Лабораторная работа номер 7.

Настройка протокола Spanning-tree и маршрутизации OSPF на Linux.

Часть 1. Сборка схемы, базовая настройка.

В данной работе рассмотрены настройки таких технологий как STP, OSPF маршрутизация на Linux, трансфер маршрутов из протокола OSPF в RIP и обратно на граничном маршрутизаторе, а так же технология агрегации физических каналов EtherChannel.

Технология STP будет настраиваться на унифицированных роутерах-коммутаторах с платой коммутации L2 на 16 портов. Данные устройства имеют названия: US1-US3. Между каждым из данных устройств вы видите по 2 физических линка, это сделано специально, чтобы разобрать ситуацию с выбором роли портов при работе протокола STP. В лекции неоднократно говорилось о том, что технология STP работает для каждого из VLAN в отдельности, но в данной работе во избежание путаницы используется самый простой режим ручной настройки протокола STP, при наличие в сети только одного VLAN с номером 1.

Зона маршрутизации OSPF --- R0-R1-R2, зона маршрутизации RIP --- R2-R3.

Задание 1. Базовая настройка схемы.

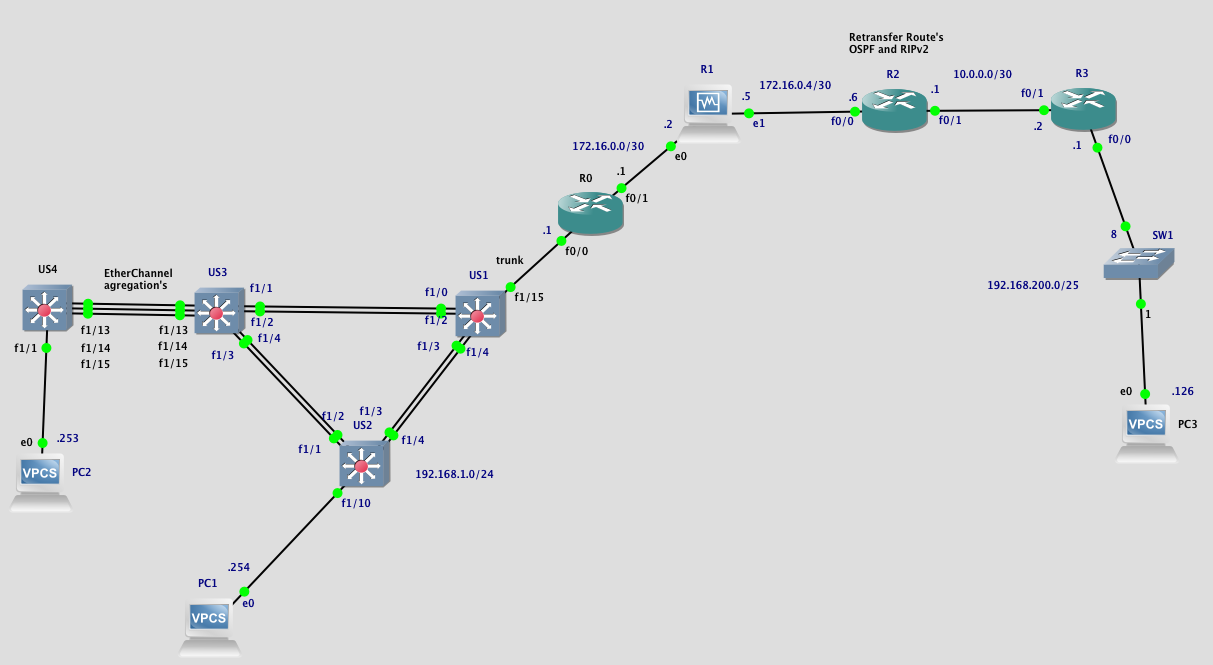


Рисунок 1.

