) + S-VLAN (внешний).
- Применение: ISP, дата-центры.

•LACP (802.3ad):

- Объединяет несколько физических соединений в один логический канал.
- Преимущества: балансировка нагрузки, отказоустойчивость, увеличение пропускной способности.
- Применение: серверы, межкоммутаторные связи.

Оборудование Cisco

- **Cisco VLAN:**
- Этапы: создание VLAN, настройка Access- и Trunk-портов.
- Trunk использует тегирование 802.1Q.
- Inter-VLAN Routing через Layer 3-коммутаторы.



Использование программных коммутаторов и виртуальных сред

Программные коммутаторы:

- Open vSwitch: VLAN, OpenFlow, SDN.
- Cisco Nexus 1000V: интеграция с VMware ESXi.
- Hyper-V Virtual Switch: VLAN ID, защита от spoofing.

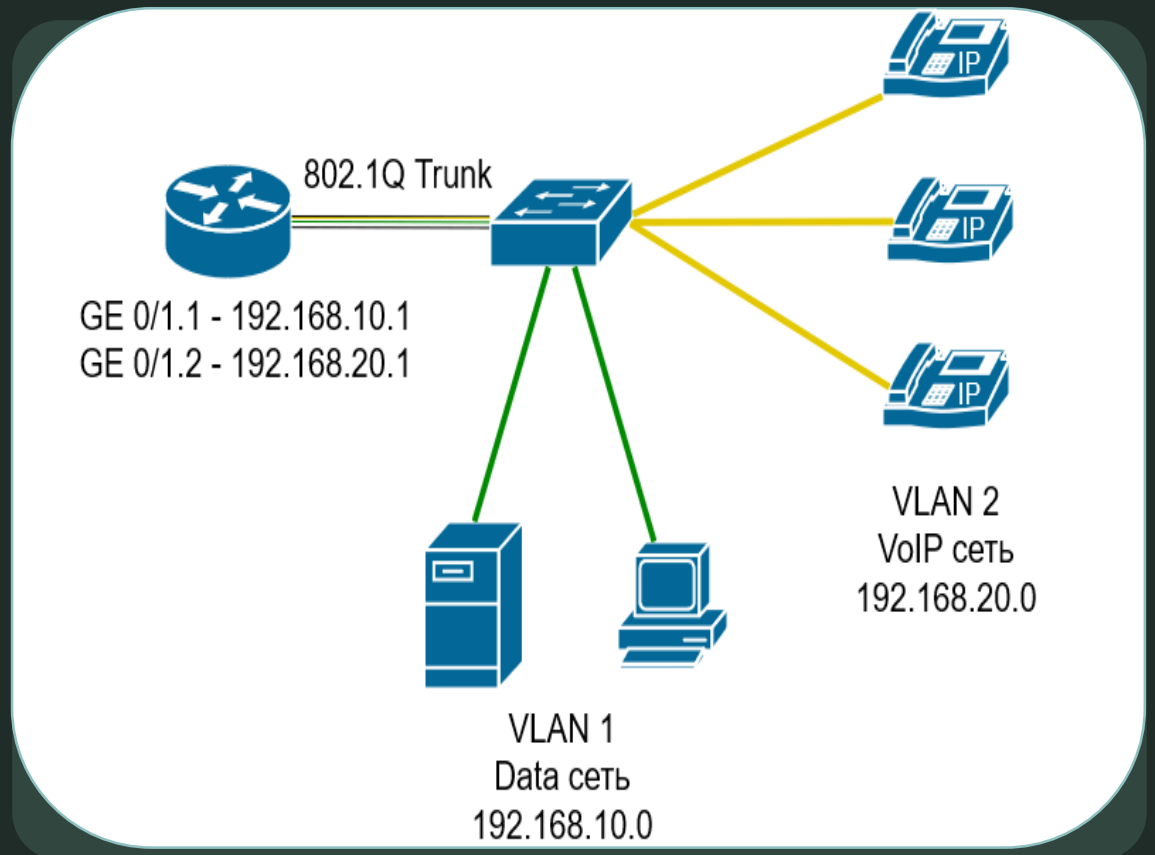
Виртуальные среды:

- VMware: VLAN через Distributed vSwitch.
- Hyper-V: VLAN ID и Network Virtualization Overlay.
- OpenStack: Open vSwitch, поддержка VXLAN.

