МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«15» 09 2020 г.

ПУСКОНАЛАДКА ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

Методические указания по выполнению курсового проекта
для студентов по направлению подготовки
11.03.02 «Инфокоммуникационные технологии и системы связи»

Курск 2020

УДК 004.71

Составитель: И.Г. Бабанин

Рецензент

Кандидат технических наук, доцент кафедры *Е.О. Брежнева*

Пусконаладка телекоммуникационной системы: методические указания по выполнению курсового проекта / Юго-Зап. гос. ун-т; сост.: И.Г. Бабанин.– Курск, 2020.– 12 с.

Содержат сведения по проведению пусконаладочных работ телекоммуникационного оборудования.

Методическое указание соответствуют требованиям ФГОС ВО 3++ по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, а также рабочей программе дисциплины.

Предназначены для студентов по направлению подготовки 11.03.02.

Текст печатается в авторской редакции

Подписано в печать 15.09.2020 . Формат 60×84 1/16.
Усл.печ.л. 0,64. Уч.-изд.л. 0,58. Тираж 100 экз. Заказ 286. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КУРСОВОГО ПРОЕКТА

Данный курсовой проект разработан с учетом различных сетевых технологий. Задание разбито на следующие блоки:

- Базовая настройка системы
- Организация виртуальных сетей
- Агрегирование и резервирование каналов
- Настройка динамической маршрутизации и трансляции сетевых адресов
- Туннелирование сетевых адресов

Все блоки являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и Multilink и т.д. Очень важно понимать, что если вам не удается решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы туннеля, построенного по протоколу 6to4, вы можете

использовать статическую маршрутизацию и продолжать работу над настройкой туннеля и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

БЛОК 1. БАЗОВАЯ НАСТРОЙКА СИСТЕМЫ

1.1 Краткая теоретическая справка

Сетевые устройства, как правило, настраиваются в командной строке ОС Cisco IOS. Подсоединение к ним осуществляется по протоколу Telnet на IP-адрес любого из его сетевых интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом устройства.

Подключение через консольный порт предпочтительнее, потому что в процессе настройки оборудования могут измениться параметры физического порта или административного IP-интерфейса, что приведет к потере соединения, установленного по протоколу Telnet.

Следует иметь в виду, что аварийное отключение консоли не регистрируется оборудованием, и сеанс остается в том состоянии, в котором находился на момент отключения. При повторном подключении пользователь окажется в том же контексте (если только не сработал автоматический выход в контекст пользователя по таймеру неактивности). Напротив, при разрыве Telnet- соединения коммутатор закрывает сеанс работы.

Для конфигурирования сетевых устройств в консольном режиме может использоваться программа HyperTerminal, входящая в состав стандартных программ ОС Windows XP, или сторонние программы, например, Putty, если используется ОС Windows более поздних версий или другая операционная система.

Синтаксис команд, вводимых для конфигурирования, несколько различается у различных производителей, однако общий смысл их остается неизменным.

1.2 Задание блока 1

1) Задайте имя всех устройств в соответствии с топологией.

2) Создайте на всех устройствах пользователей tkkafuser с паролем network

a) Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.

b) Пользователь должен обладать максимальным уровнем привилегий.

3) На всех устройствах установите пароль r2d2 на вход в привилегированный режим.

a) Пароль должен храниться в конфигурации в виде результата хэш-функции.

4) Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.

5) На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.

9) Все устройства должны быть доступны для управления по протоколу SSH версии 2.

БЛОК 2. ОРГАНИЗАЦИЯ ВИРТУАЛЬНЫХ СЕТЕЙ

2.1 Краткая теоретическая справка

Виртуальной локальной сетью (VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. Таким образом, становится невозможной передача кадров на основании адреса канального уровня между разными виртуальными сетями.

Основным назначением технологии VLAN является облегчение процесса создания изолированных сетей, впоследствии связываемых между собой с помощью маршрутизаторов (рисунок 2.1). Подобное построение сети позволяет избавиться от распространения нежелательного трафика в различных её

сегментах. Так, например, технология виртуальных сетей позволяет избежать периодического затопления всей сети широковещательными штормами.