1. Собрать схему согласно рисунку 1.
2. Настроить IP адреса на интерфейсах активного сетевого оборудования согласно схеме.
3. Не забыть настроить режим trunk для порта Fa1/15 на унифицированном коммутаторе US1.
4. Произвести базовые настройки активного сетевого оборудования:
5. Задайте имя хоста:

hostname имя\_устройства

1. Настройте приветственный баннер:

***banner motd ^Warning Router access only granted users^***

1. Защите паролем консольное подключение
2. Защитите паролем VTY сессии с 0 15
3. Включите сервис базового шифрования паролей:

**service password-encryption**

1. Задайте шифрованный пароль для активации enable режима
2. Установите синхронный вывод для консоли и VTY сессий 0 15.

Для чего использовать команду **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

1. Настройте таймаут telnet сессии 5 минут.

***exec-timeout 5 0***

1. Отключите автоматически поиск DNS серверов

no ip domain-lookup

Задание 2. Настройка агрегации каналов EtherChannel US4---US3.

Для увеличения не только надежности каналов связи, но и скорости трансфера в отсутствии высокоскоростных портов используют технологию EtherChannel. Между US4 и US3 объединим три линка Fa1/13-15.

1. Зайти на US4 в режим настройки портов Fa1/13-15:

**interface range fastEthernet 1/13 – 15**

1. Настроить для них агрегированный канал с номером 1:

**channel-group 1 mode on**

1. Зайти на US3 в режим настройки портов Fa1/13-15:

**interface range fastEthernet 1/13 – 15**

1. Настроить для них агрегированный канал с номером 1:

**channel-group 1 mode on**

1. Проверить результат на обоих унифицированных коммутаторах командой:

**show interfaces port-channel 1**

Скорость агрегированного канала должна получится 300 Mbit/s.

Задание 3. Настройка и изучение работы протокола STP.

1. На унифицированных роутерах-коммутаторах US1-US3 выполнить команды **sh spanning-tree brief** (на обычных коммутаторах команда проще show spanning-tree) и выяснить какой из них является корневым мостом, сохранить скриншоты. Коммутатор в роли корневого моста будет иметь идентификатор моста BridgeID равный указанному на нем RootID, а так же пометку о том, что This router is Bridge.

Пример показан на рисунке 2:

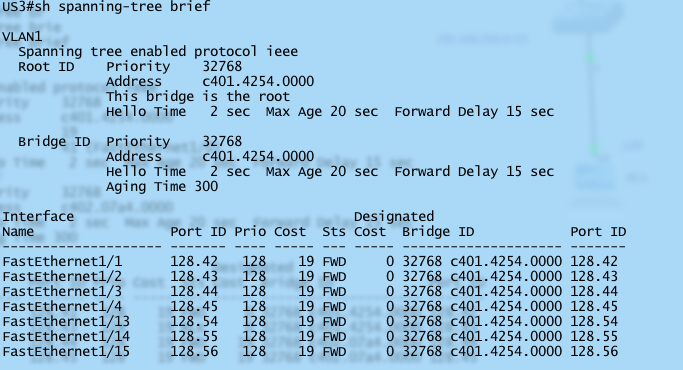


Рисунок 2.

Обратите внимание, что команда show spanning-tree brief показывает вывод настроек STP только для VLAN 1, если бы у нас были настроены еще VLAN, вывод был бы и для них. Так же стоит помнить, что в реальных сетях, где на коммутаторах настроено множество VLAN один и тот же физический коммутатор может быть для одного VLAN в роли Root Bridge, а для другого обычным мостом. Bridge Priority является суммой из двух чисел, первое из которых, значение дефолтового приоритета в 32768, второе, номер VLAN в нашем случае это 32768+1. Но на унифицированных устройствах это не отображается! Из рисунка видно, что на роль корневого моста STP выбрал роутер US3, так как он обладает самым минимальным значением MAC адреса управляющего интерфейса.

