Лабораторная работа №5

Тема: Виртуальные локальные сети

Цель работы

Научиться:

- делить сеть на виртуальные локальные сети **VLAN**;
- назначать порты коммутатора в нужные VLAN;
- настраивать **trunk** между устройствами;
- организовывать связь между VLAN через **router-on-a-stick**;
- проверять работу сети командами диагностики.

VLAN

Технология VLAN, или Virtual Local Area Network, представляет собой механизм логической сегментации коммутируемой сети, при котором одна и та же физическая инфраструктура разделяется на несколько независимых широковещательных доменов. В терминологии Cisco VLAN рассматривается как логическая сеть, формируемая по функциональному, организационному или прикладному признаку, а не по физическому расположению узлов. Такое разделение позволяет объединять устройства в одну сеть даже тогда, когда они подключены к разным коммутаторам и размещены в различных частях инфраструктуры. IEEE относит подобные механизмы к области VLAN-aware bridging, то есть к управляемой передаче кадров в мостовых сетях с учётом принадлежности к виртуальной локальной сети.

С инженерной точки зрения VLAN выполняет три ключевые функции. Во-первых, она ограничивает распространение широковещательного трафика пределами одного логического домена, что уменьшает лишнюю нагрузку на коммутируемую среду. Во-вторых, VLAN усиливает сетевую изоляцию, поскольку станции из разных VLAN не обмениваются кадрами напрямую на втором уровне модели OSI. В-третьих, VLAN упрощает эксплуатацию сети: изменение логической принадлежности узла осуществляется программно, через переназначение порта, без физической перекоммутации. В официальной документации Cisco подчёркивается, что каждая VLAN функционирует как отдельный broadcast domain, а связь между разными VLAN требует участия устройства третьего уровня.

Практически это означает, что порт коммутатора, назначенный определённой VLAN, передаёт пользовательский трафик в рамках только этой виртуальной сети. В классической схеме access-порт ассоциируется с одной VLAN и используется для подключения конечного устройства, тогда как сама VLAN обычно соотносится с отдельной IP-подсетью. Это соответствие не является обязательным по природе

технологии, однако в большинстве учебных и эксплуатационных сценариев одна VLAN проектируется как один логический сегмент второго уровня и одна подсеть третьего уровня.

Основные причины использования VLAN:

- разделение пользователей по отделам или функциям;
- уменьшение широковещательного трафика;
- повышение безопасности;
- упрощение администрирования сети.

Например, можно создать:

- VLAN 10 — бухгалтерия;
- VLAN 20 — продажи;
- VLAN 30 — IT-отдел.

Тогда устройства внутри одной VLAN смогут обмениваться кадрами напрямую на уровне коммутатора, а устройства из разных VLAN без маршрутизации друг друга видеть не будут.

Trunk

Если VLAN существует не на одном коммутаторе, а распределена между несколькими устройствами, возникает необходимость передавать трафик нескольких виртуальных сетей по одному физическому соединению. Для этой цели используется trunk-соединение. В документации Cisco trunk определяется как point-to-point link, по которому передаётся трафик сразу нескольких VLAN. Иными словами, trunk не принадлежит одной пользовательской VLAN, а выступает транспортным каналом для набора VLAN между коммутаторами либо между коммутатором и маршрутизатором.

Стандартной технологией идентификации VLAN на trunk-канале служит IEEE 802.1Q. Этот стандарт предусматривает вставку в Ethernet-кадр дополнительного четырёхбайтового тега, содержащего информацию о принадлежности кадра к конкретной VLAN; после вставки тега устройство пересчитывает контрольную последовательность кадра, а на принимающей стороне тег удаляется, после чего кадр направляется в соответствующую VLAN. IEEE 802.1Q, согласно описанию стандарта IEEE, задаёт общие принципы работы мостовых сетей и VLAN Bridges, а Cisco уточняет прикладной механизм тэгирования кадров на trunk-портах.

