**Базовая настройка**

**Настройка SSH**

**Router > enable** - входим в привилегированный режим

**Router (config)# hostname "ИМЯ"** – настройка имени устройства

**Router (config)# enable secret** wsr – настройка пароля для входа в привилегированный режим

**Router (config)# service password-encryption – шифрование всех паролей**

**Router# clock set 17:10:00 28 Aug 2009** – настройка времени (задаём время UTC)

**Router(config)# clock timezone UTC 10** – настройка часового пояса (UTC переводим в местное время VLTA)

**Router (config)# ip domain-name wsr2017.ru** - указываем имя домена (необходимо для генерации ключа)

**Router (config)# crypto key generate rsa modulus 1024** – генерируем RSA ключ (первый вариант команды)

**Router (config)# crypto key generate rsa**  - генерируем RSA ключ (второй вариант команды, если не получается по первому)

Вводим **1024** (или то, что задано)

**Router (config)# service password-encryption** - активируем шифрование паролей

**Router (config)# username wsr2017 privilege 15 password 7 0822455D0A16** - заводим пользователя с именем **wsr2017**, паролем **cisco** и уровнем привилегий 15 Чтобы ввести пароль в зашифрованном виде

**Router (config)# username wsr2017 privilege 15 secret cisco** - заводим пользователя с именем **wsr2017**, паролем **cisco** и уровнем привилегий 15 (пароль хранится в виде хэш-функции)

**Router (config)# aaa new-model** - активируем протокол ААА

Аутентификация с использованием локальной базы данных

**Router(config)# aaa authentication login default local**

**Router(config)# username wsr2017 secret cisco**

Локальная авторизация

**Router(config)# aaa authorization exec default local**

**Router(config)# username wsr2017 privilege 15 -**  1 – минимальный 15 - максимальный

**Router# show privilege** – просмотр привилегий

Аутентификации на локальной консоли

**Router (config)#aaa new-model**

**Router(config)# aaa authentication login CONSOLE local**

**Router(config)# aaa authorization exec CONSOLE local**

**Router(config)# line con 0**

**Router(config-line)# login authentication CONSOLE**

**Router(config-line)#exit**

**Router(config)# username wsr2017 privilege 1 secret cisco**

**Router (config)# line vty 0 15** - входим в режим конфигурирования терминальных линий с 0 по 15

**Router (config-line)# transport input ssh** - указываем средой доступа через сеть по умолчанию SSH

**Router (config)#login local** - Разрешите использование входящих сеансов SSH

**Router (config-line)# logging synchronous** – удаление логов

**Router (config-line)# exec-timeout 60 0** - время таймаута до автоматического закрытия SSH в 60 мин

**Router (config)#ip ssh version 2** - используем 2-ю версию SSH

**Router (config-line)# exit** - выходим из режима конфигурирования терминальных линий

**Router (config)# exit** - выходим из режима конфигурирования

**Router # copy running-config startup-config** - сохраняем конфигурационный файл

Настройка аутентификации с использованием RADIUS-сервера.

**Router (config)#aaa new-model** - включаем ААА

**Router (config)#aaa authentication banner ^ Access only for persons explicitly authorized. All rights reserved** ^ - необязательно. Баннер о том, что это закрытая система и делать здесь нечего

**Router (config)#aaa authentication fail-message ^ Authentication failed ^** - сообщение на случай неуспешной аутентификации

**Router (config)#aaa authentication login login-RADIUS group radius local** - создаем профиль аутентификации. Не забываем, как резервный указать локальный способ аутентификации

**Router (config)#aaa authorization exec auth-RADIUS-exec group radius local** - создаем профиль авторизации.

**Router (config)#radius-server host 192.168.10.100 auth-port 1812 key cisco** - указываем наш RADUIS сервер

**Router (config)#line vty 0 15** - включаем созданные профили для виртуальных консолей

**Router (config-line)#login authentication login-RADIUS**

**Router (config-line)#login authorization exec auth-RADIUS-exec**

Создание виртуального интерфейса SVI для удалённого подключения (vlan 1 используется по умолчанию, служит как native, передаёт нетегированный трафик и на неё по умолчанию подключены все порты)

**Switch(config)# interface vlan 1**

**Switch(config-if)# ip address (адрес, маска)**

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

**Switch(config)#ip default-gateway (адрес)** – настройка шлюза по умолчанию на коммутаторе

Создание подынтерфейса

По умолчанию трафик VLAN'а 1 передается не тегированым (то есть, VLAN 1 используется как native), поэтому на физическом интерфейсе маршрутизатора задается адрес из сети VLAN 1.

Задание адреса на физическом интерфейсе:

**R1(config)#interface fa0/0**

**R1(config-if)#ip address 10.0.1.1 255.255.255.0**

#### Native VLAN

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка VLAN 5 как native:

**sw1(config-if)# switchport trunk native vlan 5**

Если необходимо создать подынтерфейс для передачи не тегированного трафика, то в этом подынтерфейсе явно указывается, что он принадлежит native VLAN. Например, если native VLAN 99:

**R1(config)# interface fa0/0.99**

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

**R1(config-if)# ip address 10.0.99.1 255.255.255.0**

Для логических подынтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN соответствующий этому интерфейсу. Это задается командой в режиме настройки подынтерфейса:

**R1(config-if)#encapsulation dot1q {vlan-id}**

Создание логического подынтерфейса для VLAN 2:

**R1(config)#interface fa0/0.2**

**R1(config-if)#encapsulation dot1q 2**

**R1(config-if)#ip address 10.0.2.1 255.255.255.0**

Создание логического подынтерфейса для VLAN 10:

**R1(config)#interface fa0/0.10**

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

**R1(config-if)#ip address 10.0.10.1 255.255.255.0**

Соответствие номера подынтерфейса и номера VLAN не является обязательным условием. Однако обычно номера подынтерфейсов задаются именно таким образом, чтобы упростить администрирование.

Создание интерфейса loopback (типа петля)

**Router (config)#interface loopback 0**

**Router (config-if)#ip address 1.1.1.1 255.255.255.255**

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

Создание сети VLAN

**Switch(config)#vlan (id)**

**Switch(config-vlan)#name (имя)**

**Изменение параметров базы данных коммутатора Cisco 2960 (3 уровневые) SDM**

Чтобы разрешить коммутатору маршрутизировать данные между VLAN и поддержку статической маршрутизации используется шаблон SDM lanbase-routing

**Switch# show sdm prefer** – просмотр шаблонов (default по умолчанию)

**Switch(config)# sdm prefer lanbase-routing**

**Switch#reload**

При включённой ipv6-адресации шаблоном по умолчанию будет **dual-ipv4-and-ipv6**

Включить поддержку IPv6, перезагрузить роутер

**Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing**

**Switch(config)# ^Z**

**Switch# wr**

**Switch# reload**

Для настройки IPv6 адресов на маршрутизаторах Cisco служат следующие команды в режиме конфигурирования интерфейса:

**R1(config-if)#ipv6 enable -** автоматическая генерация IPv6 адресов в сети LAN на интерфейсе и генерирует link-local адрес.

**Router(config)# ipv6 unicast-routing** – настройка маршрутизации

**ipv6 address 2001:db80:1234::254/64** - статическое задание адреса с префиксом 64.

**ipv6 address 2001:db80:1234::/64 eui-64** - статическое задание адреса с префиксом 64  и автоматической генерацией Interface ID по механизму EUI-64.

**ipv6 route ::/0 ethernet0/0 2001:db80:1234::ffff** - настройка маршрута по умолчанию

Команды для просмотра состояния и настроек:  
**show ipv6 interface brief  
show ipv6 interface ethernet0/0   
show ipv6 route**

Назначьте интерфейсу G0/0 глобальный индивидуальный IPv6-адрес, в дополнение к индивидуальному адресу на интерфейсе назначьте локальный адрес канала и включите IPv6-маршрутизацию.

