Лабораторная работа 5.

VLAN, VTP, Inter-VLAN маршрутизация

Задание 1.

Подключение в GNS роутеров серии 3745 с поддержкой функционала L2 и L3 коммутаторов.

Нужно открыть добавление образов IOS и добавить образ роутера 3745 который мы уже использовали для включения в GNS роутеров серии 3745. Но на этапе задания имени и пароля обязательно выбрать пункт This is EtherSwitch router, рисунок 1:

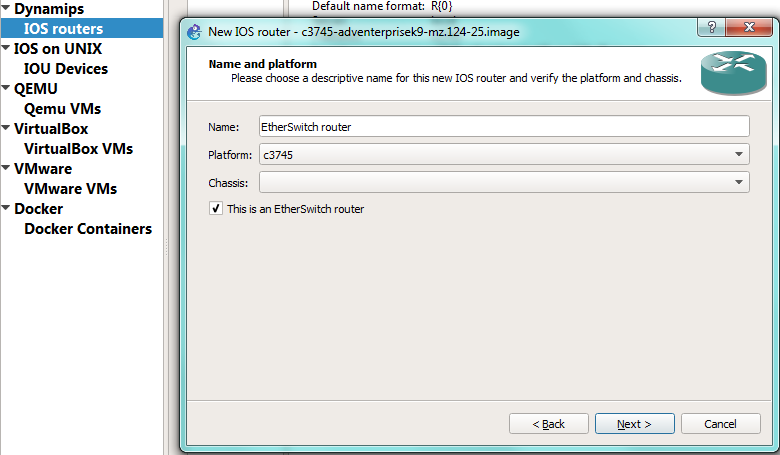


Рисунок 1.

Все остальные параметры оставляем без изменений, так же стоит обратить внимание, что 16-ти портовый FastEthernet модуль уже подключен, рисунок 2:

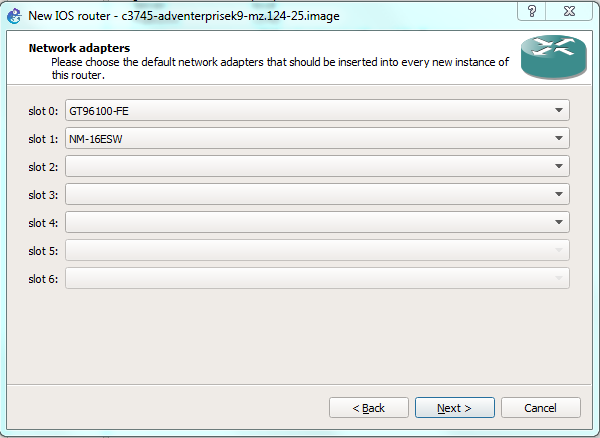


Рисунок 2.

На конечном этапе, разумеется, не стоит забывать высчитать или вставить используемый на роутерах 3745 IDLE-PC.

После чего во вкладке Коммутаторы, появится EtherSwitch роутер.

Это универсальное устройство – унифицированный роутер, то есть мощный полнофункциональный роутер со всеми возможностями на маршрутизируемых портах, а так же благодаря коммутационному модулю 16-ти портовый L2/L3 коммутатор. Это означает, что на нем можно настраивать технологии VLAN/VTP/STP/SVI/PortSecurity.

Но есть некоторые особенности использования L2/L3 функционала, а именно:

1. Настройка VLAN (создание, удаление, именование), настройка VTP осуществляется через режим командной строки (vlan)#, попасть в который можно не из глобального режима конфигурации как мы привыкли, а из root (enable) режима командной строки.

Настройка vlan с именем представляет вид:

**Switch(vlan)#vlan 10 name students**

Настройка VTP параметров осуществляется в этом же режиме, но синтаксис такой же, как на обычном коммутаторе Cisco.

После проделанных изменений нужно сохранить настройки в данном режиме командой apply, либо просто выйдя из него, командой exit.

В редких случаев при первоначальной работе с L2/L3 может возникнуть ошибка при попытке сохранить конфигурацию при выходе из режима настройки VLAN. А именно:

**% not enough space on ﬂash to store vlan database. trying squeeze...First create squeeze log by erasing the entire device**

В данном случае нужно использовать команду **erase flash:**. По какой то причине flash память, в которой в данном роутере будет храниться файл vlan.dat не инициализирована, то есть не отформатирована.

