Лабораторно упражнение 5.2
NAT

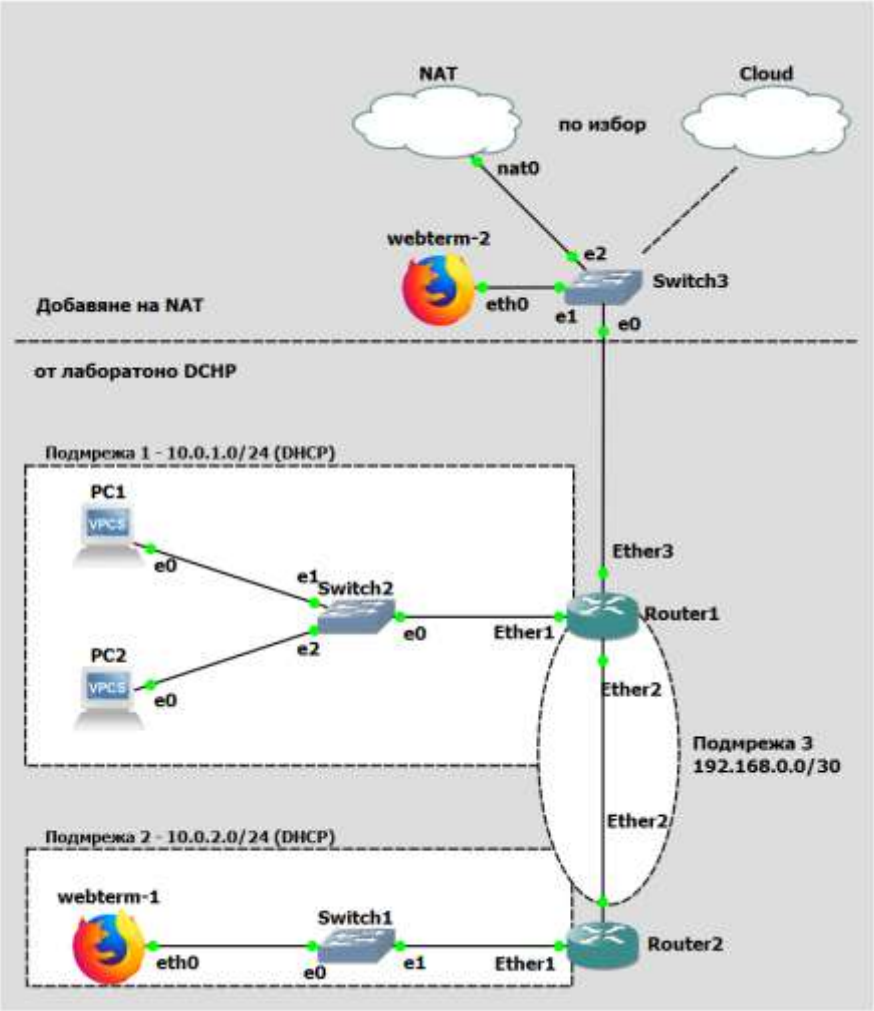
Обзор

В тази лабораторна работа ще конфигурирате виртуална GNS3 топология с интернет и ще конфигурирате преобразуване на мрежови адреси (NAT) на рутера.

При използването на логически адреси `.YY` заместваме с последните 2 цифри от факултетния номер.

Създаване на мрежата

В GNS3 създайте мрежова топология, която съответства на тази:



Мрежова диаграма 1 Лабораторно 5.2 (Забележка: Етикетите на подмрежата и пунктираните граници са само за информация)

Съвети:

- Процесът върви по-гладко, ако първо конфигурирате рутерите, а след това и компютрите във всяка подмрежа.
- Конкретният порт на комутатор няма значение
- Конкретният порт на рутера има значение. Конфигурацията на рутера в софтуера трябва да е в съответствие с начина, по който кабелите са свързани в хардуера.

Стъпки за конфигуриране:

1. Конфигурирайте имената на рутерите в GNS3, за да предотвратите объркване (чрез GUI).
2. Конфигурирайте имената на самия рутер, за да предотвратите объркване (чрез CLI).
3. Конфигурирайте IP адреси на всички интерфейси на рутера, които са свързани към подмрежи.
4. Деактивирайте DHCP клиента на всеки рутер. `ip dhcp-client print`, последван от `ip dhcp-client remove numbers=0`, ще премахне това.
5. Конфигурирайте динамично маршрутизиране (RIP) между подмрежи 1, 2 и 3. След конфигуриране проверете с отпечатване на маршрута за извличане на маршрут, че таблицата с маршрути е такава, каквато желаете.
    1) `routing rip interface add interface=etherX send=v2 receive=v2` # За интерфейса, който отива към други рутери
    2) `routing rip interface add interface=etherY passive=yes` # За интерфейса, който отива към клиентите
6. Конфигурирайте DHCP сървъра и на двата рутера, за да предостави адреси на пряко свързаната им подмрежа. Конфигурирайте и DNS, като използвате публичните DNS IP адреси на Google. `ip dns set servers=8.8.8.8,8.8.4.4`, последвано от `ip dns print`, за да потвърдите вашата настройка
7. Активирайте DHCP клиента на VPC и клиента Webterm.
8. Запазете конфигурацията на VPC чрез командата save и излезте от безопасен режим на рутера.