Особенностью работы унифицированных роутеров с протоколом STP является экзотическая система нумерации коммутационных портов в протоколе STP. Номера портов протокол spanning-tree использует для выбора порта на роль Root port так как приоритет выбора на данную роль по умолчанию у всех одинаков и равен 128. Чем ниже номер порта тем более приоритетен он на роль Root port. Но если на обычных коммутаторах приоритезация порта для скажем Fa0/1 будет выглядеть как 128.1, в случае унифицированных устройств порт Fa1/0 будет иметь номер 41! То есть приоритезация будет выглядеть так - 128.41. Это так же видно на рисунке 2.

1. Назначьте US1 принудительно корневым мостом, а US3 резервным корневым мостом с помощью команд:

Root Bridge: **spanning-tree vlan** *vlan-id* **root primary**

Secondary Root Bridge: **spanning-tree vlan** *vlan-id* **root secondary**

1. С помощью команды spanning-tree brief проверить результат и сохранить скриншоты. Обратите внимание на значение Bridge ID на них.
2. Назначьте US1 принудительно корневым мостом, а US3 резервным корневым мостом с помощью команд:

**spanning-tree vlan** *vlan-id* **priority** *value*

Примечание!!! На самом деле значение Bridge Priority у нас идет с шагом 4096, и обычно его начинают считать от числа по умолчанию 32768 в большую или меньшую сторону. Чтобы обеспечить 100% выбор коммутатора на роль Root Bridge, а так же резервного Root Bridge стоит задать им значения приоритета выбора 4096 и 8192 соответственно.

1. Проверьте, применились ли значения приоритета выбора коммутатора на роль Root Bridge на US1 и Reserved Root Bridge US3. Пример приведен на рисунках 3 и 4:

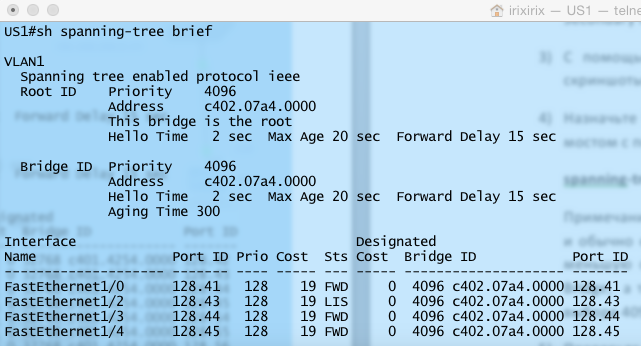


Рисунок 3.

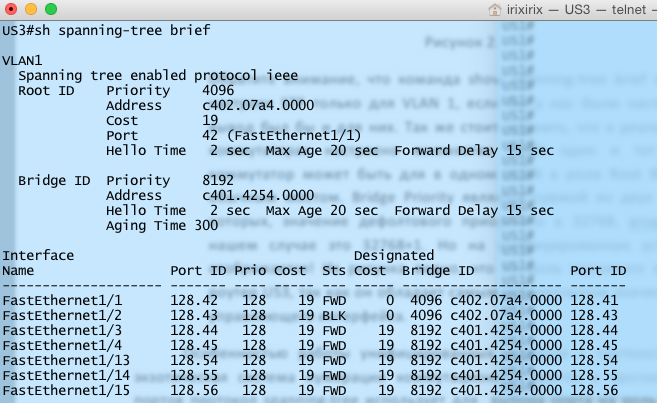


Рисунок 4.

1. В лекции описывалось 4 состояния в которых прибывает порт при работающем протоколе spanning-tree, если на нем не настроен режим работы PortFast. Это:

- Blocking

- Listen

- Learning

-Forward

Находясь в первые 3-х состояниях порт не может передавать никакой трафик кроме BPDU служебных пакетов. В последнем же разрешена передача обычного трафика. Время пребывания в режиме Listen и Learning зависит от настройки сетевого диаметра для протокола STP.

Проверить прохождение портом данных состояний. Для чего на коммутаторе US3 в привилегированном режиме выполнить команду **debug spanning-tree events**, которая активирует вывод подробной информации о работе протокола STP.

Состояние портов при полной сетевой конвергенции STP, рисунок 5.