**R1# configure terminal**

**R1(config)# interface g0/0**

**R1(config-if)# ipv6 address 2001:db8:acad:a::1/64**

**R1(config-if)# ipv6 address fe80::1 link-local**

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

**R1(config-if)# exit**

**R1(config)# ipv6 unicast-routing**

**R1(config)# exit**

Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой

**S1(config)#interface range f0/1–4 , f0/7-24 , g0/1-2**

**S1(config-if- range)#shutdown**

**Примечание**

15 – режим администратора

1 – режим EXEC

Для проверки настроек используем команду **show ip ssh**

**7** (для enable без secret, собственный алгоритм шифрования, есть программа декодирования)

**5** (для enable secret, необратимое шифрование)

**0** (незашифрованный текст) шифровать пароли (а также прочие ключи)

Чтобы подключиться по протоколу SSH, введите команду

**S1# ssh -l admin 192.168.1.1**

**R1(config)#no ip domain-lookup** – Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовать введённые команды так, как если бы они были узлами.

**R1(config-line)# logging synchronous -** Команда **logging synchronous** позволяет синхронизировать выходные данные отладки и программного обеспечения Cisco IOS, а также запрещает этим сообщениям прерывать ввод команд с клавиатуры.

**R1(config)#banner motd #Unauthorized access prohibite!#** - Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

Настройте маршрутизатор для доступа по протоколу SSH. Активируйте подключения SSH и создайте пользователя в локальной базе данных маршрутизатора.

**R1# configure terminal**

**R1(config)#ip domain-name CCNA-lab.com**

**R1(config)# username admin privilege 15 secret adminpass1**

**R1(config)# line vty 0 4**

**R1(config-line)# transport input ssh**

**R1(config-line)# login local**

**R1(config-line)# exit**

**R1(config)# crypto key generate rsa modulus 1024**

**R1(config)# exit**

Установите минимальную длину 10 символов для всех паролей.

**R1(config)#security passwords min-length 10**

Блокирование доступа к системе на 30 секунд после двух неудачных попыток входа в течение 120 сек.

**S1(config)#login block for 30 attempts 2 within 120**

Войдите в привилегированный режим EXEC и удалите файл загрузочной конфигурации.

**R1#erase startup-config**

Перезагрузите маршрутизатор.

**R1#reload**

Сохраните текущую конфигурацию в файл загрузочной конфигурации.

**R1#copy running-config startup-config**

Используя команду ping с функцией подсчета, отправьте 25 эхо запросов на узел назначения, как показано ниже. При этом в текущем каталоге будет создан текстовый файл с именем arin.txt. Этот текстовый файл будет содержать результаты эхо-запросов с помощью команды ping.

**C:\ Users\User1> ping –n 25 www.arin.net > arin.txt**

Для просмотра результатов, сохраненных в созданном файле, в окне командной строки введите more

**C:\ Users\User1> more arin.txt**

Отключить поиск в системе DNS:

**(config)# no ip domain-lookup**

Чтобы сообщения консоли не мешали вводу команд:

**(config)# line { console | vty | tty } <n>**

**(config-line)# logging synchronous**

Изменение настроек SSH

**S1(config)#ip ssh time-out 75** – лимит времени для протокола SSH

**S1(config)# ip ssh authentication-retries 2** – разрешено 2 попытки аутентификации

Чтобы завершить сеанс SSH на коммутаторе S1, введите

**Exit**

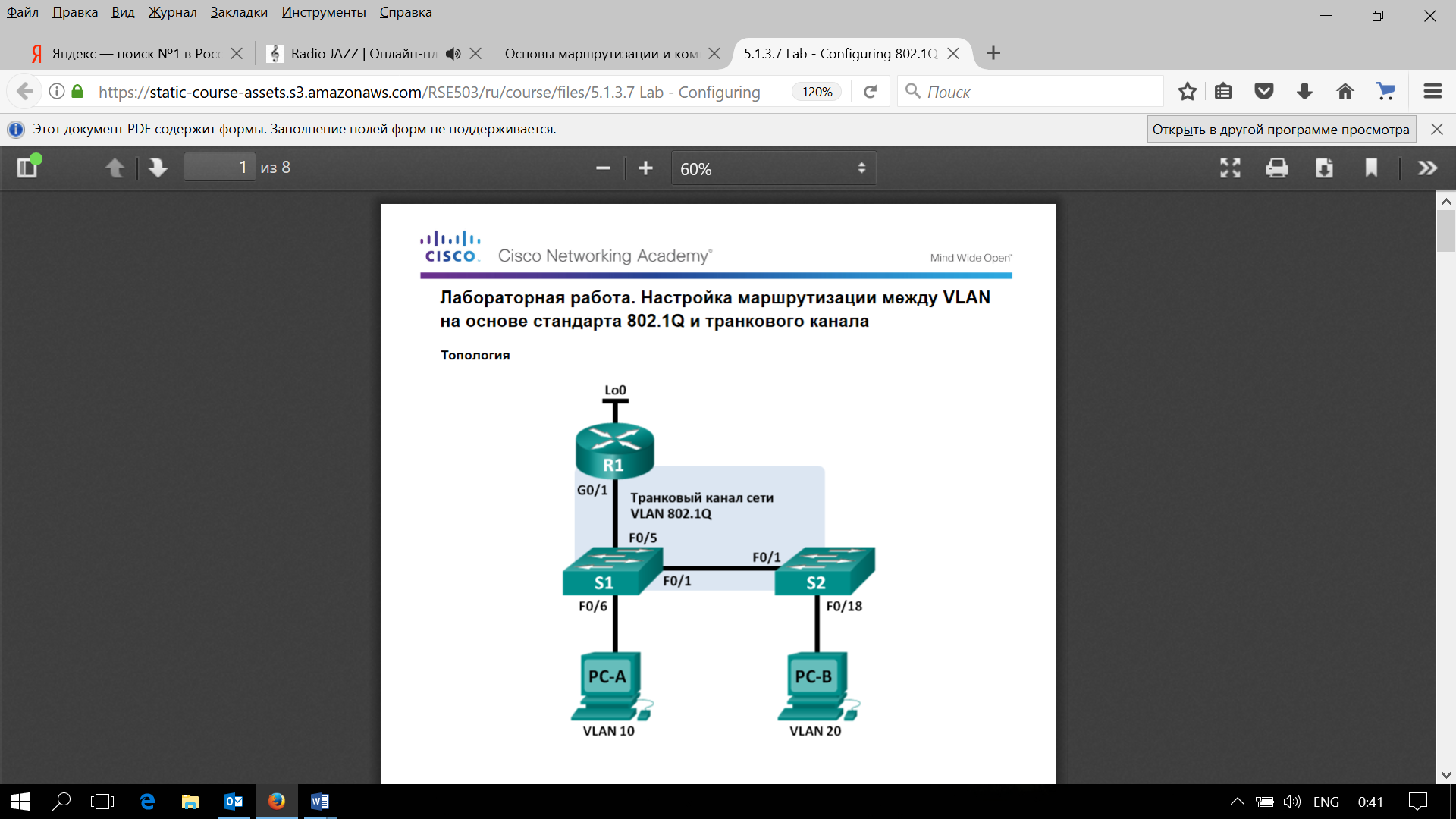
Настройте новый MAC-адрес для интерфейса, используя aaaa.bbbb.cccc в качестве адреса