Примечание: возможно при подключение устройства в GNS по каким-то причинам не включился PCMCI образ, на котором собственно и эмулируется flash память. По умолчанию если все подключение прошло без ошибок его размер равен 1 Mb, что собственно не мешает вам его увеличить до желаемых размеров. Ну а если его нет, то нужно создать размером от 1 Mb и только потом производить **erase flash:**.

1. Еще важная особенность это активация портов для работы. В конфигурации running-config не указанно, что они выключены, то есть по логике вещей они находятся в состоянии ВКЛЮЧЕНО. Но после настройки порта он не заработает, если не выключить и заново включить порт.
2. Просматривать список настроенных vlan нужно не командой show vlan, а **show vlan-switch**.
3. Порты Fa0/0 –Fa0/1 эти порты работают ТОЛЬКО в режиме роутера. Кстати пустые слоты позволяют добавить в роутер еще портов работающих только в режиме маршрутизации.
4. При настройке VTP на таких устройствах VTP апдейты приходят на постоянной основе только на коммутаторы, работающие в режиме Server, если перевести один из коммутаторов в режим клиента, то апдейт придет только при изменении VLAN конфигурации на одном из серверов. То есть если в имеющуюся структуру сети вставить подобное устройство с пустым именем VTP домена в режиме Client, автоматом имя домена VTP с VTP сервера и актуальную конфигурацию оно не получит до момента изменения VLAN конфигурации на одном из серверов.
5. Для настройки портов модуля группой используется команда range, но нумерация портов через пробел (это специфичный синтаксис для некоторых версий IOS):

**s1(config)#interface range fastethernet 1/0 - 4**

1. VLAN интерфейсы перейдут по line-protocol в состояние UP, только если на устройстве активен в состоянии line-protocol хотя бы один TRUNK порт.

Задание 2.

Соберите топологию, указанную на рисунке 3:

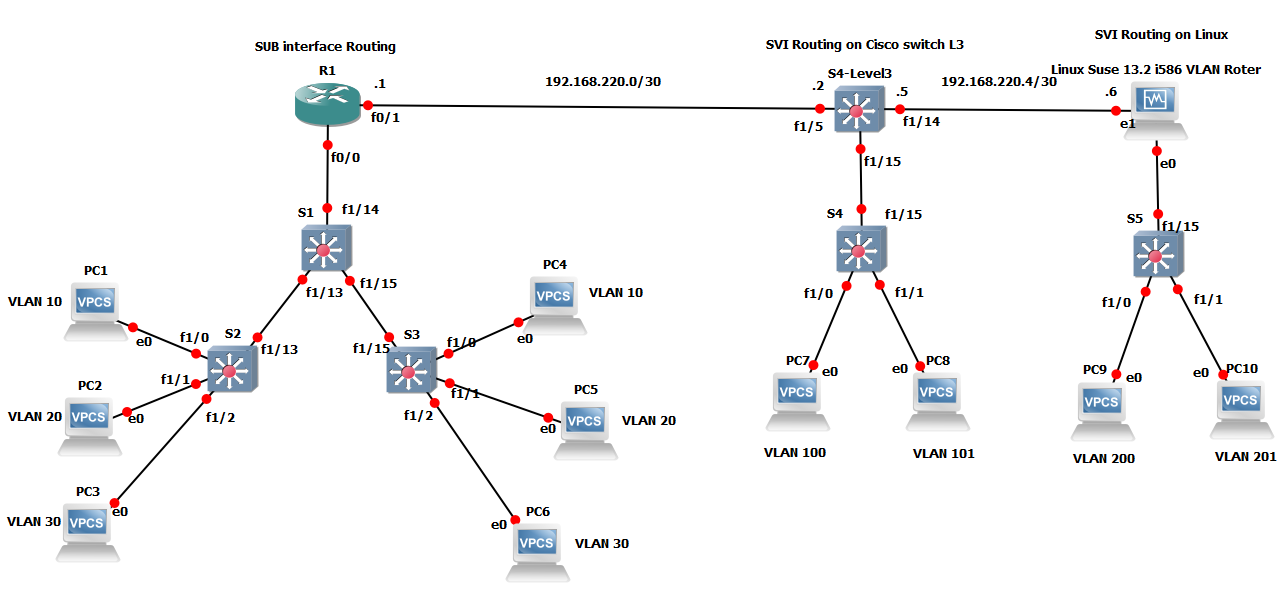


Рисунок 3

Обратите внимание, что в GNS используются не стандартные коммутаторы серий 2960, а L3 коммутаторы, функциональность которых получаем на основе роутера 3745, подключив в него 16-ти портовый модуль с FastEthernet интерфейсами. Подключение которых в GNS, описано в задание 1.