Особого внимания заслуживает понятие native VLAN. В классической реализации 802.1Q трафик native VLAN передаётся по trunk-соединению без тега, тогда как кадры остальных VLAN маркируются. Cisco указывает, что trunk-порт может принимать как tagged-, так и untagged-трафик, причём немаркированные кадры по умолчанию интерпретируются как принадлежащие native VLAN. По этой причине на обоих концах trunk-соединения native VLAN должна совпадать; её несоответствие рассматривается как типичная ошибка конфигурации, способная привести к неверной доставке трафика и к снижению безопасности.

Зачем нужен trunk

Если между двумя коммутаторами нужно передавать данные нескольких VLAN, нельзя для каждой VLAN тянуть отдельный кабель.
Вместо этого используется один trunk-канал.

Например:

- на первом коммутаторе есть VLAN 10 и VLAN 20;
- на втором тоже есть VLAN 10 и VLAN 20.

Чтобы трафик этих VLAN проходил между коммутаторами, порт между ними настраивается как trunk.

Access и Trunk: разница

Access-порт:

- принадлежит одной VLAN;
- обычно используется для подключения конечных устройств: ПК, принтеров и т.д.

Trunk-порт:

- передаёт трафик нескольких VLAN;
- обычно используется между коммутаторами или между коммутатором и маршрутизатором.

Router-on-a-Stick

Поскольку VLAN создаёт изоляцию на втором уровне, устройства из разных VLAN не могут обмениваться данными без маршрутизации. Один из классических способов организации межвлановой связи — схема, которую в учебной и эксплуатационной практике называют router-on-a-stick. Её сущность состоит в том, что между коммутатором и маршрутизатором используется один физический канал в режиме trunk, а маршрутизатор выполняет маршрутизацию между несколькими VLAN через набор подинтерфейсов, связанных с одним физическим интерфейсом. Cisco в официальной документации по inter-VLAN routing с внешним маршрутизатором и по routing over IEEE 802.1Q прямо описывает именно такую архитектуру: внешний маршрутизатор работает через 802.1Q trunk и использует subinterfaces для обслуживания различных VLAN.

На уровне конфигурационной модели каждый подинтерфейс получает собственный идентификатор VLAN через команду encapsulation dot1q vlan-id и собственный IP-адрес, который становится шлюзом по умолчанию для узлов данной VLAN. Тем самым один физический порт маршрутизатора логически превращается в несколько интерфейсов третьего уровня. Cisco указывает, что IP routing over IEEE 802.1Q расширяет возможности маршрутизации таким образом, чтобы маршрутизатор мог

обрабатывать кадры разных VLAN, представленных как отдельные subinterfaces на одном линке.

С функциональной точки зрения router-on-a-stick удобен в учебных стендах и в небольших сетях, поскольку позволяет реализовать межвлановую маршрутизацию без коммутатора третьего уровня. Однако эта схема имеет очевидное архитектурное ограничение: весь межвлановый обмен проходит через один физический канал и один маршрутизирующий интерфейс. Поэтому при росте интенсивности трафика такой подход становится менее эффективным по сравнению с использованием multilayer switch, где маршрутизация выполняется непосредственно внутри коммутирующей платформы. Сам принцип необходимости маршрутизации между VLAN и логического разделения трафика официально зафиксирован в документации Cisco по VLAN и inter-VLAN routing

Зачем нужен Router-on-a-Stick

Коммутатор второго уровня умеет передавать данные внутри одной VLAN, но не умеет маршрутизировать трафик между разными VLAN.
Поэтому, если нужно, чтобы:

- VLAN 10 общалась с VLAN 20,
- VLAN 20 общалась с VLAN 30,

нужен маршрутизатор или коммутатор 3 уровня.

Если используется обычный маршрутизатор с одним физическим интерфейсом, применяется схема **Router-on-a-Stick**.

