2️⃣

LabWork2

Подчасть 1

Можно подключить с помощью более, чем одного канала (для резервирования).

Раз 6 станций: 2 пользовательских вилана, один административный, один нативный. Два последних можно совместить.

Если ни одна станция не подключена к нативному, это не значит, что он не нужен.

С одной стороны к одному крайнему коммутатору подключены два разных польз. вилана и админ.

С другой - тоже 2 польз. вилана (в один - две станции, в другой - одна).

Подчасть 2

Резервирование с помощью агрегации.

Подинтерфейсы можно создавать и на маршрутизаторах, и на коммутаторах третьего уровня. Если не использоваться маршрутизатор, это не значит, что не спросит про подинтерфейсы маршрутизатора.

Не просто незадействованные порты виланов отключить, но и коммутаторов.

vlan10 (students: ip-address) на рабочих материалах.

На защите три случайных вопроса.

Может определить дуплексность, принудительно задать скорость на защите..

Источники

https://linkas.ru/articles/vlan-v-cisco/

https://wiki.merionet.ru/articles/protocol-vtp

https://linkmeup.gitbook.io/sdsm/2.-switching/00-teoriya/06-vlan

https://www.computernetworkingnotes.com/ccna-study-guide/configure-vtp-server-and-client-in-switch.html

https://habr.com/ru/articles/143768/

Теория

Access port — порт доступа — к нему подключаются, как правило, конечные узлы. Трафик между этим портом и устройством нетегированный. За каждым access-портом закреплён определённый VLAN. Весь трафик, приходящий на этот порт от конечного устройства, получает метку этого влана, а исходящий уходит без метки.

Trunk port — у этого порта два основных применения — линия между двумя коммутаторами или от коммутатора к маршрутизатору. Внутри такой линии, называемой в народе, что логично, транком, передаётся трафик нескольких вланов. Разумеется, тут трафик уже идёт с тегами. За транковым портом закрепляется целый диапазон вланов.

Чтобы иметь возможность передачи трафика от нескольких VLAN посредством одного порта, его следует перевести в режим trunk.

Конкретные режимы интерфейса (режим умолчания отличаются для разных моделей):

- auto – это автоматический режим порта, из которого переход в режим trunk возможен только в том случае, если порт на другом конце связи будет в режиме desirable или on;
- desirable – это режим, из которого порт может перейти к режиму trunk; в этом состоянии он периодично посылает DTP-кадры к другому порту, запрашивая его перейти в режим trunk; этот режим будет установлен, если другой порт находится в одном из трех режимов: auto, desirable или on;
- trunk – в этом случае порт постоянно пребывает в состоянии trunk, даже если другой порт не может поддерживать такой же режим;

- nonegotiate – это режим, с которого порт готов выполнить переход к режиму trunk; он не выполняет передачу DTP-кадров к другому порту. Этот режим предусмотрен для исключения конфликтных ситуаций с другим оборудованием (не бренда Cisco). В этом случае коммутационное устройство на другом конце связи должно быть настроено в ручном режиме для использования режима trunk.

При создании VLAN’а (с ним работают только управляемые коммутаторы) хосты физической сети, объединенные общей функцией, выделяются в логическую виртуальную сеть, при этом их физическое местонахождение не имеет значения.

Для обмена информацией о виланах между коммутаторами используется VLAN Trunking Protocol, который позволяет централизованно управлять виланами: вилан, созданный на коммутаторе в режиме VTP-сервера, автоматически будет добавлен и на всех остальных коммутаторах, которые настроены в режиме VTP-клиента. Удаление вилана на VTP-сервере приведёт также к его автоматическому удалению на всех VTP-клиентах.

Концепция виланов 802.1q — стандарт, описывающий как именно кадр маркируется/тегируется.