Задание 3.

Проведите базовую настройку роутеров:

1. Задайте имя хоста

hostname S1

1. Настройте приветственный баннер

***banner motd ^Warning Switch 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-enqription

1. Задайте шифрованный пароль для активации enable режима
2. Установите синхронный вывод для консоли и VTY сессий 0 15.
3. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
4. Настройте таймаут telnet сессии 5 минут.

***exec-timeout 5 0***

1. Отключите автоматически поиск DNS серверов

no ip domain-lookup

Задание 3.

1. Настройте все сетевые интерфейсы, согласно адресному плану (табл. 1)
2. Для всех интерфейсов сделайте подписи (комментарии) куда уходит линк из этого ин­терфейса. Для этого используется команды description, в режиме конфигурации интерфейса.

Таблица 1. Адресный план.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| **S1** | **VLAN 99** | 172.17.99.11 | 255.255.255.0 | 172.17.99.1 |
| **S2** | **VLAN 99** | 172.17.99.12 | 255.255.255.0 | 172.17.99.1 |
| **S3** | **VLAN 99** | 172.17.99.13 | 255.255.255.0 | 172.17.99.1 |
| **S4** | **VLAN 99** | 172.17.99.14 | 255.255.255.0 | 172.17.99.14 |
| **S4-Level3** | **VLAN 99** | 172.17.99.254 | 255.255.255.0 | N/A |
| **S4-Level3** | **VLAN 100** | 192.168.100.1 | 255.255.255.0 | N/A |
| **S4-Level3** | **VLAN 101** | 192.168.101.1 | 255.255.255.0 | N/A |
| **S4-Level3** | **Fa1/5** | 192.168.220.2 | 255.255.255.252 | N/A |
| **S4-Level3** | **Fa1/14** | 192.168.220.5 | 255.255.255.252 | N/A |
| **S5** | **VLAN 99** | 172.17.99.15 | 255.255.255.0 | N/A |
| **PC1** | **NIC** | 172.17.10.21 | 255.255.255.0 | 172.17.10.1 |
| **PC2** | **NIC** | 172.17.20.22 | 255.255.255.0 | 172.17.20.1 |
| **PC3** | **NIC** | 172.17.30.23 | 255.255.255.0 | 172.17.30.1 |
| **PC4** | **NIC** | 172.17.10.24 | 255.255.255.0 | 172.17.10.1 |
| **PC5** | **NIC** | 172.17.20.25 | 255.255.255.0 | 172.17.20.1 |
| **PC6** | **NIC** | 172.17.30.26 | 255.255.255.0 | 172.17.30.1 |
| **PC7** | **NIC** | 192.168.100.2 | 255.255.255.0 | 192.168.100.1 |
| **PC8** | **NIC** | 192.168.101.2 | 255.255.255.0 | 192.168.101.1 |
| **PC9** | **NIC** | 192.168.200.2 | 255.255.255.0 | 192.168.200.1 |
| **PC10** | **NIC** | 192.168.201.2 | 255.255.255.0 | 192.168.201.1 |
| **R1** | **Fa0/1** | 192.168.220.1 | 255.255.255.252 | N/A |
| **R1** | **Fa0/0.10** | 172.17.10.1 | 255.255.255.0 | N/A |
| **R1** | **Fa0/0.20** | 172.17.20.1 | 255.255.255.0 | N/A |
| **R1** | **Fa0/0.30** | 172.17.30.1 | 255.255.255.0 | N/A |
| **R1** | **Fa0/0.99** | 172.17.99.1 | 255.255.255.0 | N/A |
| **Linux SuSE 13.2 i586 VLAN Router** | **enp0s8** | 192.168.220.6 | 255.255.255.252 | N/A |

**ВАЖНО:**

На каждом из коммутаторов S1, S2, S3, S4 надо в режиме глобальной конфигурации настроить шлюз по умолчанию, для коммутаторов это делается командой:

**ip default-gateway 172.17.99.1**, где адрес 172.17.99.1 – IP адрес на sub интерфейсе Fa 0/0.99 маршрутизатора R1, который будет настроен в задании 5.

Для коммутатора S4 это будет IP адрес интерфейса VLAN 99 на маршрутизаторе S4-Level3, то есть 172.17.99.14.

Задание 4.