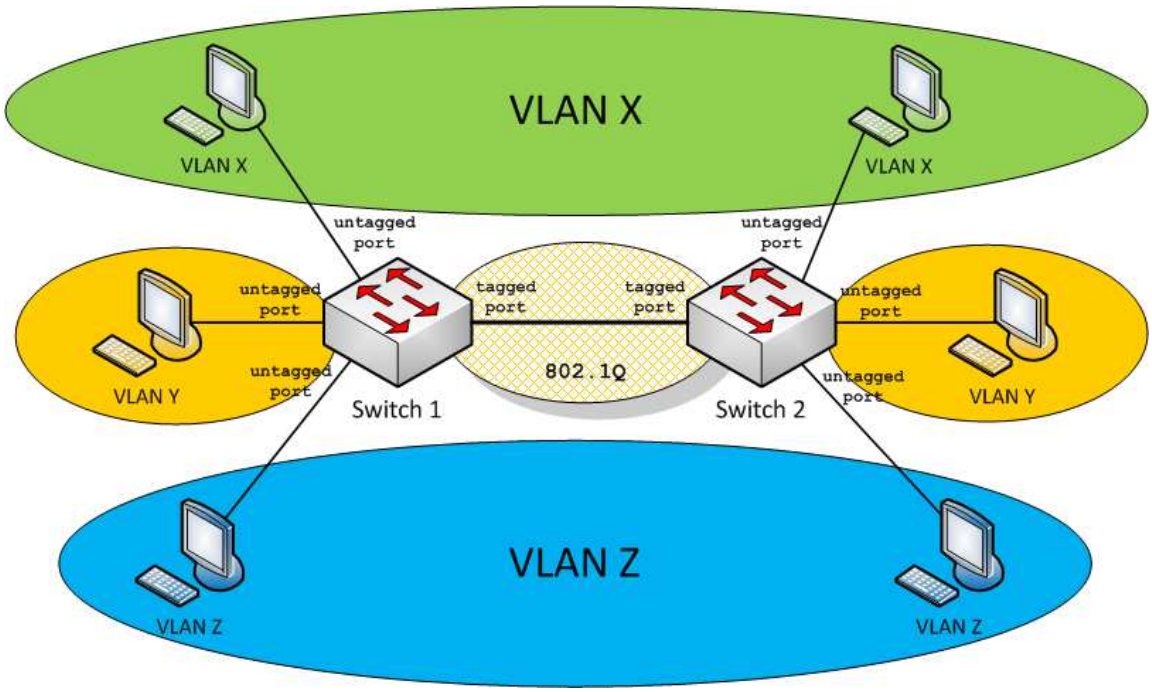


Рисунок 2.1 – Виртуальные локальные сети

Для передачи информации о принадлежности кадра к той или иной VLAN согласно стандарту IEEE 802.1Q в заголовок канального уровня добавляется дополнительный четырехбайтовый подзаголовок – тег. Кадр с инкапсулированным тегом принято называть тегированным. Пример тегированного кадра Ethernet приведен на рисунке 2.2.

6	6	4	2	42 - 1496	4
Destination address	Source address	Тег 802.1Q	Длина/ Тип	Данные	Контр. сумма

2	3 бита	1 бит	12 бит
TPID (0x8100)	PCP	CFI	VLAN ID

Рисунок 2.2 – Структура тегированного кадра Ethernet

Подзаголовок 802.1Q содержит, помимо идентификатора протокола VLAN – TPID (0x8100), индикатора канонического формата CFI и трех бит приоритета кадра (к VLAN не относящихся), также 12 бит номера виртуальной сети, к которой принадлежит кадр. Соответственно, всего возможно создать до 4096 общих виртуальных сетей.

