

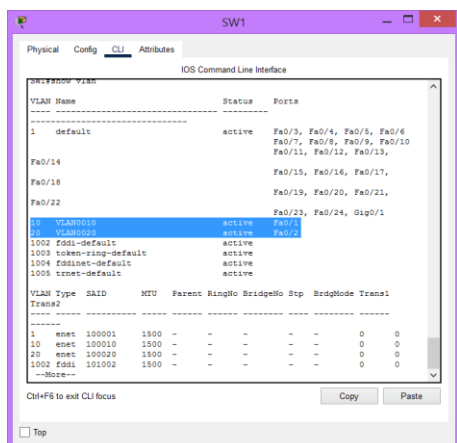
Домашнее задание:

1. Основным шлюзом для компьютера PC и для компьютера PC1 должен быть роутер R1
2. Компьютеры PC0 и PC1 должны получать IP адреса от DHCP сервера автоматически
3. Трафик от компьютера PC0 и от компьютера PC1 должен быть логически разделен на коммутаторах SW1 и SW2 (используйте vlan id 10 и 20)
4. При трассировке Web-server от компьютеров PC0 или PC1 трафик должен идти по маршруту PC->R1->R2->R3->Web-server
5. Трафик между DHCP сервером и Web сервером должен быть логически разделен (используйте vlan id 10 и 20)

Настройка VLAN

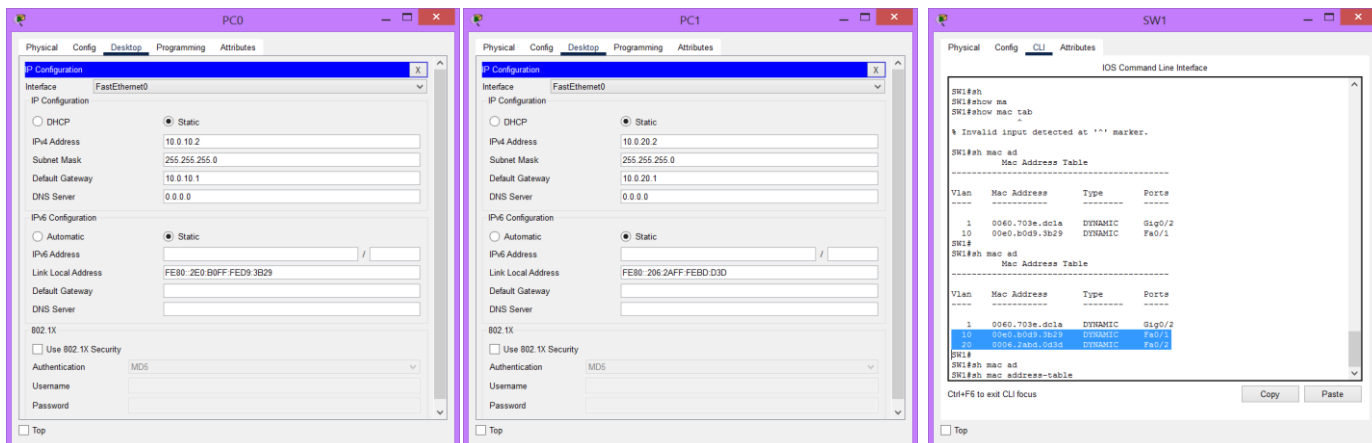
Настроим порты «Sw1» через CLI:

Switch>	enable	Переход в привилегированный режим
Switch #	show vlan	Посмотрим установленные VLANы
Switch #	configure terminal	Переход в режим конфигурирования терминала
Switch (config)#	hostname SW1	Назовем свитч
SW1(config)#	vlan 10	Создание VLAN «10»
SW1(config-vlan)#	vlan 20	Создание VLAN «20»
SW1(config-vlan)#	exit	
SW1(config)#	int fastEthernet 0/1	В режим редактирования порта «0/1»
SW1(config-if)#	switchport mode access	Установим режим работы порта «access»
SW1(config-if)#	switchport access vlan 10	Назначим на порт VLAN «10»
SW1(config-if)#	exit	
SW1(config)#	int fastEthernet 0/2	В режим редактирования порта «0/2»
SW1(config-if)#	switchport mode access	Установим режим работы порта «access»
SW1(config-if)#	switchport access vlan 20	Назначим на порт VLAN «20»
SW1(config-if)#	exit	
SW1(config)#	int gigabitEthernet 0/2	В режим редактирования порта «0/2»
SW1(config-if)#	switchport mode trunk	Установим режим работы порта «trunk» (между свитчами, для передачи VLAN «как есть»)
SW1(config-if)#	switchport trunk allowed vlan 10,20	Укажем, какие VLAN пропускать (не обязательно)
SW1(config-if)#	exit	
SW1(config)#	exit	
SW1#	show vlan	Смотрим результат настройки VLAN



Временно настроим статическую маршрутизацию на «PC0» и «PC1», чтобы убедиться, что они друг друга не видят в рамках «SW1», «SW2» и только с вводом роутера «R1» начинают пинговаться.

Кстати, если запустить на «SW1» команду «sh mac address-table», то увидим, что в ней присутствуют VLAN и МАК-адреса «PC0» и «PC1»



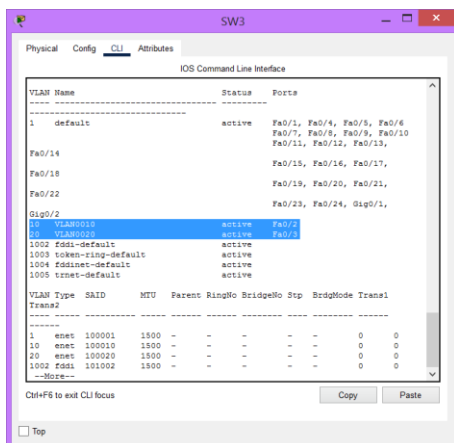
Настроим порты «Sw2» через CLI:

Switch>	enable	Переход в привилегированный режим
Switch #	show vlan	Посмотрим установленные VLANы
Switch #	configure terminal	Переход в режим конфигурирования терминала
Switch (config)#	hostname SW2	Назовем свитч
SW2(config)#	vlan 10	Создание VLAN «10»
SW2(config-vlan)#	vlan 20	Создание VLAN «20»
SW2(config-vlan)#	vlan 30	Создание VLAN «30» (для потока от «R1» к «R2»)
SW2(config)#	int gigabitEthernet 0/2	В режим редактирования порта «0/2»
SW2(config-if)#	switchport mode trunk	Установим режим работы порта «trunk» (между свитчами, для передачи VLAN «как есть»)
SW2(config-if)#	switchport trunk allowed vlan 10,20,30	Укажем, какие VLAN пропускать (не обязательно)
SW2(config-if)#	exit	
SW2(config)#	int fastEthernet 0/1	В режим редактирования порта «0/1»
SW2(config-if)#	switchport mode trunk	Установим режим работы порта «trunk» (между свитчами, для передачи VLAN «как есть»)
SW2(config-if)#	switchport trunk allowed vlan 10,20,30	Укажем, какие VLAN пропускать (не обязательно)
SW2(config-if)#	exit	
SW2(config)#	int fastEthernet 0/2	В режим редактирования порта «0/2»
SW2(config-if)#	switchport mode access	Установим режим работы порта «access» (по порту пойдет трафик от «R1» к «R2» со снятием тэга VLAN)
SW2(config-if)#	switchport access vlan 30	Назначим на порт VLAN «30»
SW2(config-if)#	exit	
SW2(config)#	exit	
SW2#	show vlan	Смотрим результат настройки VLAN