Настройка VLAN на коммутаторах и автоматизация их распространения при помощи VTP.

Таблица 2. План VLAN’s.

|  |  |
| --- | --- |
| **VLANs** | **Диапазоны сети** |
| VLAN 99 – Management&Native | 172.17.99.0/24 |
| VLAN 30 – Guest | 172.17.30.0/24 |
| VLAN 10 – Faculty/Staff | 172.17.10.0/24 |
| VLAN 20 – Students | 172.17.20.0/24 |

1. На коммутаторе S1 настройте VLAN 99, который будет использоваться в качестве Native VLAN для нашей сети:

S1(vlan)#**vlan 99 name Management&Native**

S1(vlan)#**apply**

S1(vlan)#**exit**

1. Для того, чтобы VLAN распространялись по VTP домену нужно настроить магистральные порты между коммутаторами.

***Пример:***

S1(config)#**interface fa1/13**

S1(config-if)#**switchport mode trunk**

S1(config-if)#**switchport trunk native vlan 99**

S1(config-if)#**interface fa1/14**

S1(config-if)#**switchport mode trunk**

S1(config-if)#**switchport trunk native vlan 99**

S1(config-if)#**interface fa1/15**

S1(config-if)#**switchport mode trunk**

S1(config-if)#**switchport trunk native vlan 99**

S1(config-if)#**end**

Обратите внимание, что на коммутаторе S1 порт FastEthernet 1/14 так же надо настроить как транковый с trunk native vlan 99, так как этот линк уходит к роутеру R1, который будет обеспечивать связь между VLAN.

По аналогии нужно будет настроить trunk режим с native vlan 99 для магистралей между S2-S1 и S3-S1.

1. На коммутаторе S1 выполнить команду *show interface trunk* и проверить наличие правильно сконфигурированных транков. Этой же командой проверьте настройки магистралей в режиме trunk на коммутаторах S2 и S3.
2. Настройте коммутатор S1 как VTP сервер:

S1(vlan)#**vtp mode server**

1. Настройте на S1 VTP имя домена **CCNA,** в котором будут распространяться с него информация о VLAN:

S1(vlan)#**vtp domain CCNA**

1. Настройте пароль для VTP домена **cisco**:

S1(vlan)#**vtp password cisco**

1. Проверьте правильность настройки коммутатора S1 в роли VTP сервера, командой

**S1#show vtp status**

1. Проверить настроенный пароль можно командой **show vtp password**
2. Проверьте состояние VTP настроек на коммутаторах S2 и S3, командой **show vtp status**, они должны находиться в режиме работы VTP server и иметь пустое имя домена.
3. Настроить коммутаторы S2 и S3 для работы в VTP домене CCNA как клиентов VTP.

*Пример:*

S2(vlan)#**vtp mode client**

S2(vlan)#**vtp domain CCNA**

S2(vlan)#**vtp password cisco**

1. Проверьте состояние VTP настроек на коммутаторах S2 и S3, командой **show vtp status**, они должны находиться в режиме работы VTP client и иметь имя домена CCNA. В принципе как уже писалось выше, может быть такая ситуация, что вы увидите так же пустое имя домена, это вызвано тем, что иногда VTP клиенты принимают апдейты VTP с сервера, только когда происходит изменение VLAN базы данных на одном из коммутаторов выполняющих роль VTP server. Поэтому создадим VLAN’s на S1.
2. Настройте VLAN на коммутаторе S1

S1(vlan)#**vlan 10 name Faculty/Staff**

S1(vlan)#**vlan 20 name Students**

S1(vlan)#**vlan 30 name Guest(Default)**

S1(vlan)#**apply**

S1(vlan)#**exit**

1. Проверьте создание VLAN на коммутаторе S1 командой **show vlan-switch brief** .
2. Проверьте распространение VLAN с VTP сервера, коим является коммутатор S1 на коммутаторы S2 и S3, командой **show vlan-switch**.
3. Распределите VLAN на порты коммутатора S2 и S3 согласно схеме сети, пример для коммутатора S2:

S2(config)#**interface fastEthernet 1/0**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan 10**

S2(config-if)#**interface range fastEthernet 1/1**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan 20**

S2(config-if)#**interface range fastEthernet 1/2**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan 30**

S2(config-if)#**end**

1. По аналогии распределите VLAN на коммутаторе S3.
2. Проверьте распределение VLAN на портах коммутатора **show vlan-switch**
3. Задайте IP адреса на управляющем VLAN на коммутаторе S1, S2, S3.