Коммутатор, поддерживающий работу с VLAN, оперирует таблицами коммутации, содержащими поле VLAN ID. Такой коммутатор, принимая кадр с заголовком 802.1Q, будет осуществлять в таблице поиск лишь среди тех портов, которые отмечены как участники указанного в теге VLAN.

Подробное описание технологии VLAN приводится в рекомендации IEEE 802.1Q, определяющем базовые правила построения виртуальных локальных сетей.

2.2 Задание блока 2.

1) В подсети 1 необходимо реализовать VLAN100, VLAN200, VLAN300. Компьютеры PC1, PC4, PC6 должны находиться в VLAN200 (IPv6: fc00:1::/64), а компьютеры PC2, PC3, PC5 в VLAN100 (IPv6: fc00:2::/64).

2) Native VLAN переназначить на VLAN300 (IPv6: fc00:3::/64).

3) Между компьютерами PC5 и PC6 организовать взаимодействие по технологии Router-on-a-Stick на базе маршрутизатора Router1.

4) Выполнить проверку правильности функционирования всех узлов**.**

БЛОК 3. АГРЕГИРОВАНИЕ И РЕЗЕРВИРОВАНИЕ КАНАЛОВ

3.1 Краткая теоретическая справка

EtherChannel – технология агрегации каналов, разработанная компанией Cisco Systems. Технология позволяет объединять

несколько физических каналов Ethernet в один логический для увеличения пропускной способности и повышения надёжности соединения.

EtherChannel даёт возможность объединять от двух до восьми 100 Мбит/с, 1 Гбит/с или 10 Гбит/с портов Ethernet (все порты в канале должны иметь одинаковую скорость), работающего по витой паре или по оптоволокну, что позволяет достичь результирующей скорости до 80 Гбит/с. Дополнительно, от одного до семи портов могут быть неактивны и включаться в работу при обрыве соединения по одному из активных портов. При отсутствии резервных портов, трафик автоматически распределяется по всем активным соединениям.

Spanning Tree Protocol (STP, протокол покрывающего дерева) – канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

3.2 Задание блока 3.

1) Между коммутаторами SW-1 и SW-2 необходимо реализовать агрегирование каналов Ether Channel с использованием протокола LACP.
2) Предотвращение появления петель в кольцевой топологии выполнить с использованием сетевого протокола Rapid Per-VLAN STP.
3) Корневым коммутатором назначить SW-2.

БЛОК 4. НАСТРОЙКА ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ И ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ

4.1 Краткая теоретическая справка

OSPF (англ. Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии

отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2740 (декабрь 1999 год). Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol – IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF имеет следующие преимущества:

- высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- поддержка сетевых масок переменной длины (VLSM);
- оптимальное использование пропускной способности с построением дерева кратчайших путей.

Трансляция сетевых адресов является универсальным способом расширения адресного пространства. Появление системы трансляции сетевых адресов, или NAT (Network Address Translation) обусловлено бурным ростом небольших сетей, в то время относящихся к классу С, и, как следствие, сокращение IP-адресов данного класса. Тогда одним из способов расширения адресного пространства наравне с введением бесклассовой адресации стало использование неуникальных IP-адресов, иногда называемых маскарадными. Традиционно это адреса вида 192.168.0.0 и 10.0.0.0, но в последнее время могут использоваться некоторые другие. Такие адреса уникальны только в пределах закрытой сети (например, корпоративной или сети провайдера). Для выхода в общедоступную сеть необходим уникальный адрес, который присвоен шлюзу. Система NAT позволяет осуществлять подмену адресов на шлюзе.

В курсовом проекте рассмотрена работа с такими видами трансляции сетевых адресов, как Source NAT (SNAT) и Destination NAT (DNAT). Как следует из названий, данные виды NAT подменяют адреса отправителя и получателя пакета соответственно. Маскарадингом (Masquerade) называется разновидность SNAT, в которой подменяемый адрес отправителя

может изменяться динамически в соответствии с текущим адресом шлюзового интерфейса.