Настроим порты VLAN для WEB-server и DHCP

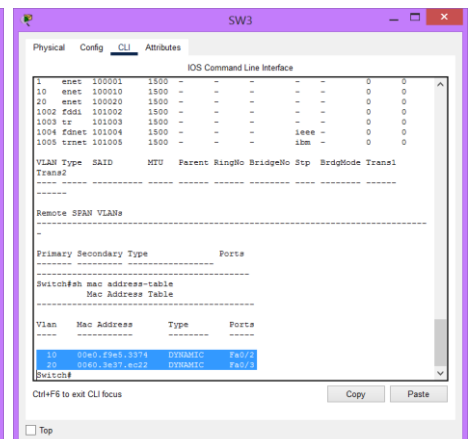
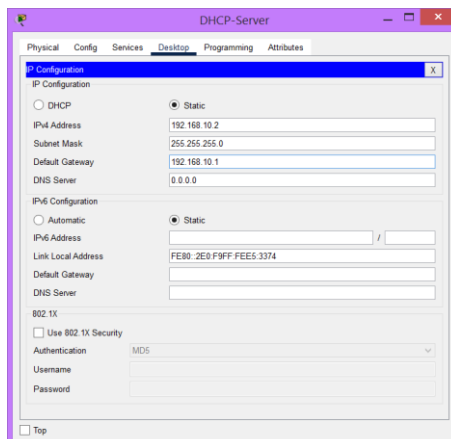
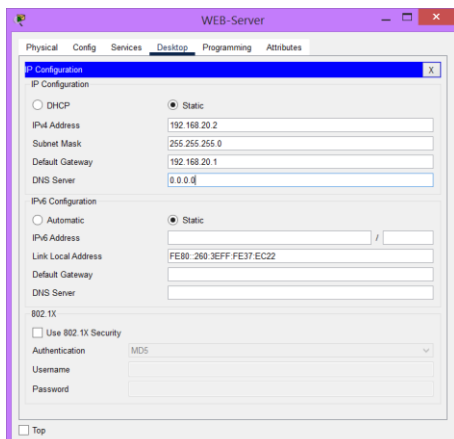
VLAN на «SW3» через CLI:

Switch>	enable	Переход в привилегированный режим
Switch #	show vlan	Посмотрим установленные VLANы
Switch #	configure terminal	Переход в режим конфигурирования терминала
Switch (config)#	hostname SW3	Назовем свитч
SW3(config)#	vlan 10	Создание VLAN «10»
SW3(config-vlan)#	vlan 20	Создание VLAN «20»
SW3(config-vlan)#	exit	
SW3(config)#	int fastEthernet 0/2	В режим редактирования порта
SW3(config-if)#	switchport mode access	Установим режим работы порта «access»
SW3(config-if)#	switchport access vlan 10	Назначим на порт VLAN «10»
SW3(config-if)#	exit	
SW3(config)#	int fastEthernet 0/3	В режим редактирования порта
SW3(config-if)#	switchport mode access	Установим режим работы порта «access»
SW3(config-if)#	switchport access vlan 20	Назначим на порт VLAN «20»
SW3(config-if)#	exit	
SW3(config)#	int fastEthernet 0/1	В режим редактирования порта
SW3(config-if)#	switchport mode trunk	Установим режим работы порта «trunk» (между свитчами, для передачи VLAN «как есть»)
SW3(config-if)#	switchport trunk allowed vlan 10,20	Укажем, какие VLAN пропускать (не обязательно)
SW3(config-if)#	exit	
SW3(config)#	exit	
SW3#	show vlan	Смотрим результат настройки VLAN



Аналогично PC0 и PC1, настроим статическую маршрутизацию на «WEB-server» и «DHSP», чтобы убедиться, что они друг друга не видят в рамках «SW3» и только с вводом роутера «R3» начинают пинговаться.