Преимущества:

- Гибкость, экономичность, масштабируемость.
- Применение в дата-центрах, облачных средах и тестовых лабораториях.

Маршрутизация между VLAN



Маршрутизация между VLAN:

•Router-on-a-Stick:

- Маршрутизация через один интерфейс маршрутизатора.
- Преимущества: экономичность, простота настройки.
- Недостатки: ограниченная производительность.

•Многослойные коммутаторы:

- Маршрутизация на Layer 3 Switch.
- Преимущества: высокая производительность, снижение задержек.
- Применение: корпоративные сети.

•SVI (Switch Virtual Interfaces):

- Логический интерфейс для каждой VLAN.
- Высокая скорость маршрутизации, интеграция функций безопасности.
- Применение: кампусы, дата-центры.

Безопасность в VLAN

Угрозы безопасности:

•VLAN Hopping: Double Tagging, Switch Spoofing.

•MAC Flooding: затопление таблицы MAC.

Методы защиты:

•Настройка Native VLAN: используйте уникальную VLAN для нетегированного трафика.

•Private VLANs: изоляция устройств в одной VLAN.

Лучшие практики:

•Отключение DTP и неиспользуемых портов.

•Включение Port Security для защиты таблиц MAC.

•Использование ACL и Management VLAN для изоляции трафика.

Лучшие практики проектирования VLAN

- **Иерархический дизайн сети:** Три уровня: Core, Distribution, Access.
- Оптимизация маршрутизации и масштабируемость.
- **Минимизация VLAN на коммутатор:** Ограничение количества VLAN для уменьшения широковещательного трафика.
- Привязка VLAN к физическим зонам.
- **Управление таблицами MAC:** Удаление неиспользуемых записей.
- Баланс между производительностью и безопасностью.
- **Документирование и мониторинг:** Фиксация структуры VLAN и связанных устройств.
- Использование инструментов мониторинга (SNMP, NetFlow).

VXLAN и его преимущества

•VXLAN: Протокол туннелирования, использующий 24-битный идентификатор VNI, что позволяет создавать до 16 миллионов изолированных сетевых сегментов.

•Масштабируемость: Преодолевает ограничение VLAN в 4094 ID, поддерживая крупные дата-центры и многопользовательские среды.

•Инкапсуляция: VXLAN использует MAC-in-UDP инкапсуляцию, передавая трафик уровня 2 поверх IP-сетей уровня 3.

•Гибкость: Обеспечивает связь между серверами и виртуальными машинами, независимо от их физического расположения.

Роль VLAN в программно-определяемых сетях (SDN)

- **Централизованное управление:** В SDN VLAN управляются контроллерами, что упрощает создание, удаление и изменение параметров в реальном времени.
- **Автоматизация:** Процессы настройки VLAN автоматизируются, минимизируя ошибки и ускоряя внедрение новых сервисов.
- **Микросегментация:** Позволяет изолировать трафик на уровне приложений, усиливая безопасность и контроль доступа.
- **Интеграция с VXLAN:** SDN-контроллеры управляют VXLAN-оверлеями, упрощая масштабируемую сегментацию в больших сетях.

Влияние облачных технологий на развитие VLAN

Текущее влияние:

•Облачные VLAN позволяют создавать изолированные сегменты внутри виртуальных сетей (VPC, VNet).

•Используются технологии туннелирования (VXLAN, NVGRE) для сегментации поверх IP-сетей.

Примеры:

•AWS VPC: настройка изолированных сегментов для приложений.