В операционной системе Linux за трансляцию сетевых адресов отвечает утилита *iptables* (или *ip6tables* для IPv6). Вообще, *iptables* является одним из командных интерфейсов межсетевого экрана Netfilter и используется для настройки разнообразных правил фильтрации сетевого трафика. Однако, в рамках курсового проета, рассмотрена только одна из его возможностей – NAT.

4.2 Задание блока 4.

1) Выполнить между Router1, Router2, Router3, Router4 маршрутизацию с использованием протокола OSPF версии 2 или 3.
2) На Router 3 необходимо настроить SNAT/маскарадинг.
3) На маршрутизаторе Router4 необходимо настроить DNAT с портом назначения 34001.

БЛОК 5. ТУННЕЛИРОВАНИЕ СЕТЕВЫХ АДРЕСОВ

5.1 Краткая теоретическая справка

С появлением сетей IPv6 возникла необходимость совместной работы сегментов сетей с разной адресацией. Скорее всего, еще довольно долгое время доминирующим протоколом останется IPv4. В таких условиях особую актуальность приобретают методы конвергенции и взаимодействия сетей различных типов. На данный момент разработано множество решений этой проблемы, из наиболее распространенных можно назвать 6to4, 6rd, Teredo, NAT64 и др. В этой части курсового проета рассмотрим универсальный способ передачи трафика IPv6 через сети IPv4, основанный на использовании протокола 6to4 (рисунок 5.1).