Если запустить на «SW3» команду «sh mac address-table», то увидим, что в ней присутствуют VLAN и MAC-адреса серверов

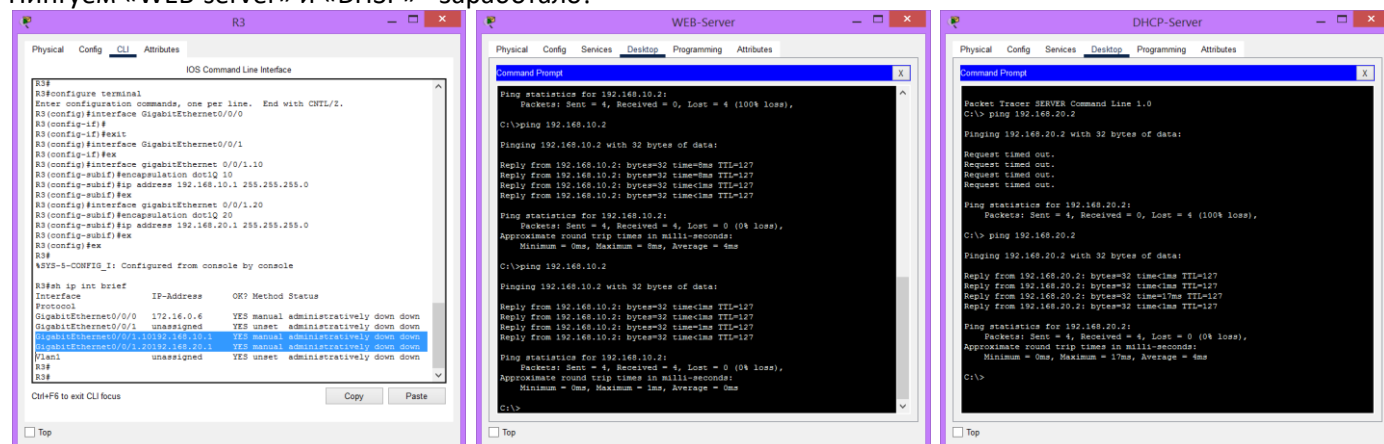


Настройка «R3»

Дело в том, что роутер «не понимает» VLAN и ждет Ethernet-пакеты...настраиваем аналогично «R1»:

Router>	enable	Переход в привилегированный режим
Router#	configure terminal	Переход в режим конфигурирования терминала
Router(config)#	hostname R3	Назовем Роутер
R3(config)#	interface gigabitEthernet 0/0/1.10	Создаем саб-интерфейс «10»
R3(config-subif)#	encapsulation dot1Q 10	Использовать протокол «.1Q» для VAN «10»
R3(config-subif)#	ip address 192.168.10.1 255.255.255.0	Установим IP адрес
R3(config-subif)#	exit	Выйти на уровень ниже
R3(config)#	interface gigabitEthernet 0/0/1.20	Создаем саб-интерфейс «20»
R3(config-subif)#	encapsulation dot1Q 20	Использовать протокол «.1Q» для VAN «20»
R3(config-subif)#	ip address 192.168.20.1 255.255.255.0	Установим IP адрес
R3(config-subif)#	exit	Выйти на уровень ниже
Router#	sh ip int brief	Выведем настроенные интерфейсы и сабинтерфейсы

Пингуем «WEB-server» и «DHSP» - заработало!



Настроим маршрутизацию по протоколу RIP2

Настроим «R1» через CLI:

R1#	show ip interface brief	Показывает настроенные порты и IP-адреса (впоследствии их удобно копировать для команды network)
R1#	configure terminal	Переход в режим конфигурирования терминала
R1 (config)#	router rip	Переход в конфигурирование протокола RIP
R1 (config-router)#	version 2	Выбираем вторую версию протокола RIP_2
R1 (config-router)#	no auto-summary	Отключаем суммирование маршрутов
R1 (config-router)#	network 172.16.0.1	Подключаем протокол к сети...
R1 (config-router)#	network 10.0.0.0	Подключаем протокол к сети...
R1 (config-router)#	End	

будем анонсировать сети «10.0.10.0/24» и «10.0.20.0/24» (иначе, без туннелирования и «танцев с бубном» впоследствии будет трудно настроить автоматическую выдачу IP от DHSP-server

