Лабораторно упражнение 7

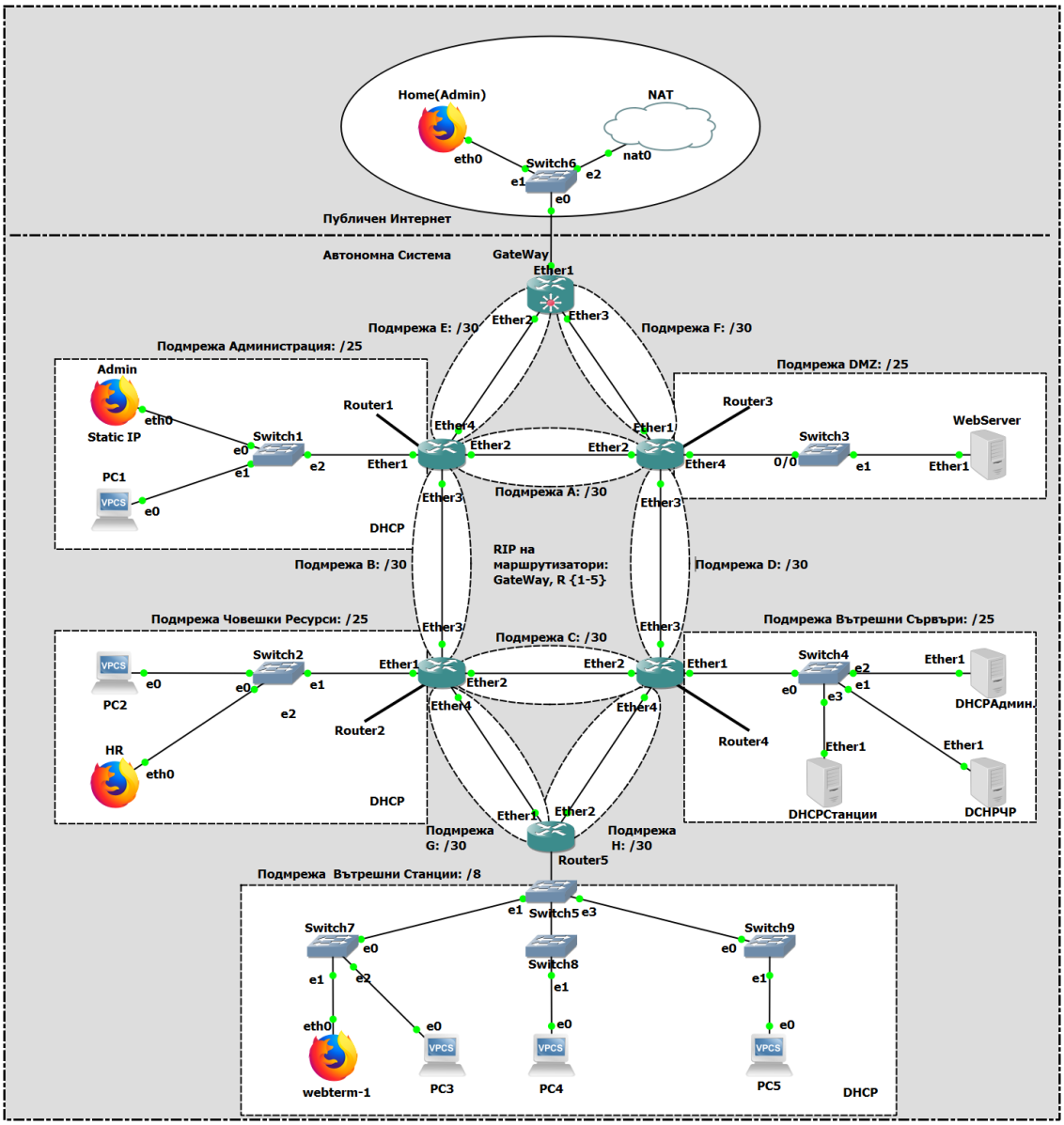
Обзор

В тази лабораторна работа ще конфигурирате виртуална GNS3 топология и ще приложим всичко изучено до момента.

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 7 (Забележка: Етикетите на подмрежата и пунктираните граници са само за информация)

Тук се създават няколко подмрежи:

„**Публичен интернет**“ – Подмрежа, представляваща устройства, които са външни за вашата AS (организация)

"**DMZ**" (демилитаризирана зона) - Подмрежа, съдържаща сървъри, които трябва да бъдат публично достъпни, както и за устройствата от AS

„**Вътрешни сървъри**“ – Подмрежа, съдържаща сървъри, които трябва да бъдат достъпни само от вътрешни устройства

„**Вътрешни работни станции**“ – Подмрежа, съдържаща компютри на крайни потребители (лаптопи, работни станции и т.н.), които трябва да бъдат достъпни само от вътрешни устройства и нямат достъп до „Администрация“ и „Човешки ресурси“

„**Администрация**“ – Подмрежа, съдържаща компютри на крайни потребители (лаптопи, работни станции и т.н.), които имат достъп до всичко (AS и „Публичен интернет“)

„**Човешки ресурси**“ – Подмрежа, съдържаща компютри на крайни потребители (лаптопи, работни станции и т.н.), които трябва да бъдат достъпни само от „Администрация“ и могат да достъпват „Работните станции“, „Вътрешни сървъри“ и „Публичен Интернет“

Изключение:

“**Home (Admin)**”- има изключителни права да достига „Admin“ от AS(освен нормалния достъп до “DMZ”).