***Пример:***

S1(config)#**interface vlan 99**

S1(config-if)#**ip address 172.17.99.11 255.255.255.0**

S1(config-if)#**no shutdown**

1. Проверьте связь между управляющими интерфейсами в VLAN 99 настроенными на коммутаторах. Связь с коммутатора S1 до S2 и S3 должна быть успешной.

Задание 5.

Настройка маршрутизации между VLAN (Inter-VLAN типа Router-in-a-stick) для коммутаторов S1, S2 и S3.

1. Настроить на маршрутизаторе R1 сабинтерфейсы для маршрутизации между VLAN в нашем VTP домене.

R1(config-if)#**interface fastethernet 0/0**

R1(config-if)#**no** **ip address**

R1(config-if)#**no shutdown**

R1(config-if)#**interface fastethernet 0/0.1**

R1(config-subif)#**encapsulation dot1q 1**

R1(config-subif)#**ip address 172.17.1.1 255.255.255.0**

R1(config-subif)#**interface fastethernet 0/0.10**

R1(config-subif)#**encapsulation dot1q 10**

R1(config-subif)#**ip address 172.17.10.1 255.255.255.0**

R1(config-subif)#**interface fastethernet 0/0.20**

R1(config-subif)#**encapsulation dot1q 20**

R1(config-subif)#**ip address 172.17.20.1 255.255.255.0**

R1(config-subif)#**interface fastethernet 0/0.30**

R1(config-subif)#**encapsulation dot1q 30**

R1(config-subif)#**ip address 172.17.30.1 255.255.255.0**

R1(config-subif)#**interface fastethernet 0/0.99**

R1(config-subif)#**encapsulation dot1q 99 native**

R1(config-subif)#**ip address 172.17.99.1 255.255.255.0**

Обратите внимание на то, что виртуальные sub интерфейсы не надо включать командой no shutdown, они включаются автоматически при включении физического интерфейса к которому они привязаны. Так же стоит помнить, что перед настройкой sub интерфейсов, надо убедиться, что на данном физическом интерфейсе не настроен IP адрес. Если настроен его надо удалить командой **no ip address**.

Для каждого sub интерфейса обязательна команда **encapsulation dot1q 30**, с помощью которой фреймы, идущие через него будут маркироваться тэгами dot1q, то есть номером VLAN, указанным в ней, в данном случае - 30.

1. Проверить связь между компьютером PC1 и PC2, PC3, PC4, PC5, PC6. Связь должна быть успешна, так как мы настроили Inter-VLAN маршрутизацию через роутер R1.
2. Связь с PC1 до S1, S2 и S3 должна быть успешной.

Задание 6.

Настройка маршрутизации между VLAN (Inter-VLAN типа SVI) посредством коммутатора L3 уровня для VLAN 100 и 101 настроенных на коммутаторе S5.

1. На коммутаторе S4-Level3 создать VLAN 100 с именем Reklama и VLAN 101 с именем IKSP.
2. На нем же создать VLAN 99 c именем Management&Native и задать ему IP адрес согласно адресному плану.
3. На интерфейсе коммутатора S4 настроить порт Fa1/15 как транковый с native VLAN 99

S4(config-if)# **switchport trunk native vlan 99**

S4(config-if)# **switchport mode trunk**

1. На коммутаторе S4-Level3 создать VLAN 99, 100, 101 и настроить на них IP адреса согласно адресному плану.
2. На интерфейсе Fa1/15 коммутатора S4-Level3 разрешить тегирование трафика командой **switchport trunk encapsulation dot1q**, после чего появиться возможность перевести порт в транковый режим работы, командой **switchport mode trunk**.

Так же надо разрешить прохождение через него трафика для VLAN 100 и VLAN 101 с помощью команды **switchport trunk allowed vlan 100-101**.

Настроить на нем VLAN 99 как нативный **switchport trunk native vlan 99**.