Свързване на GNS3 към интернет

Мрежовият симулатор на GNS3 предоставя два различни възела, които позволяват достъп до физическата мрежа - Cloud node и NAT node.

- **Cloud node** свързва вашата GNS3 топология с вашата физическа мрежа, сякаш основната операционна система, и вашата GNS3 мрежа са свързани към един и същ физически комутатор. Това е полезно, когато искате да разрешите външен достъп до вашата GNS3 мрежа без никаква намеса. За да настроите „облачния възел“, трябва да изберете конкретния физически мрежов интерфейс, с който искате да се свържете. Мрежовото свързване е най-успешно с кабелни мрежови адаптери (например Ethernet) и по-малко успешно с безжични мрежови адаптери. Една от причините е, че точката за достъп до безжичната мрежа проследява удостоверяването по MAC адрес и без някаква „софтуерна хитрост“, втория MAC адрес, който се появява в безжичната мрежа, няма да бъде удостоверен. По този начин ще „се свържете“, но всичко, което изпратите, ще бъде игнорирано.
- **NAT node** също така позволява на вашата GNS3 топология да има достъп до физическата мрежа, но чрез транслация на адреси, така че GNS3 заявките изглежда идват от вашата хост ОС. Това е подходящо за изтегляне на файлове от Интернет (като софтуерни актуализации за виртуални машини),

но не и за разрешаване на външен достъп до вашата GNS3 мрежа. Обаче е по-надежден за използване в голямо разнообразие от системни конфигурации.

Изберете типа възел, който е най-вероятно да работи във вашата система.. Можете да опитате първо да настойте Cloud Node и да се върнете към NAT, ако е необходимо. Плъзнете този “възел” във вашата мрежова диаграма. **Забележка**: За разлика от всяко друго устройство, използвано в лабораторните, тук НЕ е препоръчително да стартирате своя Cloud или NAT възел във VM GNS3, което след това ще изисква от вас да отстранявате и проблеми с мрежата на виртуалната машина. Вместо това изберете Cloud или NAT възелът да работи на вашия хост компютър. **НО** в случай че използвате WI-Fi като активна връзка на вашия компютър може да възникнат проблеми и да не работи NAT Node, затова пробвайте и с VM GNS.

Стартирайте DHCP на интерфейса на `Router1`, свързан към възела Cloud/NAT, така че вашият рутер да може да поиска IP от тази мрежа. Първо добавете услугата DHCP-клиент с `ip dhcp-client add interface=ether3 disabled=no`. След това проверете дали работи с `ip dhcp-client print` и накрая проверете дали адресът на интерфейса е зададен с `ip address print`

Проверете таблицата за маршрутизиране за `Router1` с `ip route print`. Какво прави рутерът с пакет, който не съответства на нито едно съществуващо правило? (Потърсете маршрут по подразбиране, `0.0.0.0/0`). `Router1` ще го препрати към `ether3` към възела Cloud/NAT.

След това проверете таблицата за маршрутизиране за `Router2`. Какво прави рутерът с пакет, който не съответства на съществуващо правило? (Потърсете маршрут по подразбиране, 0.0.0.0/0). Нищо! Все още няма маршрут по подразбиране.

Конфигурирайте RIP на `Router1`, за да разпространявате информация за маршрута по подразбиране `(0.0.0.0/0)` до други рутери. Това не е активирано по подразбиране, но може да се активира с `routing rip set distribute-default=if-installed`. Това правило е необходимо само на Router1, който има маршрут по подразбиране, зададен чрез DHCP клиента, който преди това сте конфигурирали на порта, свързан към Cloud/NAT.

Изисква се една последна стъпка. Имате определен брой подмрежи във вашата GNS3 мрежа, които всички искат достъп до Интернет. Въпреки това, NAT възелът в софтуера ще картографира само една подмрежа към хост мрежата. Облачният възел има подобно ограничение, макар и такова, което е наложено от вашата физическа мрежа и физически рутер. Освен да промените вашата физическа мрежа да говори RIP с `Router1`, най-лесният начин да се справите с това е да стартирате транслиране на адреси и на `Router1`, така че целият изходящ трафик (от много устройства) изглежда идва само от Router1. Тази функция - IP "Masquerading", е стандартна функция на Linux и е налична и в защитната стена на MikroTik IP. Активирайте го чрез: `ip firewall nat add chain=srcnat action=masquerade out-interface=ether3`. (out-interface е интерфейсът, свързан към облака).

Тестване на мрежата

Трябва да можете да осъществите ping до google.com отвсякъде. Опитайте го от webterm-1, Router1, Router2 и PC1.