VTP коммутатор имеет два режима работы:

- Server: можно создавать новые и вносить изменения в существующие VLAN’ы. Коммутатор будет обновлять свою базу VLAN’ов и сохранять информацию о настройках во Flash-памяти в файле vlan.dat. Генерирует и передает сообщения как от других коммутаторов, работающих в режиме сервера, так и от клиентов.
- Client: коммутатор в этом режиме будет передавать информацию о VLAN’ах, полученную от других коммутаторов и синхронизировать свою базу. Настройки нельзя будет поменять через командную строку такого устройства.
- Transparent: коммутатор будет передавать VTP-информацию другим участникам, не синхронизируя свою базу и не генерируя собственные обновления.

Статическая и динамическая агрегация — это методы объединения нескольких физических каналов в один логический интерфейс для увеличения пропускной способности и отказоустойчивости.

Признак сравнения	Статическая агрегация	Динамическая агрегация
Настройка параметров агрегации	Вручную	Автоматическая
Проверка и настройка агрегации на обеих сторонах	—	Протокол LACP
Проверка линков	—	Автоматическая
Простота	+	-
Гибкость	-	+

Выполнение работы

▼ L3-коммутатор vs доп. маршрутизатор:

К L3 подключено сразу несколько коммутаторов ⇒ трафик проходит через большее кол-во каналов ⇒ больше пропускная способность, меньше переходов.

Коммутатор с маршрутизатором столкнется с большим кол-вом транзитного трафика.

L3-коммутатор: нет лишних внешних связей, доп. функции.

Замена Root-коммутатора Switch3 на L3 (3560).

▼ VTP:

Меньше команд (только 3 на каждом), потом изменения нужно заносить лишь на сервер.

Если не настроить VTP, остальные коммутаторы не будут видеть созданные vlan’ы.

Root — server.

▼ Создание vlan’ов на VTP-сервере:

Обычно используются номера от 10 и выше для пользовательских VLAN: 10 — первый польз., 20 — второй польз.

Часто используют 99 или 100 для административных целей: 100 — админ.

По умолчанию VLAN 1 является нативным VLAN: 999 — нативный.

▼ Реализация концепции 802.1Q:

Перевод портов в режим trunk: тех, которые связывают коммутаторы.

На Root порты не дают установить режим trunk. Пришлось явно задать тип инкапсуляции в dot1q. На коммутатор 3650 не было бы такой проблемы, так как он поддерживает только один тип инкапсуляции.

Чтобы запретить передачу по транкам пакетов из неизвестных VLAN, нужно настроить транковый интерфейс таким образом, чтобы он принимал и передавал пакеты только из разрешенных VLAN. Это можно сделать с помощью команды `switchport trunk allowed vlan [номер VLAN]`.

Со стороны PC к крайнему коммутатору подключены два разных польз. вилана (PC1 — 10, PC2 — 20) и админ. (PC0).

Со стороны Laptops — тоже 2 польз. вилана (в один — две станции (Laptop0 и 1), в другой — одна (Laptop 2)).

Для задания нативного VLAN на транковом интерфейсе, используется команда `switchport trunk native vlan [номер VLAN]`.

▼ Агрегация каналов:

Root имеет три соседних коммутатор: Switch2, Switch7 и Switch6.

К каждому из них подключено не более двух других коммутаторов посредством одного физ. канала ⇒ более двух физических каналов не требуется.

Динамическая агрегация: отслеживание возникновения ошибок за счёт согласования настроек с противоположной стороной.

Номера групп на одном устройстве должны быть уникальными.

Настройки для Port Channel применяются для относящихся к ним интерфейсов.

Для интерфейсов Fast Ethernet, которые поддерживают максимальную скорость 100 Мбит/с, наиболее подходящая скорость — это 100 Мбит/с с полным дуплексом (full duplex).

▼ Работоспособность PVST+:

Чтобы проверить работоспособность PVST+, нужно отключить активное соединение в районе петли, после этого ранее выключенное

для исключения возможности появления петель соединение должно перейти в режим forwarding.