**Примечание: на cамом деле можно не указывать конкретно VLAN 100 и 101, тогда будут разрешены все.**

1. Несмотря на то что у нас унифицированный роутер 3745 с функцией коммутацией L2/L3 и на нем имеются порты, работающие исключительно в режиме роутинга, но для теста используем порты с 16-ти портового модуля L2/L3, которые так же можно перевести в режим роутинга. На порту Fa 1/5 настроить IP адрес согласно адресному плану. Чтобы удалось это сделать, перед заданием IP адреса надо данный порт переключить в режим порта маршрутизатора (по умолчанию-то он работает как порт коммутатора и на нем IP адрес настраивать нельзя), командой **no switchport**.
2. Аналогично настроить согласно адресному плану порт Fa 1/14. Для обеспечении связи с сегментом сети, где в качестве маршрутизатора выступает ВМ Linux VLAN Router.
3. На коммутаторе S4-Level3, чтобы работала Inter-VLAN маршрутизация на основе SVI интерфейсов надо выполнить команду **ip routing**, которая включит на коммутаторе L3 режим работы маршрутизации.
4. Проверить таблицу маршрутизации на S4-Level3, она должна содержать Directly-Connected маршруты до сетей VLAN 99, VLAN 100-101.
5. Проверить связь между компьютерами PC7 и PC8. Связь должна быть успешной.
6. Проверить связь компьютера PC7 с коммутатором S4 по протоколу ICMP. Связь должна быть успешной.

Задание 7.

Настройка связи между роутерами и сегментами сетей с помощью протокола RIPv2 между роутером R1 и унифицированным роутером S4-Level3.

1. На роутере R1 активизировать процесс маршрутизации RIPv2, отключить автосуммаризацию маршрутов в пределах классовых границ и включить в процесс маршрутизации все Directly-Connected интерфейсы, в том числе SUB интерфейсы.
2. На унифицированном маршрутизаторе S4-Level3 активизировать процесс маршрутизации RIPv2, отключить автосуммаризацию маршрутов в пределах классовых границ и включить в процесс маршрутизации все Directly-Connected интерфейсы, в том числе VLAN интерфейсы.
3. Проверить таблицы маршрутизации на R1 и S4-Level3, они должны содержать маршруты ко всем физическим и виртуальным сетям этих роутеров.
4. Проверить связь между компьютерами PC1<--->PC7, PC2<--->PC7, PC3<--->PC8, хождение ICMP трафика должно быть успешно.

Задание 8.

Настройка сегмента сети, в котором роль маршрутизатора выполняет Linux сервер.

На Linux возможна настройка как Sub интерфейсов, так и VLAN-SVI интерфейсов, правда если внимательно рассмотреть конфигурационные файлы не совсем понятно, чем они отличаются в Linux.

На данной ВМ используется Linux OpenSuSE 13.2 i586, преимущество OpenSuSE в настройке маршрутизации и виртуальных интерфейсов имеет как очевидные преимущества, так и минусы.

Плюсы:

1) Возможность настройки виртуальных VLAN интерфейсов и статических постоянных маршрутов из графической или псевдографической централизованной панели управления YAST.

Минусы:

2) Как ни странно сам YAST. Несмотря на то, что OpenSuSE это RedHat совместимая ОС, многие настройки, описанные в интернете для ОС Red Hat Linux/CentOS/Fedora ставшие по сути каноническими, имеют немного другой вид в OpenSuSE. Хотя и очень близкий.

Пример отличий:

Файл настройки виртуального sub интерфейса enp0s3.20 имеющий вид:

VLAN=yes

DEVICE=enp0s3.20

BOOTPROTO=static

ONBOOT=yes

TYPE=Ethernet

IPADDR=192.168.20.1

NETMASK=255.255.255.0

После перезапуска службы network активирует виртуальный интерфейс enp0s3.20 в Linux CentOS, однако данные настройки не могут активизировать этот же интерфейс в openSuSE.

Тем не менее, в SuSE есть замечательная графическая панель управления YAST, в которой можно создать виртуальный интерфейс типа VLAN и прикрепить его к нужной физической сетевой карте. Причем стоит обратить внимание, что в конфигурационном файле все параметры указаны в расхождении с канонами RedHat - в одинарных кавычках:

**VLAN='yes'**

**DEVICE='enp0s3.20'**

**BOOTPROTO='static'**

**ONBOOT='yes'**

**TYPE='Ethernet'**

**IPADDR='192.168.20.1'**

**NETMASK='255.255.255.0'**

В интернете мало хороших инструкций по настройке сетевых интерфейсов и маршрутизации на OpenSuSE в режиме командной строки, все мануалы описывают настройку с помощью YAST. Поэтому чтобы узнать как должен выглядеть тот или иной конфигурационный файл, нужно прежде настроить данную функционал через YAST.