**R1(config-if)#mac-address aaaa.bbbb.cccc**

**R1(config-if)#no mac-address aaaa.bbbb.cc**

Сеансы HTTP отправляют все данные в незашифрованном виде. Вам нужно отключить сервис HTTP, который работает на коммутаторе S1

**S1(config)#no ip http server**



Коммутатор S1

**S1(config)# vlan 10**

**S1(config-vlan)# name Students**

**S1(config-vlan)# vlan 20**

**S1(config-vlan)# name Faculty**

**S1(config-vlan)# exit**

**S1(config)# interface f0/1**

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

**S1(config-if)# interface f0/5**

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

**S1(config-if)# interface f0/6**

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

**S1(config-if)# switchport access vlan 10**

Коммутатор S2

**S2(config)# vlan 10**

**S2(config-vlan)# name Students**

**S2(config-vlan)# vlan 20**

**S2(config-vlan)# name Faculty**

**S2(config)# interface f0/1**

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

**S2(config-if)# interface f0/18**

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

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

Маршрутизатор R1

**R1(config)# interface g0/1.1**

**R1(config-subif)# encapsulation dot1Q 1**

**R1(config-subif)# ip address 192.168.1.1 255.255.255.0**

**R1(config-subif)# interface g0/1.10**

**R1(config-subif)# encapsulation dot1Q 10**

**R1(config-subif)# ip address 192.168.10.1 255.255.255.0**

**R1(config-subif)# interface g0/1.20**

**R1(config-subif)# encapsulation dot1Q 20**

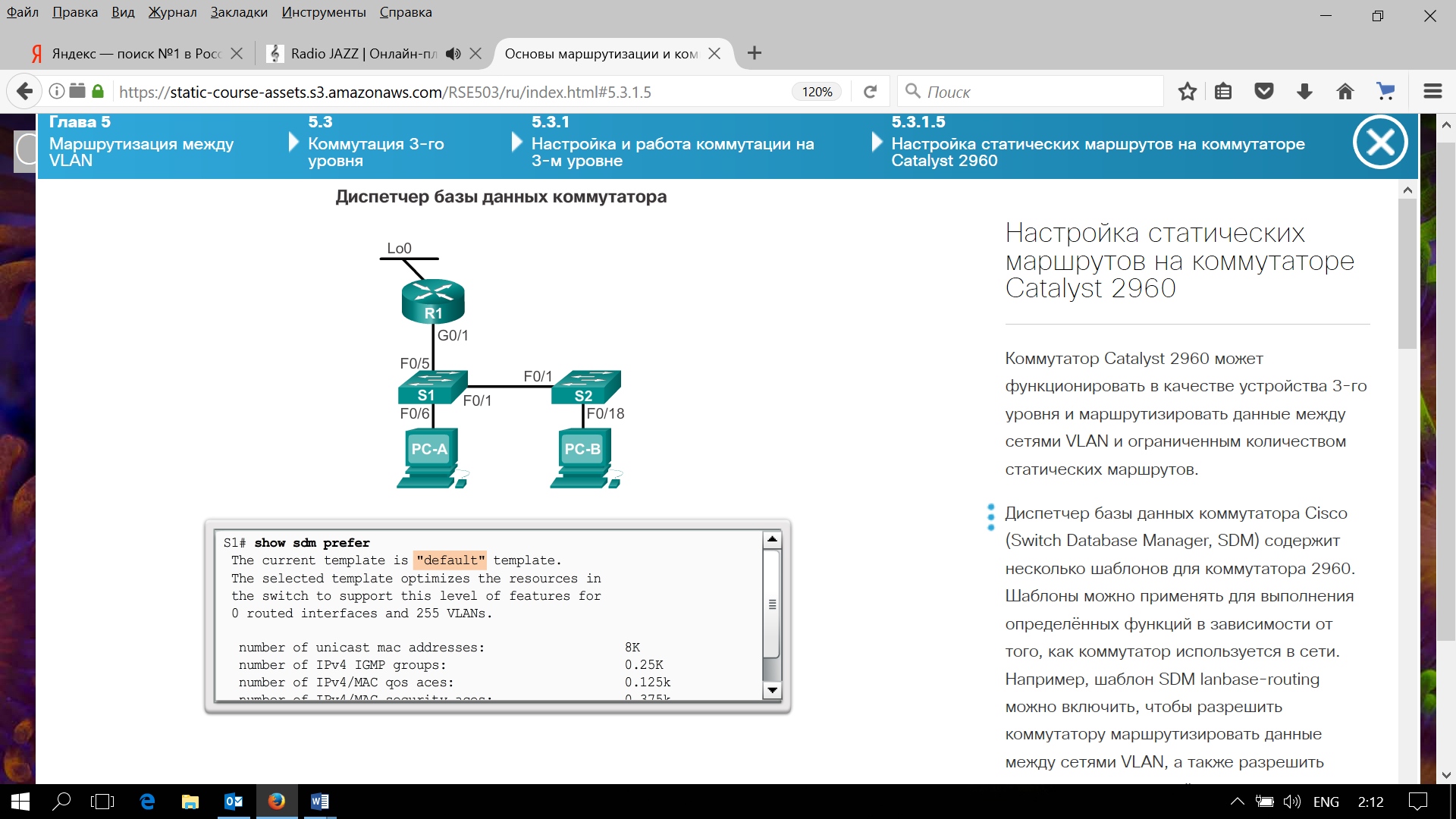
**R1(config-subif)# ip address 192.168.20.1 255.255.255.0**