Настроим «R2» через CLI:

R2#	show ip interface brief	Показывает настроенные порты и IP-адреса (впоследствии их удобно копировать для команды network)
R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	router rip	Переход в конфигурирование протокола RIP
R2 (config-router)#	version 2	Выбираем вторую версию протокола RIP_2
R2 (config-router)#	no auto-summary	Отключаем суммирование маршрутов
R2 (config-router)#	network 172.16.0.2	Подключаем протокол к сети...
R2 (config-router)#	network 172.16.0.5	Подключаем протокол к сети...
R2 (config-router)#	End	

Настроим «R3» через CLI:

R3#	show ip interface brief	Показывает настроенные порты и IP-адреса (впоследствии их удобно копировать для команды network)
R3#	configure terminal	Переход в режим конфигурирования терминала
R3 (config)#	router rip	Переход в конфигурирование протокола RIP
R3 (config-router)#	version 2	Выбираем вторую версию протокола RIP_2
R3 (config-router)#	no auto-summary	Отключаем суммирование маршрутов
R3 (config-router)#	network 172.16.0.6	Подключаем протокол к сети...
R3 (config-router)#	network 192.168.10.0	Подключаем протокол к сети...
R3 (config-router)#	network 192.168.20.0	Подключаем протокол к сети...
R2 (config-router)#	End	
будем анонсировать сети «192.168.10.0/24» и «192.168.20.0/24» (в задании не указано сокрытие за NAT)		

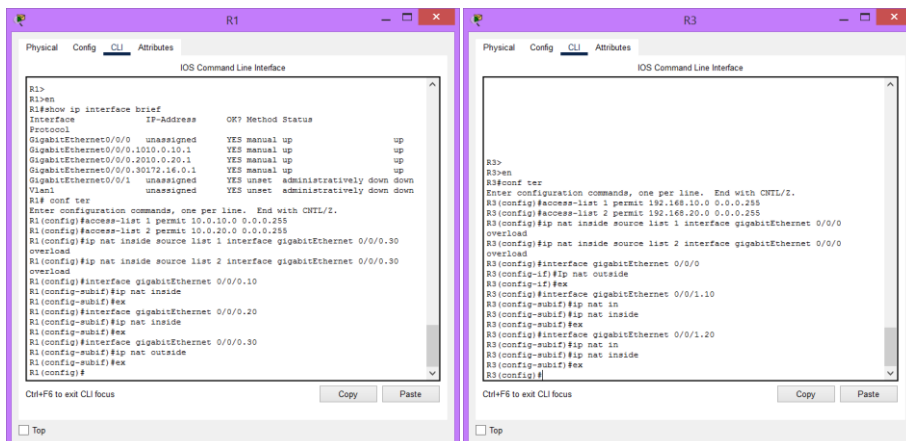
Настроим NAT

«R1» (для «PC0» и «PC1»):

R1#	configure terminal	Переход в режим конфигурирования терминала
R1 (config)#	access-list 1 permit 10.0.10.0 0.0.0.255	создаем список доступа, указывая, какие адреса могут использовать NAT
R1 (config)#	access-list 2 permit 10.0.20.0 0.0.0.255	создаем список доступа, указывая, какие адреса могут использовать NAT
R1 (config)#	ip nat inside source list 1 interface gigabitEthernet 0/0/0.30 overload	Укажем, что пакеты клиентов с IP-адресов из списка 1 будут подвергаться перегруженной NAT-трансляции при следовании через саб-интерфейс 0/0/0.30
R1 (config)#	ip nat inside source list 2 interface gigabitEthernet 0/0/0.30 overload	Укажем, что пакеты клиентов с IP-адресов из списка 1 будут подвергаться перегруженной NAT-трансляции при следовании через саб-интерфейс 0/0/0.30
R1 (config)#	interface gigabitEthernet 0/0/0.10	Редактировать интерфейс
R1 (config-router)#	ip nat inside	Укажем, что это внутренний сетевой интерфейс для NAT
R1 (config-router)#	Exit	
R1 (config)#	interface gigabitEthernet 0/0/0.20	Редактировать интерфейс
R1 (config-router)#	ip nat inside	Укажем, что это внутренний сетевой интерфейс для NAT
R1 (config-router)#	Exit	
R1 (config)#	interface gigabitEthernet 0/0/0.30	Редактировать интерфейс «fastEthernet 1/0»
R1 (config-router)#	ip nat outside	Укажем, что 0/0/1 – внешний сетевой интерфейс для NAT