•Azure Virtual Network: интеграция VLAN с облачными сервисами.

Будущее VLAN:

•Интеграция с SDN для автоматизации и масштабирования.

•Использование технологий, таких как VXLAN, Geneve и AI-управление.

Корпоративные сети

VLAN используются для разделения трафика между отделами (например, бухгалтерия, продажи, ИТ, гости).

Обеспечивается изоляция данных, безопасность, управляемость и снижение широковещательного трафика.

Пример: VLAN 10 — бухгалтерия, VLAN 20 — продажи, VLAN 30 — ИТ, VLAN 40 — гостевая сеть.

Дата-центры

VLAN применяются для изоляции трафика между клиентами (арендаторами) и уровнями инфраструктуры.

Технологии VXLAN используются для преодоления ограничений традиционных VLAN, обеспечивая масштабируемость.

Пример: VLAN 100 для клиента A, VLAN 200 для клиента B, VLAN 300 для клиента C.

Поставщики услуг(ISP). Примеры из практики

VLAN обеспечивают разделение трафика различных услуг (интернет, IPTV, VoIP) и клиентов.

Улучшается качество обслуживания (QoS) и безопасность благодаря изоляции и управлению трафиком.

Пример: VLAN 50 — интернет-доступ, VLAN 60 — IPTV, VLAN 70 — VoIP.

Университет: VLAN сегментируют студентов, преподавателей и администрацию (VLAN 10, VLAN 20, VLAN 30).

Гостиница: VLAN создаёт изолированную гостевую сеть для доступа в интернет, защищая внутренние ресурсы отеля.