Обърнете внимание, че „сървърите“, показани на мрежовата диаграма, са просто MikroTik рутери, които са преназначени за нова роля. GNS3 е в състояние да поддържа пълноправни виртуални машини, използвани за сървър, като част от симулираната мрежа. Тук напълно достатъчно ни е Mikrotik OS за всички нужди.

Свободни сте да избирате адреси на подмрежите, както сметнете за добре, със следните ограничения:

1. Всички подмрежи трябва да са в диапазони на частни IP адреси - Много лоша практика е да се припокриват с легитимни публични IP адреси
2. Подмрежа Администрация трябва да е /25 мрежа - тя е сравнително малка
3. Подмрежа Човешки Ресурси трябва да е /25 мрежа - тя е сравнително малка
4. Подмрежа DMZ трябва да е /25 мрежа - тя е малка
5. Подмрежа Вътрешни Сървъри трябва да е /25 мрежа - тя е сравнително малка
6. Подмрежа Работни станции трябва да е /8 - тя е много голяма (изберете подходяща частна мрежа!!!)
7. Подмрежи A-H трябва да са /30 мрежа – те са малки и свързват само двата рутера заедно
8. Устройство **Admin** трябва да има статичен адрес a.b.c.YY/25, където a,b,c за избраните за мрежа Администрация
9. Добра практика е да се изберат IP адресите на шлюза по подразбиране да бъдат или първият използваем хост адрес, или последният използваем хост адрес в подмрежата. (С изключение на подмрежа A-H, където всеки хост е рутер)

Преди да започнете попълнете таблиците. Това ни дава увереност, че няма да има грешки и конфликти в IP адресите. Чак след това пристъпете към изпълнението в GNS3 симулатора.

Подмрежи:

Подмрежа	Адрес на мрежа	Маска	Бр. IP адреси	Бр. изп. IP	Първия използваем IP адрес	Последния използваем IP адрес
A						
B						
C						
D						
E						
F						
G						
H						
Админ.						
Човешки Ресурси						
DHCP						
DMZ						
Работни Станции						

IP адреси на интерфейсите

Хост	Интерфейс	IP адрес	Адрес на мрежа
Gateway	Ether1	DHCP	
	Ether2		
	Ether3		
Router1	Ether1		
	Ether2		
	Ether3		
	Ether4		
Router2	Ether1		
	Ether2		
	Ether3		
	Ether4		
Router3	Ether1		
	Ether2		
	Ether3		
	Ether4		
Router4	Ether1		
	Ether2		
	Ether3		
	Ether4		
Router5	Ether1		
	Ether2		
	Ether3		
	Ether4		
WebServer	Ether1		
DHCP Админ.	Ether1		
DHCP ЧР	Ether1		

DHCP Станции	Ether1		
HR	Eth0	DHCP	
Webtern-1	Eth0	DHCP	
Admin	Eth0		
PC1	E0	DHCP	
PC2	E0	DHCP	
PC3	E0	DHCP	
PC4	E0	DHCP	
PC4	E0	DHCP	

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 A-H. След конфигуриране проверете с `routing rip route print`, че таблицата с маршрути е такава, каквато желаете.
6. Конфигурирайте статичен IP адрес на `Admin` и вътрешните сървъри
7. Конфигурирайте DHCP сървърите и нужните Relays
8. Активирайте DHCP клиента на `Home(Admin)`, `GateWay`(Ether1), всички вътрешни устройства.

Тестване на мрежата преди FireWall

За тестване:

1. Уверете се, че устройствата са получили IP адрес чрез DHCP. (Изпълнете `ip dhcp-server lease print` на `DHCPServer`)
2. Уверете се, че всеки може успешно да осъществява ping до всеки.
3. Уверете се, че `Admin` може да зареди уеб страницата на уеб сървъра
4. Уверете се, че `Admin` може да зареди публична уеб страница

FireWall

Изберете внимателно на кои рутер да конфигурирате нужните правила, за да може да осъществите зададените условия за достъп до различните мрежи и устройства.

Тестване на мрежата след FireWall

За тестване:

1. Уверете се, че устройствата са получили IP адрес чрез DHCP. (Изпълнете `ip dhcp-server lease print` на `DHCPServer`)
2. Уверете се, че Admin може успешно да осъществява ping до всеки.
3. Уверете се, че `Admin` може да зареди уеб страницата на уеб сървъра
4. Уверете се, че `Admin` може да зареди публична уеб страница
5. Уверете се, че `Home(Admin)` може да зареди публична уеб страница
6. Уверете се, че `Home(Admin)` може да осъществи ping до `Admin`, но не и до друг в AS
7. Уверете се, че са изпълнени останалите зададени ограничения за достъп в AS

Проверете с помощта на Wireshark какви пакети се получават и изпращат в мрежата. Започнете да изключвате различни връзки между устройствата и наблюдавайте как се отразява това на мрежата.