Принцип работы

1. Порт коммутатора, ведущий к маршрутизатору, настраивается как **trunk**.
2. На маршрутизаторе один физический интерфейс делится на несколько **подинтерфейсов**.
3. Каждый подинтерфейс обслуживает свою VLAN.
4. На каждом подинтерфейсе задаётся IP-адрес, который становится шлюзом для соответствующей VLAN.

Пример:

- G0/0.10 → VLAN 10 → 192.168.10.1
- G0/0.20 → VLAN 20 → 192.168.20.1
- G0/0.30 → VLAN 30 → 192.168.30.1

Как это работает на практике

Если ПК из VLAN 10 хочет отправить пакет в VLAN 20:

- пакет идёт на шлюз VLAN 10;
- шлюзом является подинтерфейс маршрутизатора для VLAN 10;
- маршрутизатор принимает пакет, анализирует IP-адрес назначения;
- после этого пересылает его через подинтерфейс VLAN 20;
- коммутатор доставляет пакет в нужную VLAN 20.

То есть маршрутизатор выполняет межвлановую маршрутизацию через один физический линк.

В научно-техническом смысле VLAN следует рассматривать как механизм логической декомпозиции сети второго уровня на независимые широковещательные домены. Trunk является транспортной формой переноса нескольких VLAN через единое физическое соединение с использованием тэгирования по IEEE 802.1Q. Router-on-a-stick, в свою очередь, представляет собой частный способ реализации межвлановой маршрутизации, при котором один физический интерфейс маршрутизатора разделяется на подинтерфейсы, каждый из которых обслуживает отдельную VLAN. Вместе эти три понятия образуют последовательную архитектурную цепочку: сначала сеть сегментируется, затем сегменты переносятся между устройствами, после чего при необходимости между ними организуется маршрутизируемое взаимодействие.

Материал опирается на официальные документы Cisco и IEEE по VLAN, 802.1Q trunking и inter-VLAN routing

Задача лабораторной работы

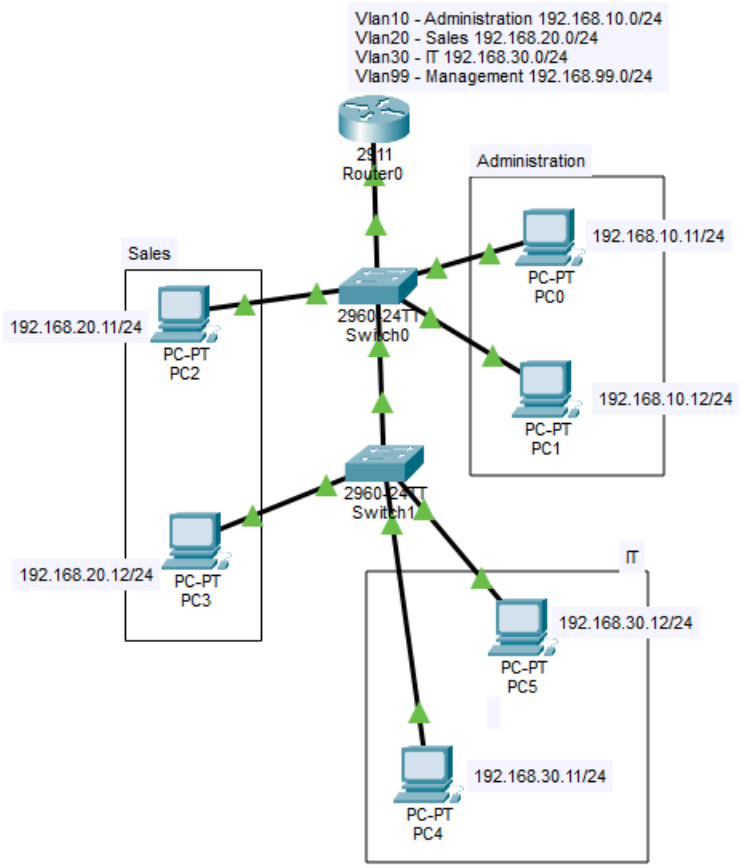
Нужно собрать сеть небольшой организации из трех отделов:

- **VLAN 10 — Administration**
- **VLAN 20 — Sales**
- **VLAN 30 — IT**
- **VLAN 99 — Management** (служебная VLAN)

Для реализации поставленной задачи необходимо использовать следующее оборудование в Packet Tracer

- 1 маршрутизатор Cisco 2911
- 2 коммутатора Cisco 2960
- 6 ПК

Топология



План адресации

Для выполнения своей работы каждый студент берет следующие данные для реализации данной работы X - его порядковый номер по списку группы

VLAN 10 — Administration

- Сеть: `192.168.X+5.0/24`

VLAN 20 — Sales

- Сеть: `192.168.X+15.0/24`

VLAN 30 — IT

- Сеть: `192.168.X+25.0/24`

VLAN 99 — Management

- Сеть: `192.168.X+50.0/24`

`Шлюз ставим как первый доступный IP сети`

IP - Адресса компьютеров

Название	IP	Defaut Gateway
PC1	192.168.X+5.X+4	
PC2	192.168.X+5.X+8	
PC3	192.168.X+15.X+4	
PC4	192.168.X+15.X+8	
PC5	192.168.X+25.X+2	
PC6	192.168.X+25.X+4	

Порты подключения

Device 1	port	Device 2	port
R1	G0/0	S1	F0/24
S1	F0/23	S2	F0/23
PC1	Ethernet	S1	F0/1
PC2	Ethernet	S1	F0/2

PC3	Ethernet	S1	F0/3
PC4	Ethernet	S2	F0/1
PC5	Ethernet	S2	F0/2
PC6	Ethernet	S2	F0/3

Задачи

Шаг 1

Соберите представленную топологию в соответсвии с таблицей портов подключения

Шаг 2

Создайте VLAN на обоих комутаторах в соответсвии с планном адресации

Шаг 3

Назначьте access порты и trunk на обоих маршрутизаторах

Шаг 4

Поднимите trunk до маршрутизатора и настройте машрутизатор по схеме Route-on-a-Stick

Шаг 5

Настройте IP адресса и Default GateWay на всех компьютерах в соответсвии с планом адресации

Шаг 6

Проверьте доступность сети командами ping. Просмотрите маршруты пакета при помощи команды tracert между устройствами с одного vlan и с разных vlan

Необходимые команды

команда	действие
show vlan brief	выводит краткую сводку по VLAN на коммутаторе: номера VLAN, имена, статус и назначенные access-порты
show interfaces trunk	показывает trunk-интерфейсы и их параметры, включая активные trunk-порты и сведения о передаваемых

	VLAN
show ip interface brief	выводит краткую таблицу интерфейсов с IP-адресами и их текущим состоянием
encapsulation dot1Q	включает 802.1Q-инкапсуляцию на подинтерфейсе и привязывает его к указанной VLAN для межвлановой маршрутизации
switchport mode trunk	переводит интерфейс в режим trunk, чтобы по одному физическому каналу передавался трафик нескольких VLAN
switchport trunk allowed	задаёт список VLAN, которым разрешено проходить через данный trunk-порт
switchport mode access	переводит интерфейс в постоянный режим access, то есть в режим нетранкового порта для одной VLAN
switchport access	назначает access-порт в конкретную VLAN
interface range	позволяет одновременно войти в режим настройки сразу нескольких интерфейсов и применить к ним одинаковую конфигурацию

Контрольные вопросы

1. Что такое VLAN и зачем она используется?
2. Чем access-порт отличается от trunk-порта?
3. Для чего нужен протокол 802.1Q?
4. Почему устройства из разных VLAN не обмениваются данными без маршрутизации?
5. Что такое Router-on-a-Stick?
6. Зачем нужна management VLAN?