После чего следует выключить оба порта Fa1/1 и Fa1/2, командой **interface range fastethernet** 1/1 – 2. Далее смотреть за выводом консоли, пример на рисунке 6. У вас должен получится аналогичный вывод. Fa1/2 перейти в состояние Blocking и иметь обозначение Alt (Alternate), а порт Fa1/1 определенное время будет находится в состоянии Listen и Learning и только затем перейдет в режим разрешения передачи пользовательского трафика – Forward.

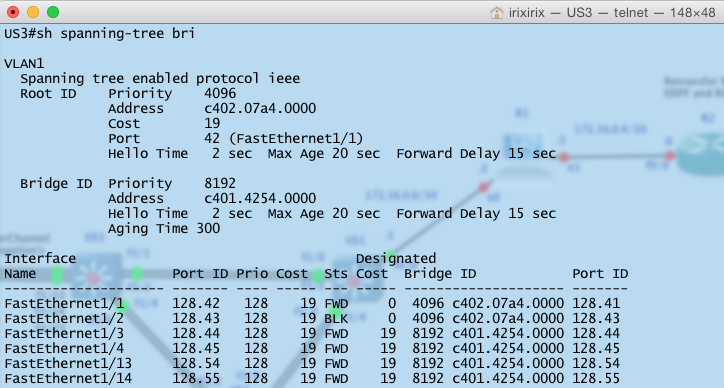


Рисунок 5.

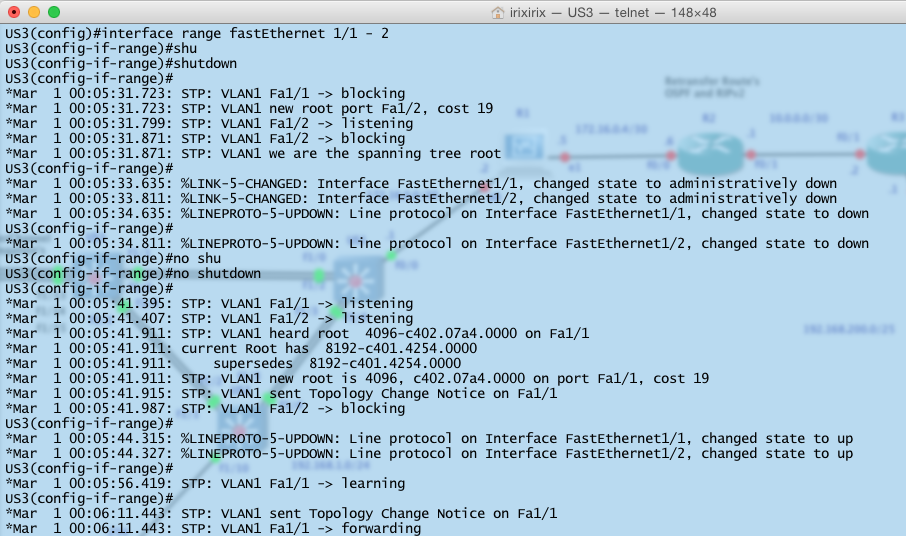


Рисунок 6.

7) Конфигурируйте на коммутаторе US2 для порта Fa1/10 и коммутаторе US4 для порта Fa1/1 режим работы portfast, то есть режим при котором порт тут же переходит в рабочие состояние. Так как на него планируется подключать только пользовательские устройства. Для чего используйте команду:

**spanning-tree portfast**

1. Включить debug режим для spanning-tree на унифицированном коммутаторе US2. Запустите ping c ПК PC1 до шлюза (Fa0/0 R0), с опцией –t.
2. Выключите и включите порт Fa 1/10 на US2 и проверьте вывод debug режима STP, пример, рисунок 7:



Рисунок 7.

Из него видно, что порт Fa 1/10 форсировано перешел из режима blocking в режим передачи пользовательского трафика forward.

Часть 4. Настройка OSPF на R0.