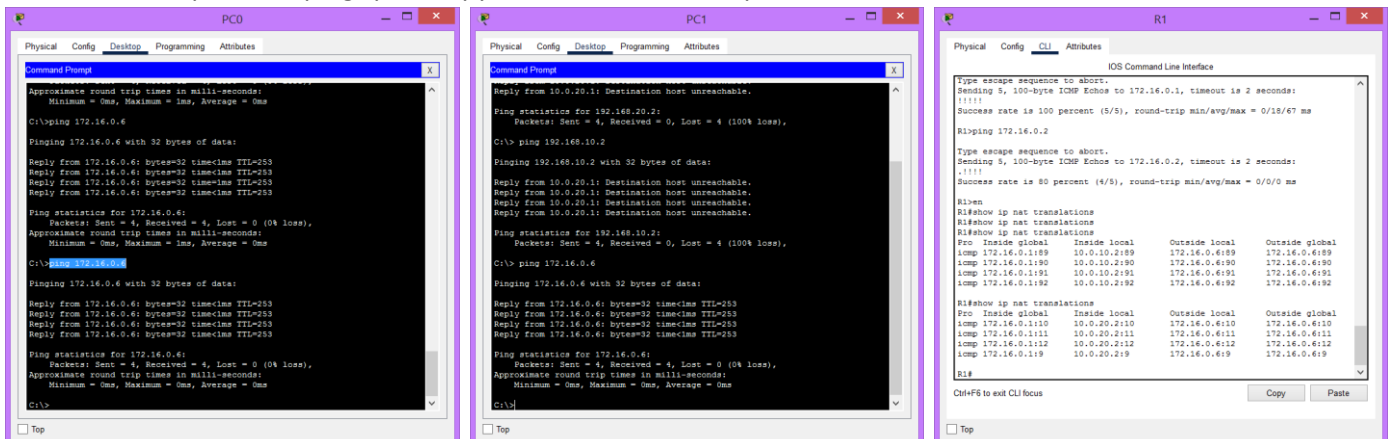
«R3» (для «WEB-server» и «DHCP»):

R3#	configure terminal	Переход в режим конфигурирования терминала
R3 (config)#	access-list 1 permit 192.168.10.0 0.0.0.255	создаем список доступа, указывая, какие адреса могут использовать NAT
R3 (config)#	access-list 2 permit 192.168.20.0 0.0.0.255	создаем список доступа, указывая, какие адреса могут использовать NAT
R3 (config)#	ip nat inside source list 1 interface gigabitEthernet 0/0/0 overload	Укажем, что пакеты клиентов с IP-адресов из списка 1 будут подвергаться перегруженной NAT-трансляции при следовании через интерфейс
R3 (config)#	ip nat inside source list 2 interface gigabitEthernet 0/0/0 overload	Укажем, что пакеты клиентов с IP-адресов из списка 2 будут подвергаться перегруженной NAT-трансляции при следовании через интерфейс
R3 (config)#	interface gigabitEthernet 0/0/0	Редактировать интерфейс
R3 (config-router)#	Ip nat outside	Укажем внешний сетевой интерфейс для NAT
R3 (config-router)#	exit	
R3 (config)#	interface gigabitEthernet 0/0/1.10	Редактировать интерфейс
R3 (config-router)#	Ip nat inside	Укажем внутренний сетевой интерфейс для NAT
R3 (config-router)#	Exit	
R3 (config)#	interface gigabitEthernet 0/0/1.20	Редактировать интерфейс
R3 (config-router)#	Ip nat inside	Укажем внутренний сетевой интерфейс для NAT
R3 (config-router)#	exit	