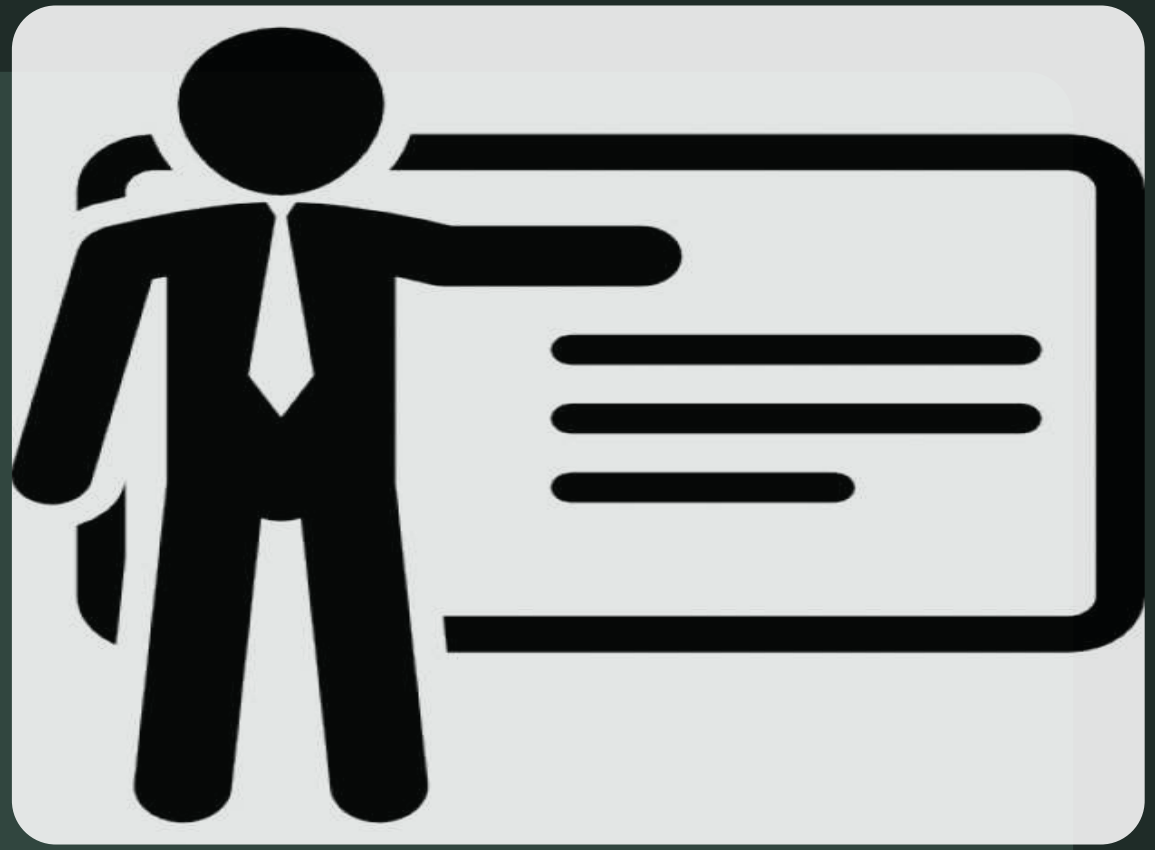
Рекомендации по использованию VLAN

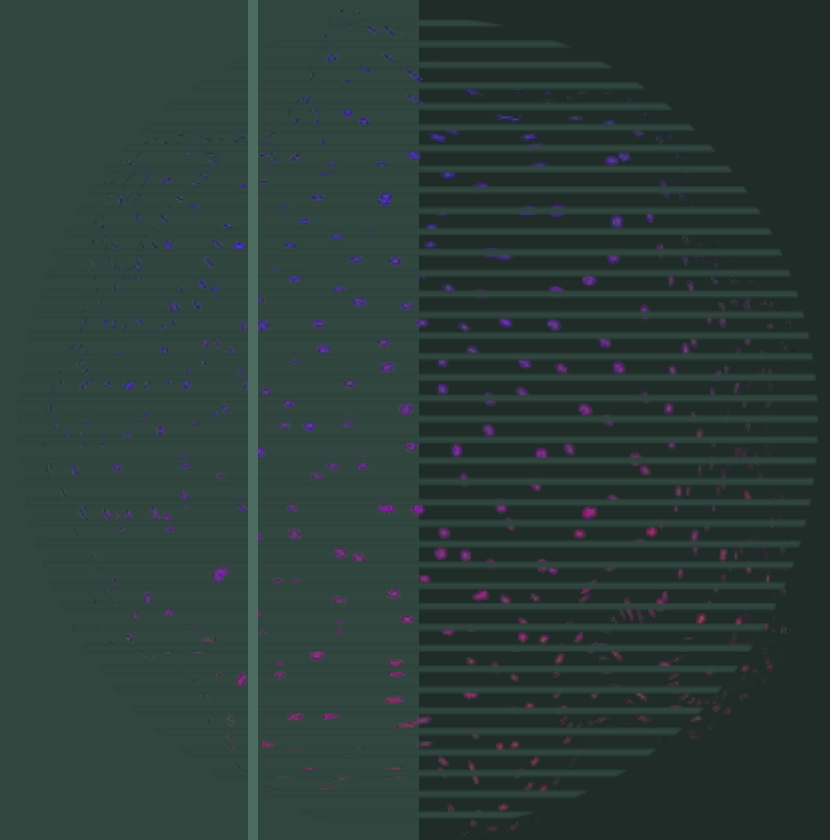
Проектирование: Спланируйте количество VLAN и используйте иерархическую структуру сети.

Безопасность: Настройте Native VLAN, используйте PVLAN и ограничьте доступ с помощью Port Security.

Масштабируемость: Применяйте VXLAN для больших сетей и интеграцию с SDN для автоматизации.

Мониторинг: Используйте инструменты для анализа и контроля трафика.





Заключение

Значение VLAN: Повышают изоляцию, безопасность и управляемость сетей.

Технологии: VXLAN и SDN расширяют возможности традиционных VLAN.

Использование: Корпорации, дата-центры и провайдеры активно внедряют VLAN.

Будущее: Автоматизация и интеграция с облачными сервисами.