1. На унифицированном устройстве US1 активируйте маршрутизацию OSPF с номером процесса 2.
2. Добавьте в процесс маршрутизации интерфейс Fa0/0 и Fa0/1.
3. Сделать интерфейс Fa0/0 пассивным для процесса маршрутизации OSPF, так как за ним сеть из унифицированных устройств выполняющих только коммутацию трафика и данные OSPF туда отсылать не имеет смысла.

Часть 5. Настройка OSPF на Linux.

В Linux поддержка динамической маршрутизации реализована посредством программного обеспечения quagga, разработчики данного программного продукта стремятся максимально унифицировать процесс настройки протоколов OSPF, RIP, BGP для IPv4 и IPv6 c Cisco IOS. Данный пакет доступен в репазитории дистрибутива. Для реализации маршрутизации на Linux в лабораторной работе используется Linux OpenSuSE 13.2 i586, но настройки любого из динамических протоколов с помощью сервиса маршрутизации quagga одинаково для всех дистрибутивов Linux.

1. Развернуть ВМ R1. Запустить ее и установить ПО quagga:

**zipper install quagga**

1. Выключить ВМ и перевести сетевой интерфейс в тип подключения “Не подключено”. Активировать второй сетевой интерфейс и выставить ему тот же тип.
2. Разрешить использование данной ВМ в GNS, выставив в ее настройках использование двух сетевых интерфейсов.
3. Включить ВМ R1 и настроить IP адреса на интерфейсах enp0s3 (интерфейс e0 в схеме GNS) и интерфейсе enp0s8 (e1 в схеме GNS) согласно схеме. IP адреса настроить на постоянной основе, то есть или через текстовые файлы конфигурации сервиса network в /etc/sysconfig/network, для каждого из интерфейсов или с помощью YAST.

*Примечание: обратите внимание, что для правильной работы графической панели управления YAST количество RAM в ВМ должно быть не менее 1024 Мб.*

1. Все настройки маршрутизации хранятся в каталоге /etc/quagga. Для работы процесса маршрутизации OSPF нам надо создать и сконфигурировать два файла /etc/zebra.conf и /etc/ospfd.conf. Если шаблонного файла не существует, его можно создать командой touch. В файле zebra.conf находятся настройки интерфейсов. В файлике ospfd.conf настройка процесса маршрутизации.

Ниже приведены примеры файлов конфигурации роутера R1:

**ospfd.conf**

! -\*- ospf -\*-

!

! OSPFd sample configuration file

!

!

hostname R1

password password-1

enable password password-1

!

interface enp0s3

ip ospf cost 1

!ip ospf hello-interval 1

interface enp0s8

ip ospf cost 1

!ip ospf hello-interval 1

router ospf

router-id 10.0.0.1

network 192.168.10.0/24 area 0

network 10.0.0.0/30 area 0

neighbor 10.0.0.2

log stdout

log file /var/log/quagga/ospfd.log

**zebra.conf**

hostname quagga

password quagga

enable password quagga

!interfaces!

interface lo

description loopback

ip address 127.0.0.1/8

ip forwarding

interface enp0s3

description LAN1

ip address 192.168.10.1/24

ip forwarding

interface enp0s8

description link R1---R2

ip address 10.0.0.1/30

ip forwarding

log file /var/log/quagga/quagga.log

*Примечание – в примере приведены настройки IP адресов и маршрутизируемых сетей отличных от тех что используются в схеме. Но вам надо лишь сделать по аналогии. Quagga не поддерживает автономные номера систем для OSPF, тем не менее принимает все маршруты OSPF c любым номером процесса.*

Как вы видите настройки очень похожи на таковые в Cisco IOS, к чему и стремились разработчики программного пакета для маршрутизации Quagga. Восклицательным знаком помечаются комментарии, но тут есть одно отличие от Cisco IOS. В Cisco IOS после той или иной настройки, в той же строке можно было поставить “!” и сделать комментарий, тут так нельзя, это вызовет ошибку при перезапуске службы.

Quagga поддерживает настройку маршрутизации и через командную строку похожую на Cisco IOS, для подключения к которой используется telnet с подключением к localhost.