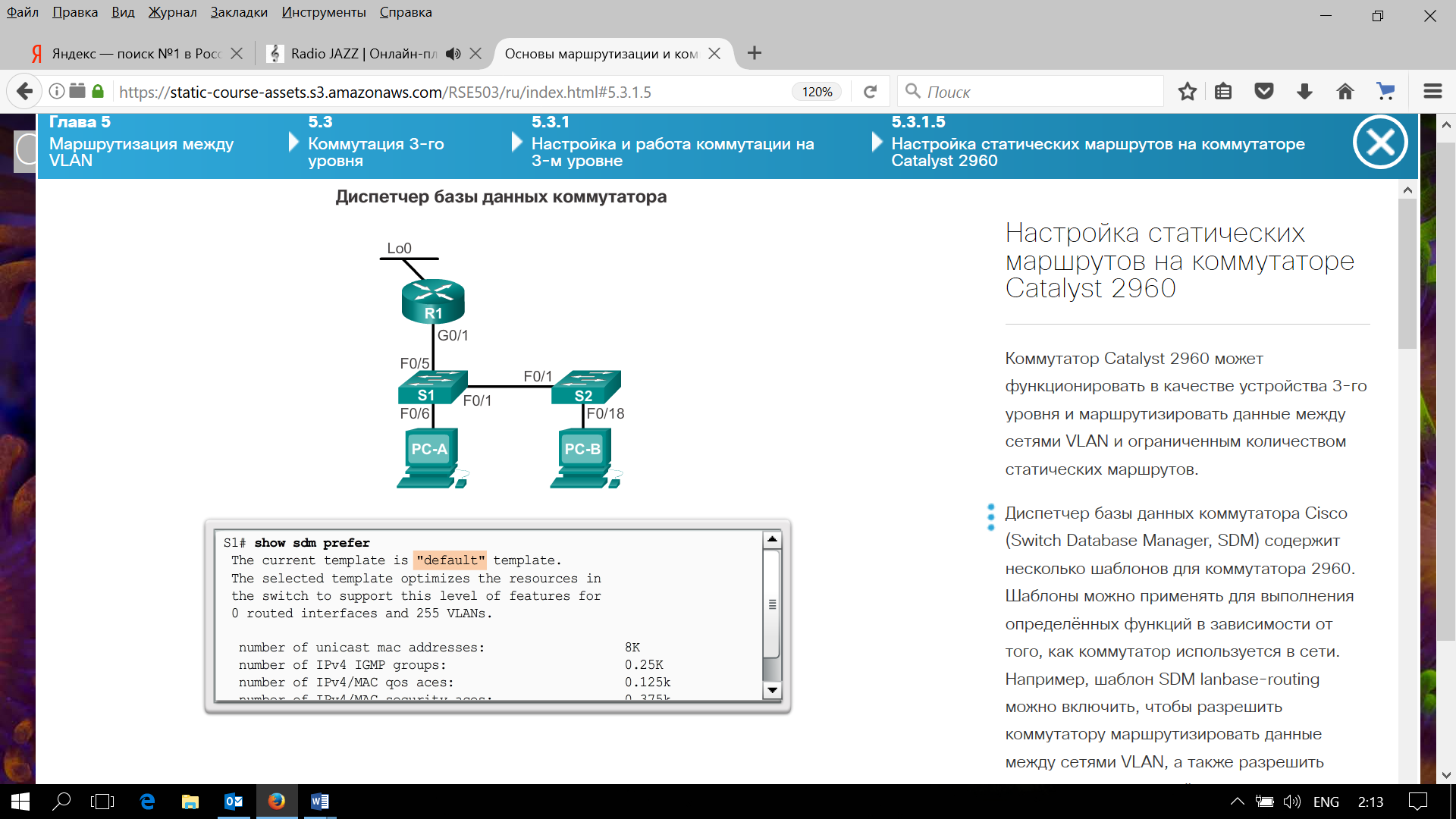
**R1(config-subif)# exit**

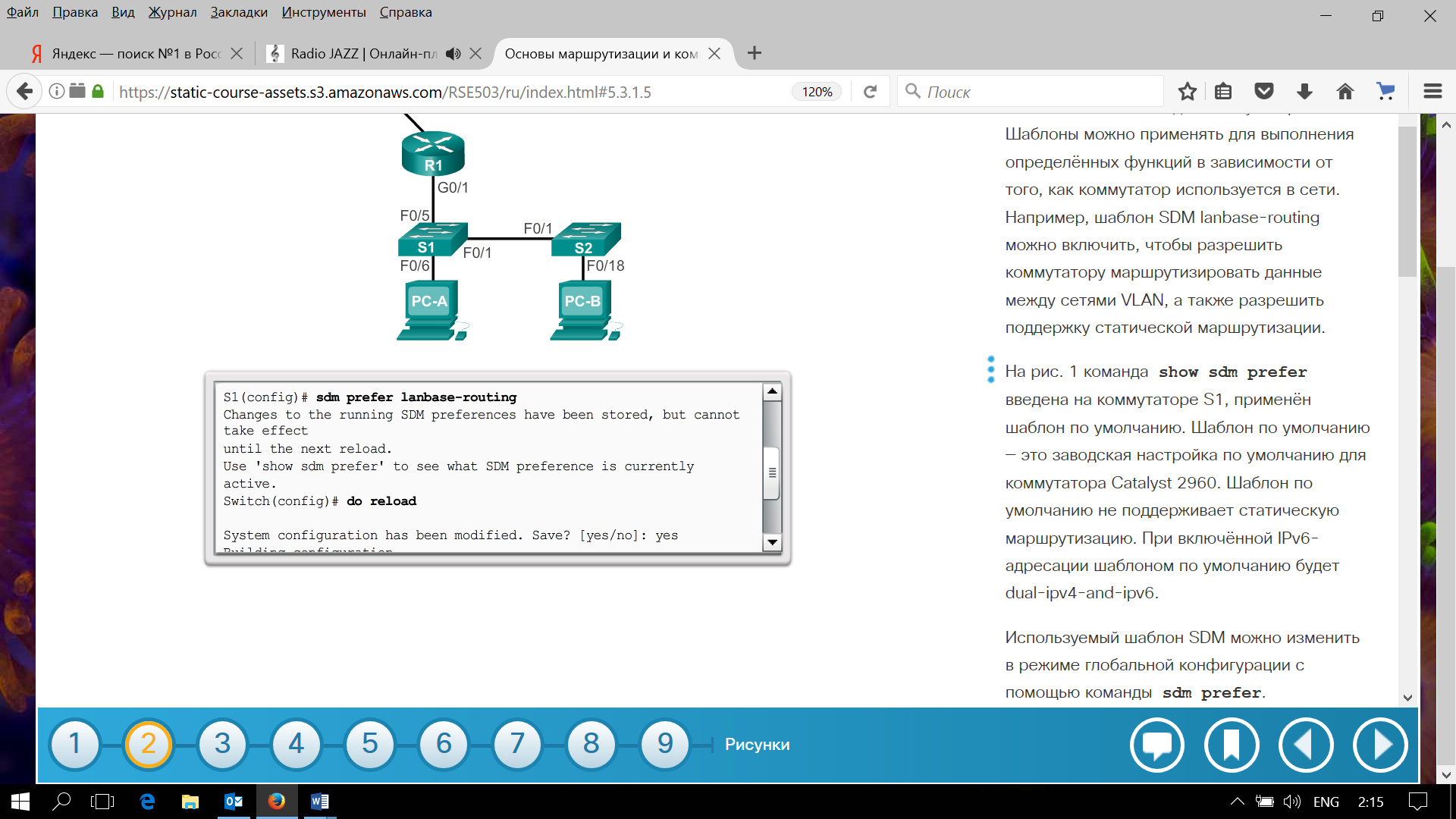
**R1(config)# interface g0/1**

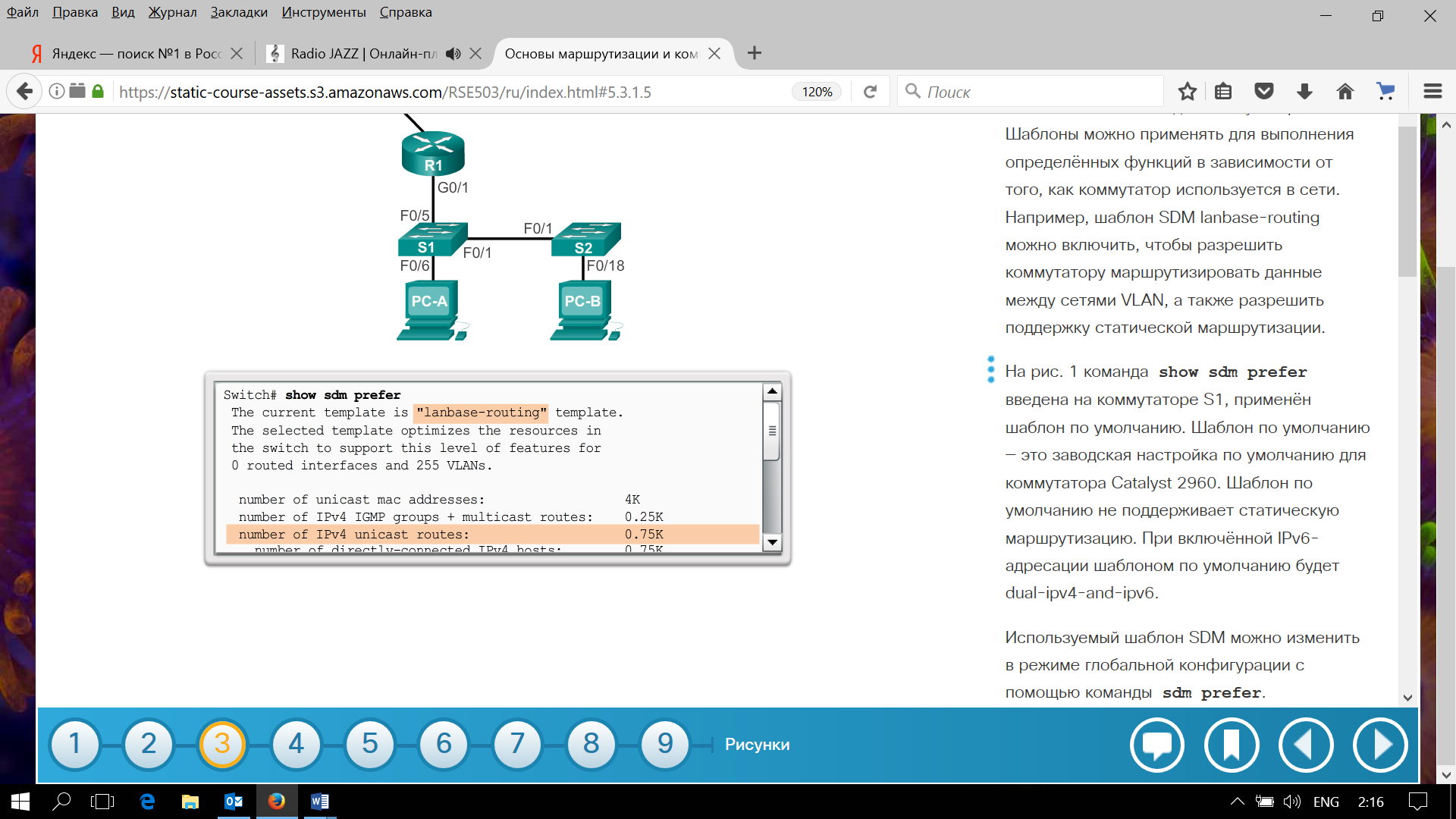