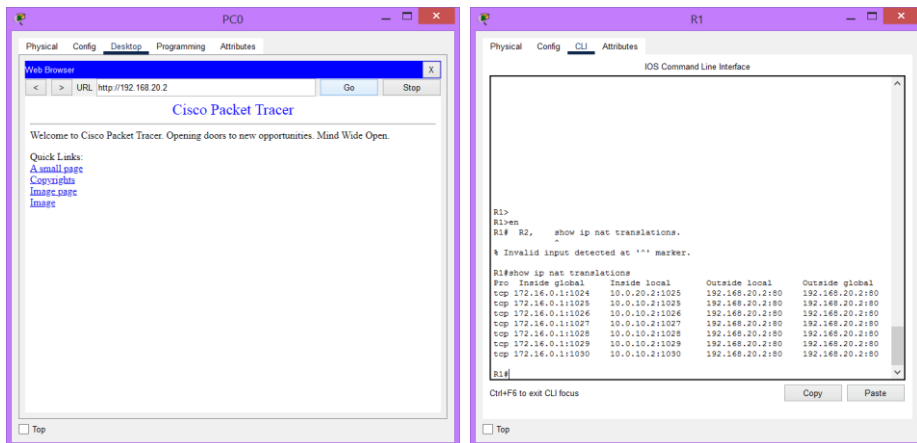
Проверим ping с «PC0» на роутер «R3», находящийся в Internet – все Ok

На «R1» посмотрим, как ping транслируются пакеты «show ip nat translations»



Проверим на «PC0» и «PC1» доступ WEB-server по адресу «192.168.20.2» - все отлично!

Посмотрим на «R1», как транслируются маршруты.

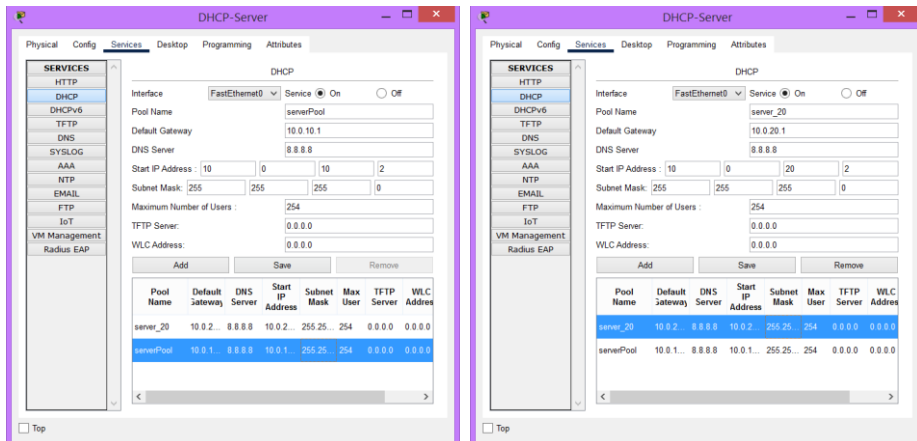


Настройка динамической выдачи адресов

«R1»:

R1#	configure terminal	Переход в режим конфигурирования терминала
R1 (config)#	interface gigabitEthernet 0/0/0.10	Редактируем интерфейс
R1 (config-if)#	ip helper-address 192.168.10.2	Укажем адрес источника выдающего адреса
R3 (config-if)#	exit	
R1 (config)#	interface gigabitEthernet 0/0/0.20	Редактируем интерфейс
R1 (config-if)#	ip helper-address 192.168.10.2	Укажем адрес источника выдающего адреса

DHCP-server настроим через графический интерфейс.



В ПК установим режим получения адресов по DHSP – получение Default Gateway и IP происходит корректно!!!