TEST

Вопрос 1: Что такое VLAN?

a) Устройство для ускорения интернета
b) Логическое разделение сети на уровне 2 модели OSI
c) Протокол маршрутизации между сетями
d) Физический сегмент сети

Вопрос 2: **Какая основная задача VLAN?**

a) Увеличение скорости интернет-соединения
b) Логическая сегментация сети для изоляции трафика
c) Снижение задержек в широковещательной сети
d) Обеспечение беспроводного доступа

Вопрос 3: Какой стандарт используется для тегирования трафика в VLAN?

a) IEEE 802.1X
b) IEEE 802.3ad
c) IEEE 802.1Q
d) IEEE 802.11

Вопрос 4: Что происходит, если на Trunk-порту разрешена только одна VLAN?

a) Trunk-порт работает как Access-порт
b) Трафик передается без тегирования
c) Trunk-порт не передает трафик
d) Передается только трафик из указанной VLAN

Вопрос 5: Какая основная цель использования Native VLAN?

a) Для передачи нетегированного трафика
b) Для маршрутизации между VLAN
c) Для создания изолированных сегментов
d) Для передачи данных только в гостевой сети

Вопрос 6: Какую функцию выполняет DTP (Dynamic Trunking Protocol)?

a) Автоматическое определение Native VLAN
b) Переключение портов между режимами Access и Trunk
c) Управление таблицами MAC-адресов
d) Настройка QoS для трафика

Вопрос 7: Какое преимущество имеет VXLAN перед традиционными VLAN?

a) Поддержка до 16 миллионов сегментов вместо 4094
b) Ускорение маршрутизации на Layer 2
c) Упрощение настройки Access-портов
d) Отсутствие необходимости использования маршрутизаторов

Вопрос 8: Что делает протокол VTP (VLAN Trunking Protocol)?

a) Передает трафик между VLAN
b) Управляет VLAN на нескольких коммутаторах
c) Создает изолированные сегменты VLAN
d) Ограничивает MAC-адреса на порту

Вопрос 9: Какова роль SVI (Switch Virtual Interface) в сети?

a) Передача нетегированного трафика между VLAN
b) Логический интерфейс для маршрутизации между VLAN
c) Обеспечение безопасности Trunk-портов
d) Настройка QoS для VLAN

Вопрос 10: Почему рекомендуется использовать Management VLAN?

a) Для передачи только широковещательного трафика
b) Для изоляции служебного трафика управления коммутатором
c) Для маршрутизации трафика между VLAN
d) Для хранения резервных копий конфигурации

Вопрос 11: Какую проблему решает использование Private VLAN (PVLAN)?

a) Позволяет изолировать устройства внутри одной VLAN
b) Увеличивает пропускную способность Trunk-портов
c) Снижает количество MAC-адресов в таблице коммутатора
d) Упрощает настройку межсетевых экранов

Вопрос 12: Какие ограничения имеет VLAN на основе IEEE 802.1Q?

a) Поддержка только широковещательного трафика
b) Ограничение числа VLAN до 4094
c) Невозможность работы на коммутаторах Layer 3
d) Требование отдельных физических портов для каждой VLAN

Вопрос 13: Почему VXLAN использует MAC-in-UDP инкапсуляцию?

a) Для улучшения производительности маршрутизации
b) Чтобы передавать трафик уровня 2 поверх IP-инфраструктуры
c) Для увеличения количества доступных MAC-адресов
d) Чтобы исключить использование Native VLAN

Вопрос 14: Какая главная роль SDN в управлении VLAN?

a) Создает физические сети поверх логических VLAN
b) Централизует управление и автоматизирует конфигурацию VLAN
c) Увеличивает размер таблицы MAC-адресов
d) Настраивает VLAN только на Access-портах

Вопрос 15: Какие технологии обеспечивают масштабируемость и гибкость VLAN в дата-центрах?

a) STP и PVLAN
b) VTP и DTP
c) VXLAN и SDN
d) QoS и DHCP