**R1(config-if)# no shutdown**

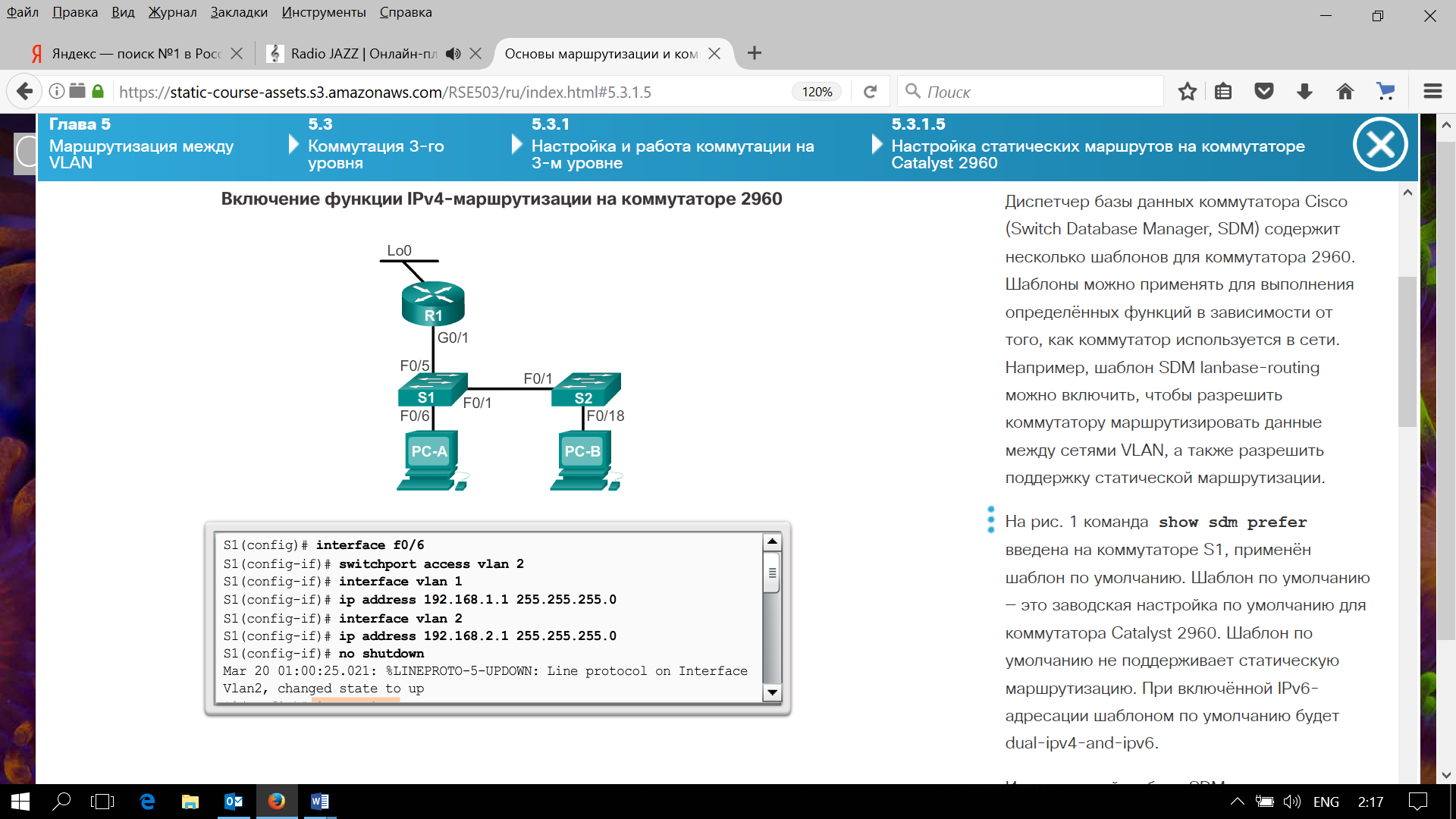
**Настройка коммутаторов 3 уровня для коммутации между VLAN**