1. На унифицированном роутере S5 создать VLAN 200 и VLAN 201.
2. Назначить на интерфейс Fa1/0 VLAN 200, на интерфейс Fa1/1 VLAN 201.
3. Интерфейс Fa1/15 перевести в режим работы Trunk.
4. Настроить IP адреса на компьютерах PC9 и PC10 согласно адресному плану.
5. Добавить в схему ВМ Linux SuSE 13.2 i586 VLAN Router. Затем зайти в его свойства, открыть вкладку Network и включить использование 2-ух сетевых интерфейсов. Один из них будет использоваться в качестве TRUNK магистрали до унифицированного роутера S5 (линк e0), а второй (линк e1) будет использоваться как магистраль для осуществления маршрутизации с унифицированным роутером S4-Level3.
6. Перед включением ВМ активировать второй сетевой интерфейс и выставить ему тип “Не подключен”.
7. Включить ВМ на которой проверить работоспособность сетевых интерфейсов командой ifconfig, они должны обозначаться именами enp0s3 и enp0S8.
8. Открыть конфигуратор YAST-Network и настроить виртуальные интерфейсы VLAN200 и VLAN201 с адресами согласно адресному плану, рисунок 4:

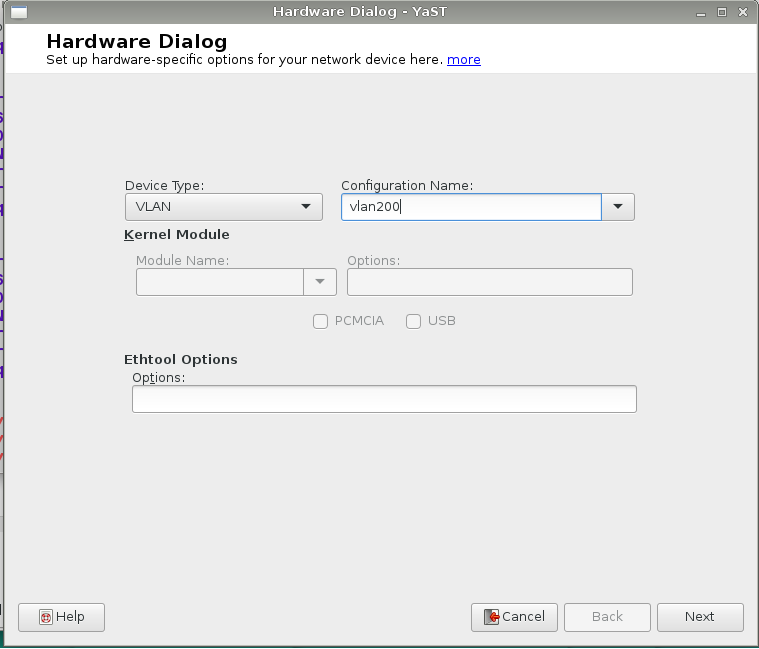


Рисунок 4.

1. Проверить настройки IP адресов на интерфейсах командой ifconfig.
2. Проверить настройки интерфейсов в файлах конфигурации в директории /etc/sysconfig/network, они будут иметь названия ifcfg-vlan200 и ifcfg-vlan201, привести скриншоты настроек.
3. Отключить интерфейс vlan200 командой ifdown vlan200. Проверить командой ifconfig, что он исчез из активных интерфейсов.
4. Запустить интерфейс перезапустив службу сети:

**service network restart**

1. ВКЛЮЧИТЬ маршрутизацию пакетов между физическими и виртуальными интерфейсами в Linux для протокола ipv4, для чего открыть файл /etc/sysctl.conf и в строке net.ipv4.ip\_forward = **0** изменить параметр 0 на 1. Если данной строчки нет, то добавить **net.ipv4.ip\_forward = 1**

После чего необходимо перезагрузить ВМ и проверить работоспособность маршрутизации между интерфейсами командой **cat /proc/sys/net/ipv4/ip\_forward**.

1. Проверить хождение ICMP трафика между компьютерами PC9 и PC10. Оно должно быть успешным.
2. Посредством YAST настроить статический IP адрес согласно адресному плану на сетевой карте enp0s8 (линк к S4-Level3). Проверить настройки командой ifconfig, а так же в файле настроек интерфейса ifcfg-enp0s8. Привести в отчете скриншоты настроек.
3. Проверить связь между ВМ и унифицированным маршрутизатором S4-Level3. Она должна быть успешной.
4. Открыть YAST-Network, вкладку Routing и настроить статические маршруты до всех сетей, которые маршрутизируются унифицированным маршрутизатором S4-Level3 и роутером R1, пример рисунок 5 и 6:

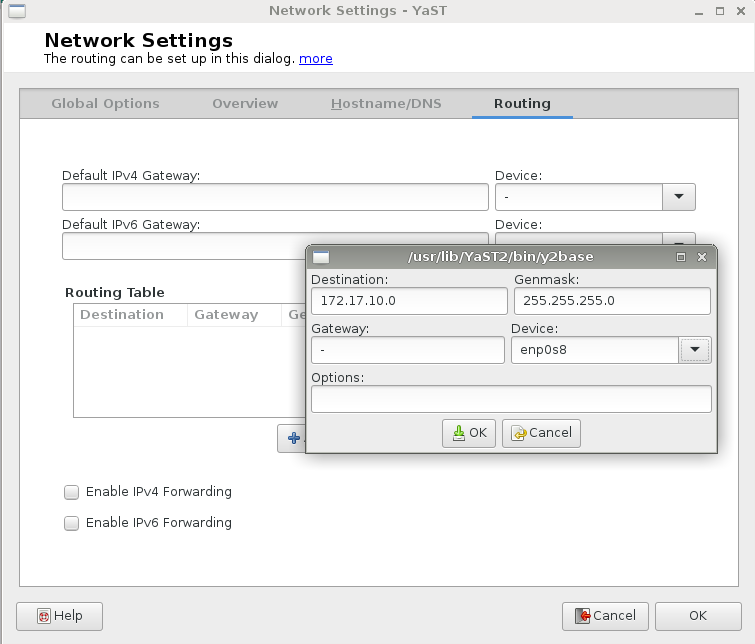


Рисунок 5.

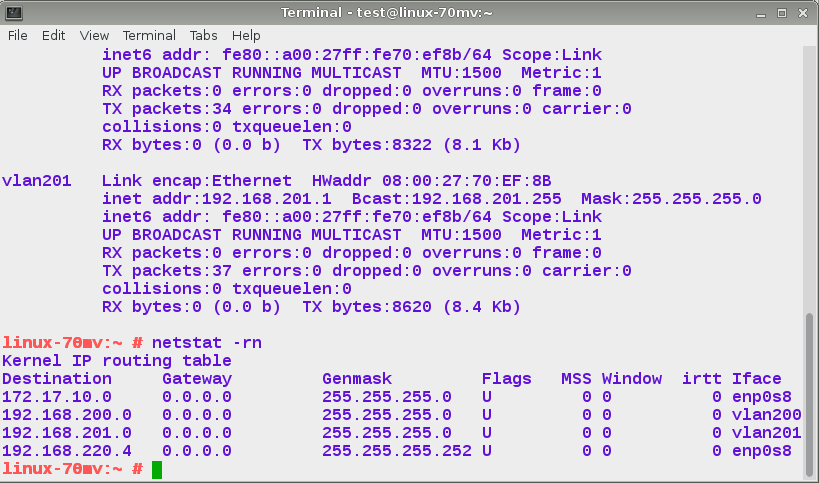


Рисунок 6.

На данных примерах настроен маршрут до сети 172.17.10.0/24 (VLAN10). Привести в отчете скриншоты списка маршрутов из командной строки для всех сетей маршрутизируемых R1 и S4-Level3.

1. На унифицированном маршрутизаторе S4-Level3 настроить маршрут по умолчанию с интерфейсом выхода Fa 1/14. Распространить его с помощью процесса маршрутизации RIP, командой default-information originate. Проверить его наличие на R1.
2. Проверить командой ping связь между компьютерами PC1<--->PC9, PC2<--->PC9, PC3<--->PC10, PC7<--->PC9, PC8<--->PC10. Связь по протоколу icmp должна быть успешной.

Задание 9.

Оптимизация процесса маршрутизации RIPv2.

1. Включить захват трафика для его анализа с помощью ПО Wireshark на линке между S4-Level3 и ВМ Linux.
2. Убедится, что на данном линке с интерфейса Fa1/14 унифицированного роутера S4-Level3 каждые 30 секунд отсылаются периодические модификации протокола RIPv2 в виде multicast трафика.
3. Так как ВМ Linux не участвует в процессе RIP и на ней настроена статическая маршрутизация отключить рассылку модификаций маршрутизации RIPv2 c интерфейса Fa1/14.
4. С помощью Wireshark убедится, что модификации перестали отсылаться.
5. Применить данную настройку на интерфейсах унифицированного роутера S4-Level3 там, где это еще необходимо.