Например, на S4 int Fa0/3 отключить. Должен перейти в Forwarding ранее заблокированный Fa0/1.

▼ PortFast:

PortFast рекомендуется только на портах подключённых к конечному оборудованию. В случае использования PortFast на truck портах могут возникать петли.

%Warning (от CLI Cisco Packet Trcaer): portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.

Чтобы проверить PortFast, следует отключить и сразу включить один из портов, соединяющих коммутатор и станцию, порт сразу же должен перейти в состояние forwarding (загорится зелёным), что свидетельствует о пропуске состояний listening и learning.

▼ BPDU Guard:

Для проверки BPDU Guard необходимо к одному из настроенных для станций портов, предварительно отключив Port Security, если он настроен на этом порту, подключить коммутатор. После этого порт сразу же будет переведён в состояние error-disabled.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/4, putting 0/4 in err-disable state

▼ Маршрутизация:

ip routing на Root.

Создание и конфигурирование SVI (Switch Virtual Interface) на Root — ассоциированного с виланом виртуального сетевого интерфейса.

Подсети любые 4 из списка.

На остальных коммутаторах: виртуальный админ. интерфейс.

На станциях: IP из соответствующей подсети, шлюз по умолчанию на соответствующий виртуальный интерфейс (кроме админ.).

▼ Port Sequrity:

Присвоить разрешенный MAC-адрес: MAC-адрес порта станции PC0.

▼ SSH:

`enable password` — устанавливает вход в привилегированный режим.

`line vty 0 15` — переход в режим конфигурации линий (таким образом одинаковые параметры настраиваются и для 0 4, и для 5 15):

- `transport input ssh` — настройка разрешенного протокола подключения к линии;
- `login local` — аутентификация производится посредством локального пароля.

Для подключения к коммутатору по SSH:

- `ssh -l [имя пользователя] [IP-адрес]`
- `ssh <имя_пользователя>@<IP-адрес_целевого_коммутатора>`

Вопросы на защите

При IVR, как изолировать административный вилан?

Зачем на коммутаторе нужно назначать шлюз по умолчанию? Если коммутатор нужно администрировать из другой подсети.

Особенности вывода на экран команды show vlan (слайд 2.2.7.11 в доп.).

Какие порты коммутаторы назначены портами доступа?

Как продемонстрировать BPDU Guard?

Вопросы по использованию и по выводу команды show spanning-tree. Данный коммутатор является корневым мостом или нет? Не является, если прописаны Root ID и Bridge ID или если в таблице указан настоящий Root. Если this Bridge is Root, то является.

Что такое оранжевый цвет? Можно увидеть, если один вилан по умолчанию. Может не быть, если в разных виланах разные корневые мосты. Может зависеть от версии коммутатора и iOS.

Доказать, что используется именно PVST.

tracerout с Laptop0 до Laptop1 (между разными виланами).

tracerout с Laptop1 (v20) до PC1 (v10) / PC2.

Сколько должно быть хопов?

Зайти на конкретный коммутатор удаленно с целью администрирования (используя SSH или еще как).

Допустим, на коммутаторе нужно создать еще один вилан. Как это сделать?

ping с одного коммутатора на другой.

Как просмотреть, какие созданы виланы? Как определить, какие порты являются trunk в активном состоянии? Если их нет, значит, они trunk (но это не факт).

Продемонстрировать, как назначается коммутатор корневым мостом.

Как просмотреть состояние системы STP?

Как определить, какой коммутатор является корневым в таком-то вилане?

Допустим, в системе есть еще один вилан. Что нужно сделать, чтобы включить поддержку вилана (на маршрутизаторе)?

Как одной командой на коммутаторе административно выключить все незадействованные порты?

Как определить порт является trunk или access.

Допустим, между коммутаторами необходимо сделать режим, чтобы скорость канала была 100. Как доказать, что именно 100.

Продемонстрировать, что работает защита с помощью Port Security.