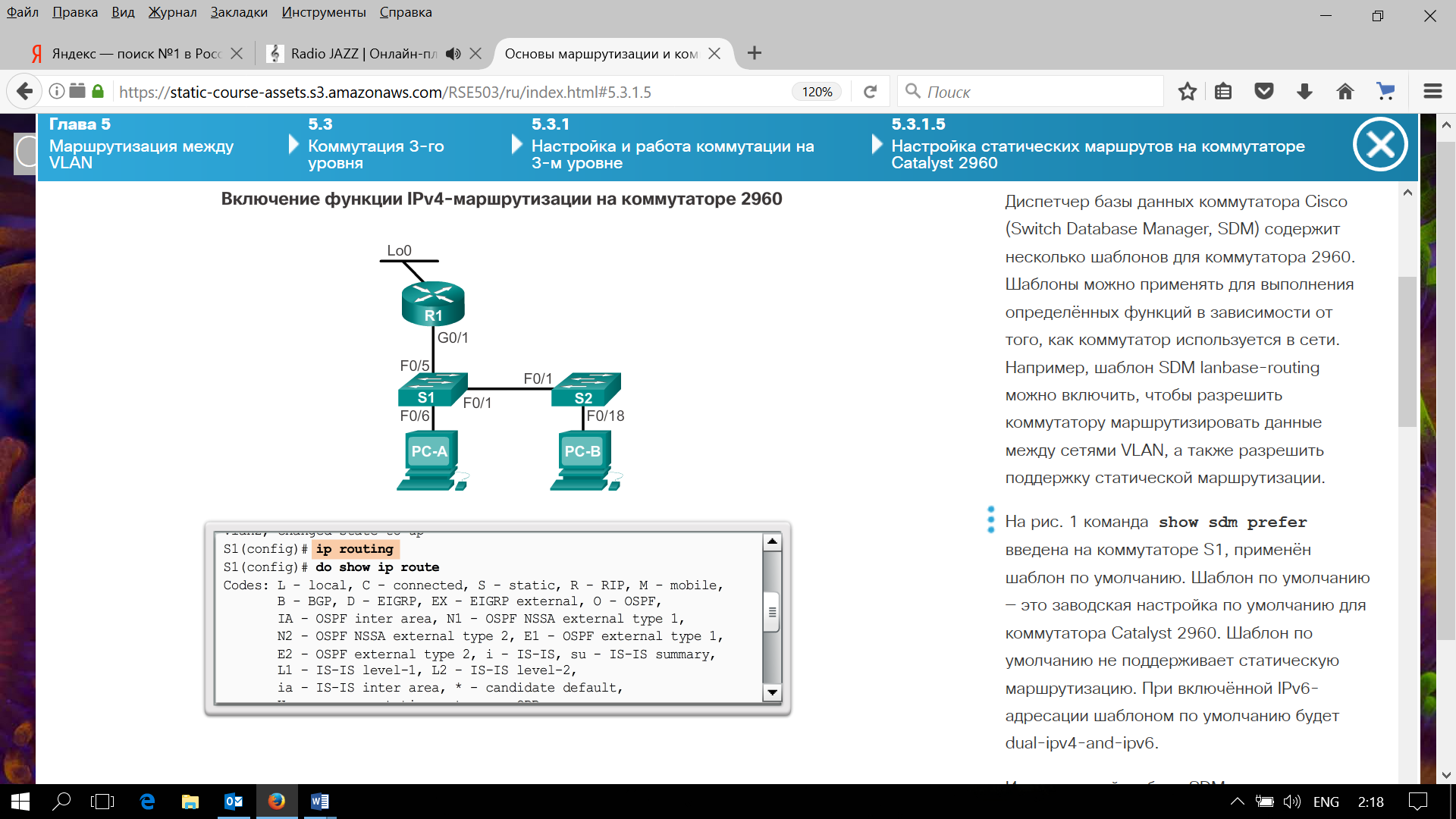


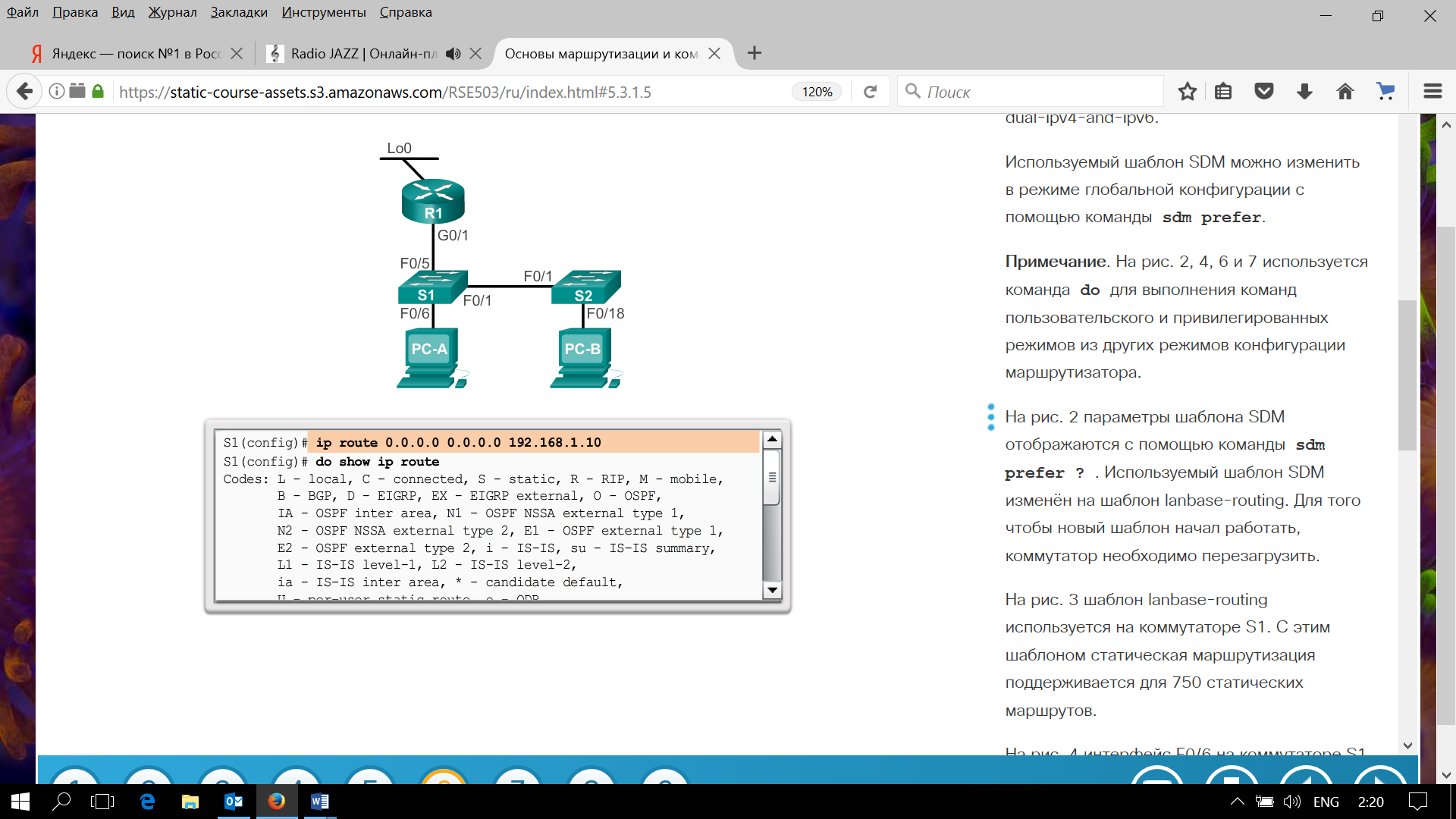


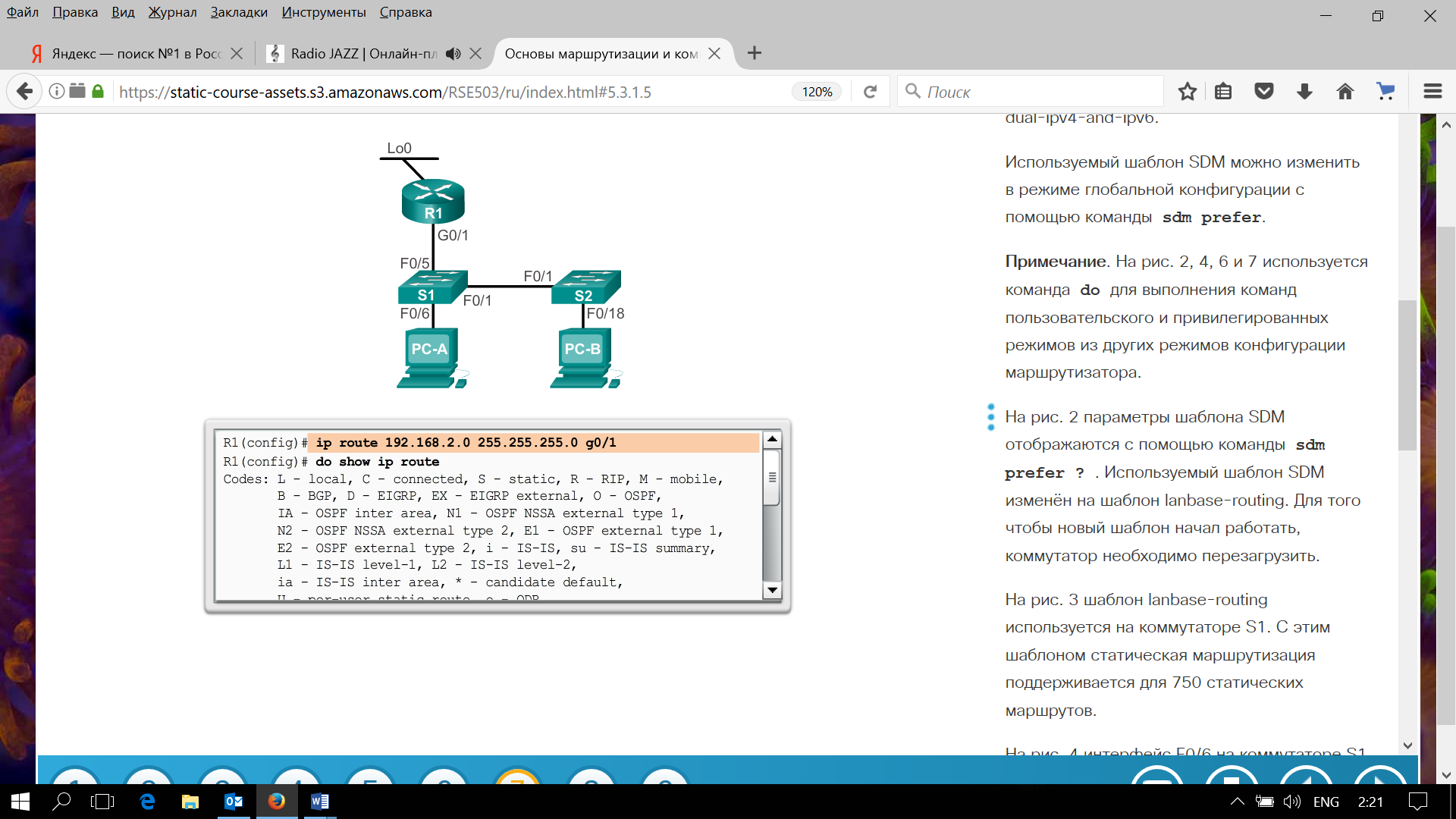












Подключение S0/0/0 - это подключение DCE, которое требует выполнения команды clock rate. Настройка интерфейса S0/0/0 маршрутизатора R3 отображена ниже.

**R3(config)# interface s0/0/0**

**R3(config-if)# ip address 10.1.1.2 255.255.255.252**

**R3(config-if)# clock rate 128000**

**R3(config-if)# no shutdown**

Настройка статического маршрута

Настройка рекурсивного статического маршрута.

**R1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2**

Настройка статического маршрута с прямым подключением.

**R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0**

Удаление статического маршрута.

**R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1**

или

**R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2**

или

**R1(config)# no ip route 209.165.200.224 255.255.255.224**

Настройка маршрута по умолчанию

**R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1**

**R1(config)# ipv6 route ::/0 { ipv6-address | exit-intf }**

**Настройка статических маршрутов IPv 6 и маршрутов IPv-6 по умолчанию**

Для того чтобы маршрутизатор мог осуществлять пересылку пакетов для IPv6, необходимо настроить команду глобальной конфигурации **ipv6 unicast-routing**.

В режиме глобальной конфигурации активируйте IPv6-маршрутизацию на маршрутизаторе R1.

**R1(config)# ipv6 unicast-routing**

Присвойте сетевым интерфейсам маршрутизатора R1 IPv6-адреса. Обратите внимание на то, что протокол IPv6 активирован на каждом интерфейсе. Интерфейс G0/1 имеет глобально маршрутизируемый индивидуальный адрес, EUI-64 используется для создания идентификатора в адресе. Интерфейс S0/0/1 имеет локально-маршрутизируемый, уникальный локальный адрес, который рекомендуется использовать для последовательных соединений типа точка-точка.

**R1(config)# interface g0/1**

**R1(config-if)# ipv6 address 2001:DB8:ACAD:A::/64 eui-64**

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

**R1(config-if)# interface serial 0/0/1**

**R1(config-if)# ipv6 address FC00::1/64**

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

**R1(config-if)# exit**

В режиме глобальной конфигурации активируйте IPv6-маршрутизацию на маршрутизаторе R3.

**R3(config)# ipv6 unicast-routing**

Присвойте сетевым интерфейсам маршрутизатора R3 IPv6-адреса. Обратите внимание на то, что протокол IPv6 активирован на каждом интерфейсе. Интерфейс G0/1 имеет глобально маршрутизируемый индивидуальный адрес, EUI-64 используется для создания идентификатора в адресе. Интерфейс S0/0/0 имеет локально-маршрутизируемый, уникальный локальный адрес, который рекомендуется использовать для последовательных соединений типа точка-точка. Значение тактовой частоты уже установлено, поскольку это DCE-конец последовательного кабеля.