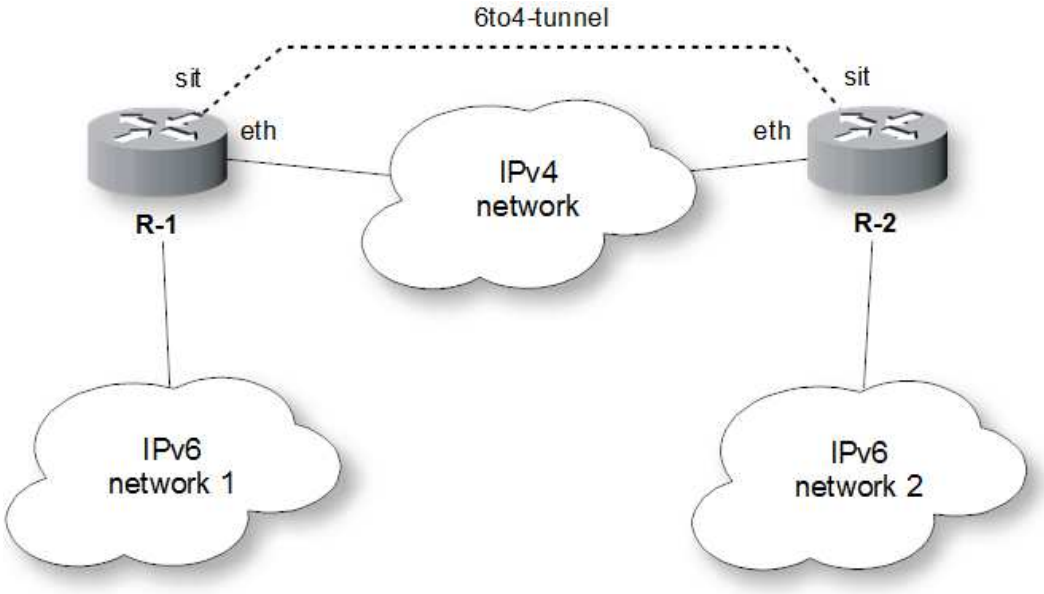


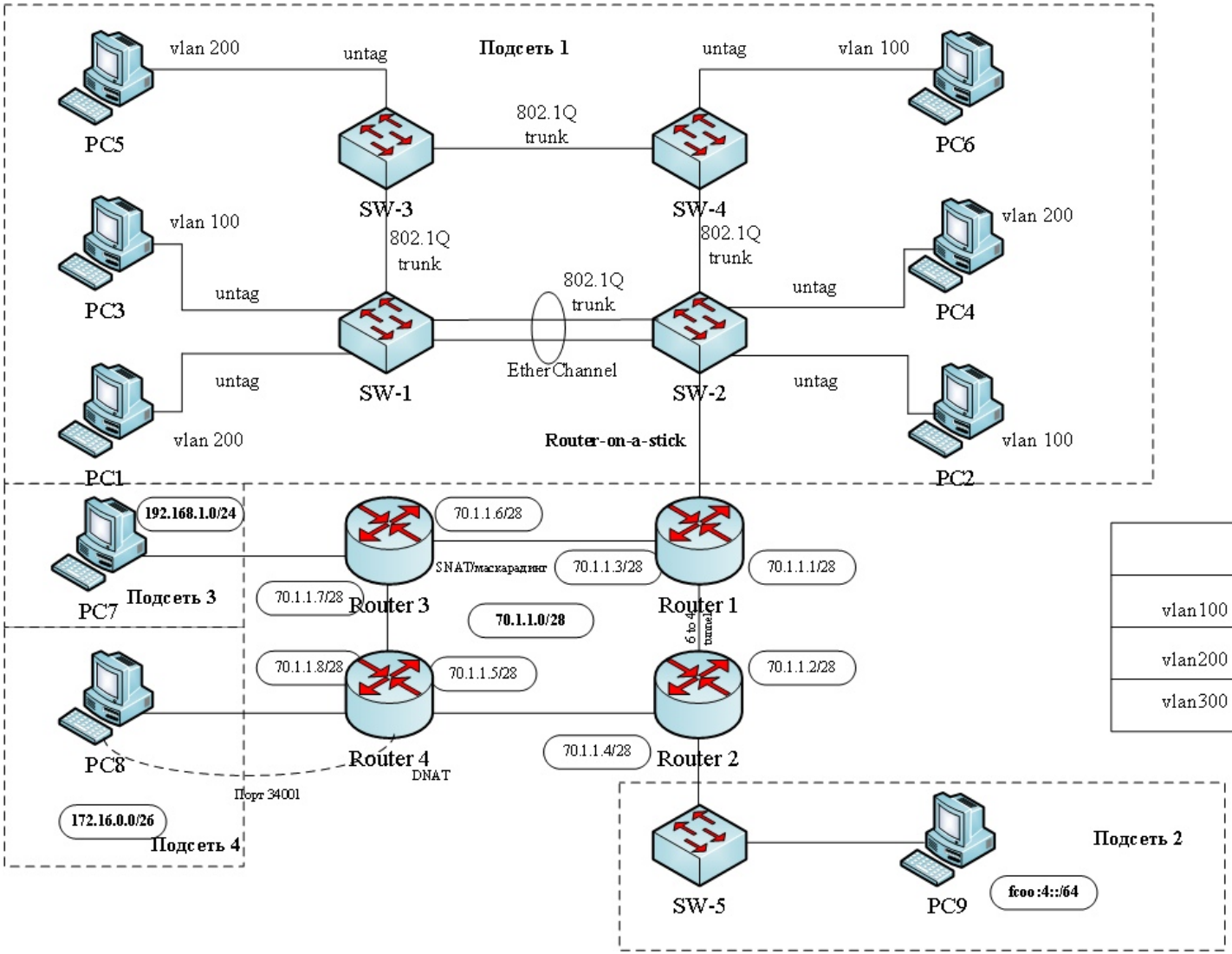
Рисунок 5.1 – Туннель 6to4

Протокол 6to4 предназначен для связи двух подсетей IPv6 через IPv4 и инкапсулирует пакеты версии 6 в тело обыкновенных IPv4-пакетов. Подробное описание работы протокола 6to4 вы можете найти в RFC3056

5.2 Задание блока 5.

1) Создайте 6to4 туннель между подсетью 1 и 2.
2) Проверьте работу созданного туннеля.

Приложение А
(обязательная)
Структурно-функциональная схема разрабатываемой сети



Подсеть 1	
vlan100	fcoo:2::/64
vlan200	fcoo:1::/64
vlan300	fcoo:3::/64