Чтобы появилась такая возможность, надо открыть файл /etc/services, где расписано какие службы на каких TCP/UDP портах работают и внести следующие изменения:

**zebra 2601/tcp # zebra vty**

**ospfd 2604/tcp # ospf vty**

После чего можно подключаться к Cisco Like командной строке, для настройки интерфейсов - **telnet localhost zebra**, для настройки процесса маршрутизации OSPF - **telnet localhost ospfd**.

Создайте файлы zebra.conf и ospfd.conf и внесите в них настройки по образцу приведенных выше примеров в соответствие с схемой.

1. Проверьте в каком режиме запуска настроены сервисы ospfd и zebra, командой:

**chkconfig –list**.

1. Настройте автозапуск сервисов ospfd и zebra на уровнях инициализации системы 2,3 и 5, для чего воспользоваться командой:

**chkconfig --level 235 название\_службы on**

1. Запустить службы zebra и ospfd:

**service zebra start**

**service ospfd start**

1. Проверьте, смогли ли служба ospfd активировать маршрутизацию на Linux, для чего использовать команду: **cat /proc/sys/net/ipv4/ip\_forward**. Если результат “1”, значит маршрутизация активирована.

*Примечание. При этом файл /etc/sysctl.conf не содержит строчки net.ipv4.ip\_forward = 0. Значит, процесс маршрутизации активируется непосредственно сервисом ospfd.*

1. Проверьте таблицу маршрутизации, командой **netstat -rn**. Если маршрутизация OSPF на унифицированном роутере R0 настроена правильно, вы увидите маршруты, для сети 192.168.1.0/24.

Часть 6. Настройка RIPv2 на роутере R3.

1. Настройте на маршрутизаторе R3 протокол маршрутизации RIPv2, отключить автосуммаризацию маршрутов.
2. Добавить в процесс маршрутизации все активные интерфейсы.
3. Сделать пассивным для RIPv2 интерфейс Fa 0/0, так как за ним расположен коммутатор и ПК.

Часть 7. Настройка ретрансфера маршрутов из OSPF зоны маршрутизации в RIPv2 и обратно.

1. На маршрутизаторе R2 активировать два протокола маршрутизации OSPF с номером процесса 2 и RIPv2. Для RIPv2 не забыть отключить автосуммаризацию.
2. Настроить ретрансфер маршрутов из RIPv2 области в OSPF. Для чего на роутере R2 зайти в настройки процесса маршрутизации OSPF 2 и разрешить принятие маршрутов из RIP области:

**redistribute rip subnets**

1. На роутерах R0 и R1 проверить появление соответствующих маршрутов из RIP области.
2. Настроить ретрансфер маршрутов из OSPF 2 области в RIP. Для чего на роутере R2 зайти в настройки процесса маршрутизации RIP и разрешить принятие маршрутов из OSPF 2 области:

**redistribute ospf 2 metric 3**

Где параметр metric 3 это метрика которая будет ставится всем маршрутам в RIP *области прибывшим из OSPF 2 области.*

*Примечание – под словом область подразумевается домен процессов маршрутизации OSPF 2 (R0---R1—R2) и RIP (R2---R3), а не области распределения LSP пакетов протокола OSPF.*

1. Проверить таблицы маршрутизации на роутерах R0-R1-R2-R3 и сохраните скриншоты.
2. Проверить доступность по протоколу ICMP ПК PC1---PC3 и PC2---PC3, связь должна быть успешной.

!

router ospf 2

log-adjacency-changes

redistribute rip subnets

network 172.16.0.4 0.0.0.3 area 0

!

router rip

version 2

redistribute ospf 2 metric 3 match internal

network 10.0.0.0

no auto-summary

!

router ospf 2

log-adjacency-changes

redistribute rip subnets

network 172.16.0.4 0.0.0.3 area 0

!

router rip

version 2

redistribute ospf 2 metric 3

network 10.0.0.0

no auto-summary