**R3(config)# interface gigabit 0/1**

**R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64**

**R3(config-if)# no shutdown**

**R3(config-if)# interface serial 0/0/0**

**R3(config-if)# ipv6 address FC00::2/64**

**R3(config-if)# clock rate 128000**

**R3(config-if)# no shutdown**

**R3(config-if)# exit**

На маршрутизаторе R1 удалите рекурсивный статический маршрут и добавьте статический маршрут по умолчанию.

**R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2**

**R1(config)# ipv6 route ::/0 serial 0/0/1**

Настройка маршрутизации OSPFv3

**R1(config)# ipv6 router ospf 1**

**R1(config-rtr)# router-id 1.1.1.1**

Выполните команду ipv6 ospf 1 area 0 для каждого интерфейса маршрутизатора R1, который должен участвовать в маршрутизации OSPFv3.

**R1(config)# interface g0/0**

**R1(config-if)# ipv6 ospf 1 area 0**

**R1(config-if)# interface s0/0/0**

**R1(config-if)# ipv6 ospf 1 area 0**

**R1(config-if)# interface s0/0/1**

**R1(config-if)# ipv6 ospf 1 area**

**Настройка, применение и проверка стандартных ACL-списков**

Создайте ACL-список с номером 1 на маршрутизаторе R2, установив запрет доступа к сети 192.168.20.0/24 от сети 192.168.11.0/24.

**R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255**

По умолчанию список доступа отклоняет трафик, не соответствующий заданному правилу. Чтобы разрешить другой трафик, задайте следующее правило:

**R2(config)# access-list 1 permit any**

Чтобы ACL-список осуществлял фильтрацию трафика, он должен быть применён на каком-либо маршрутизаторе. Примените ACL-список, разместив его для исходящего трафика интерфейса Gigabit Ethernet 0/0.

**R2(config)# interface GigabitEthernet0/0**

**R2(config-if)# ip access-group 1 out**

Настройте стандартный именованный ACL-список.

**R1(config)# ip access-list standard File\_Server\_Restrictions**

**R1(config-std-nacl)# permit host 192.168.20.4**

**R1(config-std-nacl)# deny any**

Проверьте конфигурацию и работоспособность списка ACL.

Введите команду **show access-list**, чтобы проверить конфигурации ACL-списков. Введите команду **show run** или **show ip interface gigabitethernet 0/0**, чтобы проверить размещения ACL-списков.

В процессе тестирования ACL-списка, счётчики можно обнулить, выполнив команду **clear access-list counters.**

**Настройка и проверка ACL-списков для IPv6**

Настройте IPv6-параметры на маршрутизаторе R1.

Настройте индивидуальный IPv6-адрес на интерфейсах G0/0, G0/1 и S0/0/0.

Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте FE80:: 1в качестве локального адреса канала.

На интерфейсе S0/0/0 установите тактовую частоту 128000.

Включите интерфейсы.

Включите IPv6-маршрутизацию одноадресной передачи.

Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/0.

**R1(config)# ipv6 route ::/0 s0/0/0**

Настройте параметры IPv6 на маршрутизаторе R

Настройте и проверьте ограничения VTY на маршрутизаторе R1.

Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64. Все узлы должны обладать доступом к маршрутизатору R1 только через telnet.

**R1(config)# ipv6 access-list RESTRICT-VTY**

**R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any**

**R1(config-ipv6-acl)# permit tcp any any eq 22**

Примените ACL-список под именем RESTRICT-VTY на линиях VTY маршрутизатора R1.

**R1(config-ipv6-acl)# line vty 0 4**

**R1(config-line)# ipv6 access-class RESTRICT-VTY in**

**R1(config-line)# end**

**R1#**

Примените список на интерфейсе

**R1(config)#interface s0/0/0**

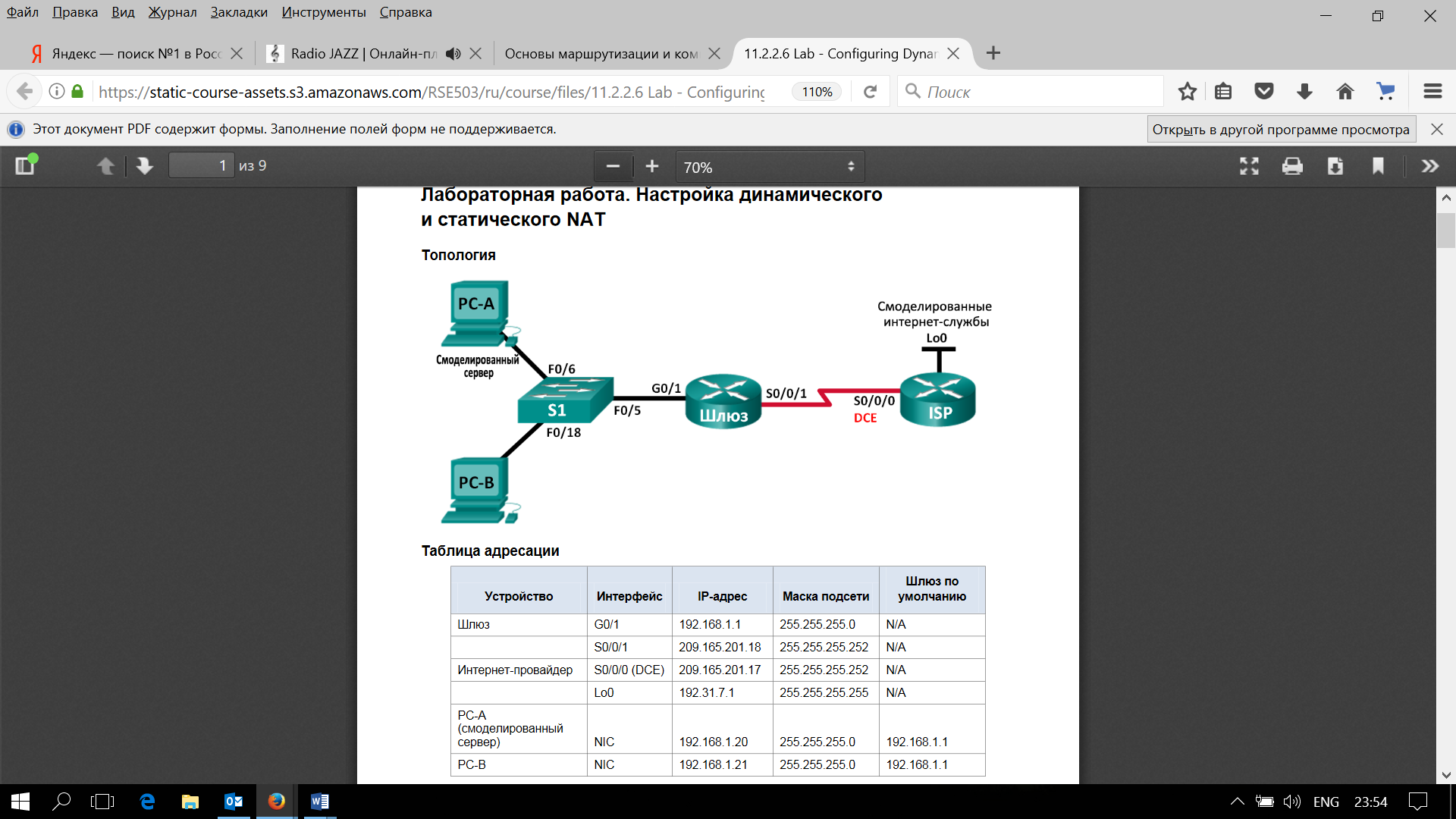
**R1(config-if)#ipv6 traffic-filter RESTRICT-VTY in**

Отобразите новый ACL-список.

**R1# show access-lists**

Для того чтобы отменить действие косвенного отказа, присутствующего в конце любого ACL-списка и запрещающего весь трафик, можно добавить разрешающую команду **permit ip any any**

**Настройка статического и динамического NAT**



Настройте статическую маршрутизацию.

Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза, используя диапазон назначенных публичных сетевых адресов 209.165.200.224/27.

**ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18**

Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

**Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201**

Настройте статическое сопоставление.

**Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225**

Задайте интерфейсы.

**Gateway(config)# interface g0/1**

**Gateway(config-if)# ip nat inside**

**Gateway(config-if)# interface s0/0/1**

**Gateway(config-if)# ip nat outside**

Проверьте конфигурацию.

**Gateway# show ip nat translation**

Перед добавлением динамических преобразований очистите все NAT и удалите статистику

**Gateway# clear ip nat translation \***

**Gateway# clear ip nat statistics**

Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.

**Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255**

Определите пул пригодных к использованию публичных IP-адресов.

**Gateway(config)#ip nat pool public\_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224**

Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.

**Gateway(config)# ip nat inside source list 1 pool public\_access**

На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT.

**Gateway# show ip nat translation**

**Команды show**

**show running-config**

**show interfaces**

**show interfaces fastEthernet 0/18**

**show arp**

**show ip route**

**show protocols**

**show version**

**show cdp neighbors**

**arp –a**

**arp -d для очистки кэша**

**ipconfig /all**

**ipconfig /displaydns**

**show ip interface brief**

**show ip ssh**

**show ssh**

**show ip http server status**

**show port-security interface f0/5**

**show vlan**

**show vlan brief**

**show interfaces f0/18 switchport**

**show vlan summary**

**show dtp interface** *(id)* - Чтобы определить текущий режим DTP (транковый канал)

**show interfaces trunk**

**show ipv6 int brief** - Чтобы проверить параметры IPv6 на маршрутизаторе

**show ipv6 route**

**show ipv6 route static**

**show ipv6 route network**

**show access-lists**

**show access-lists 1 – отобразите текущий ACL-список**

**show running-config | section dhcp**

**show ip dhcp server statistics**

**show ipv6 interface**

**show ipv6 dhcp pool**

**show ipv6 dhcp binding**

**show ip nat translations** - проверка работы NAT

**show ip nat statistics**

**Горячие клавиши:**

**Стрелка вниз** — позволяет пользователю пролистывать предыдущие команды вперед

**Стрелка вверх** — позволяет пользователю пролистывать предыдущие команды назад

**Tab** — завершает частично набранную команду или ключевое слово

**Ctrl-А** — перемещает в начало строки

**Ctrl-Е** — перемещает в конец строки

**Ctrl-R** — обновляет строку

**Ctrl-Z** — выходит из режима конфигурации и возвращает в пользовательский режим

**Ctrl-C** — выходит из режима конфигурации или прерывает текущую команду

**Ctrl-Shift-6** — позволяет пользователю прервать процесс IOS, например, ping или traceroute.