МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**NAT**

Отчет по лабораторной работе № 7

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-231(2)  
Аметов Кемран Ленверович

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2024

Теория

**NAT (Network Address Translation)** — это технология, используемая для преобразования IP-адресов в заголовках сетевых пакетов при их прохождении через маршрутизатор или другой сетевой узел.

### Основные цели NAT:

1. **Экономия публичных IP-адресов**: NAT позволяет использовать один или несколько публичных IP-адресов для множества устройств с частными IP-адресами в локальной сети.
2. **Безопасность**: Скрывает внутреннюю структуру сети от внешнего мира, так как устройства с частными адресами не доступны напрямую из Интернета.
3. **Упрощение управления сетью**: Устройства в локальной сети могут использовать внутренние адреса, которые легко администрировать и менять.

### Типы NAT:

**Static NAT (статический NAT)**:

* 1. Каждому частному IP-адресу сопоставляется конкретный публичный IP-адрес.
  2. Используется, когда внутренние устройства должны быть доступны извне.

**Dynamic NAT (динамический NAT)**:

* 1. Частным адресам выделяются публичные адреса из заранее настроенного пула.
  2. При этом может быть доступно меньше публичных адресов, чем частных.

**PAT (Port Address Translation), или NAT Overload**:

* 1. Наиболее популярный вид NAT.
  2. Использует один публичный IP-адрес (или небольшой пул) для множества устройств, различая их по номерам портов.
  3. Например, запросы от разных устройств проходят через один IP, но с разными номерами портов.

### Как работает NAT:

**Исходящий трафик**:

* 1. Когда устройство с частным IP-адресом отправляет пакет через NAT-устройство, его адрес заменяется на публичный IP-адрес.
  2. Устройство запоминает соответствие между внутренним адресом и портом, чтобы направить ответный трафик.

**Входящий трафик**:

Пакеты, приходящие на публичный IP-адрес, NAT преобразует обратно, перенаправляя их на соответствующий частный адрес в локальной сети.

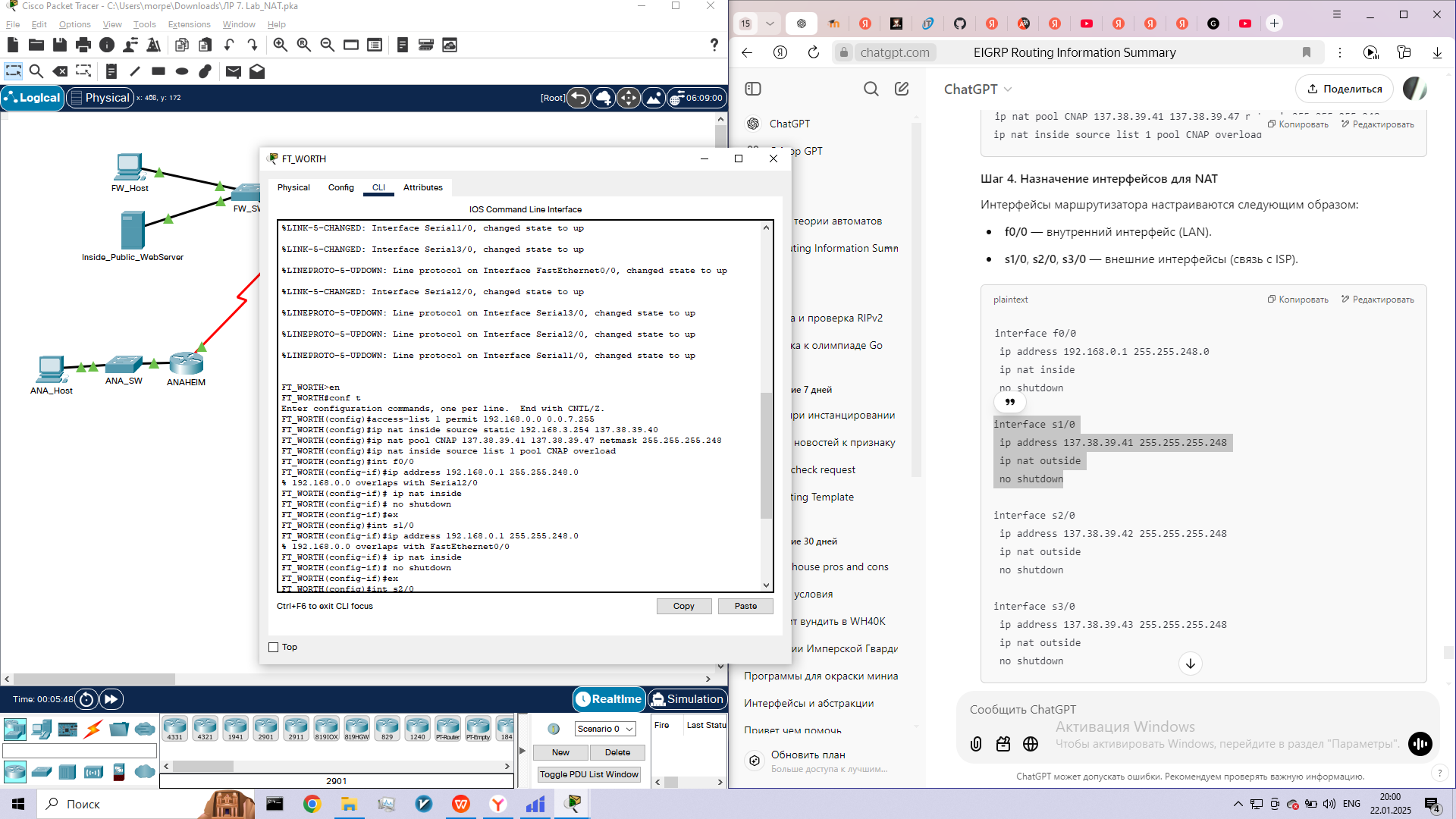
### Преимущества:

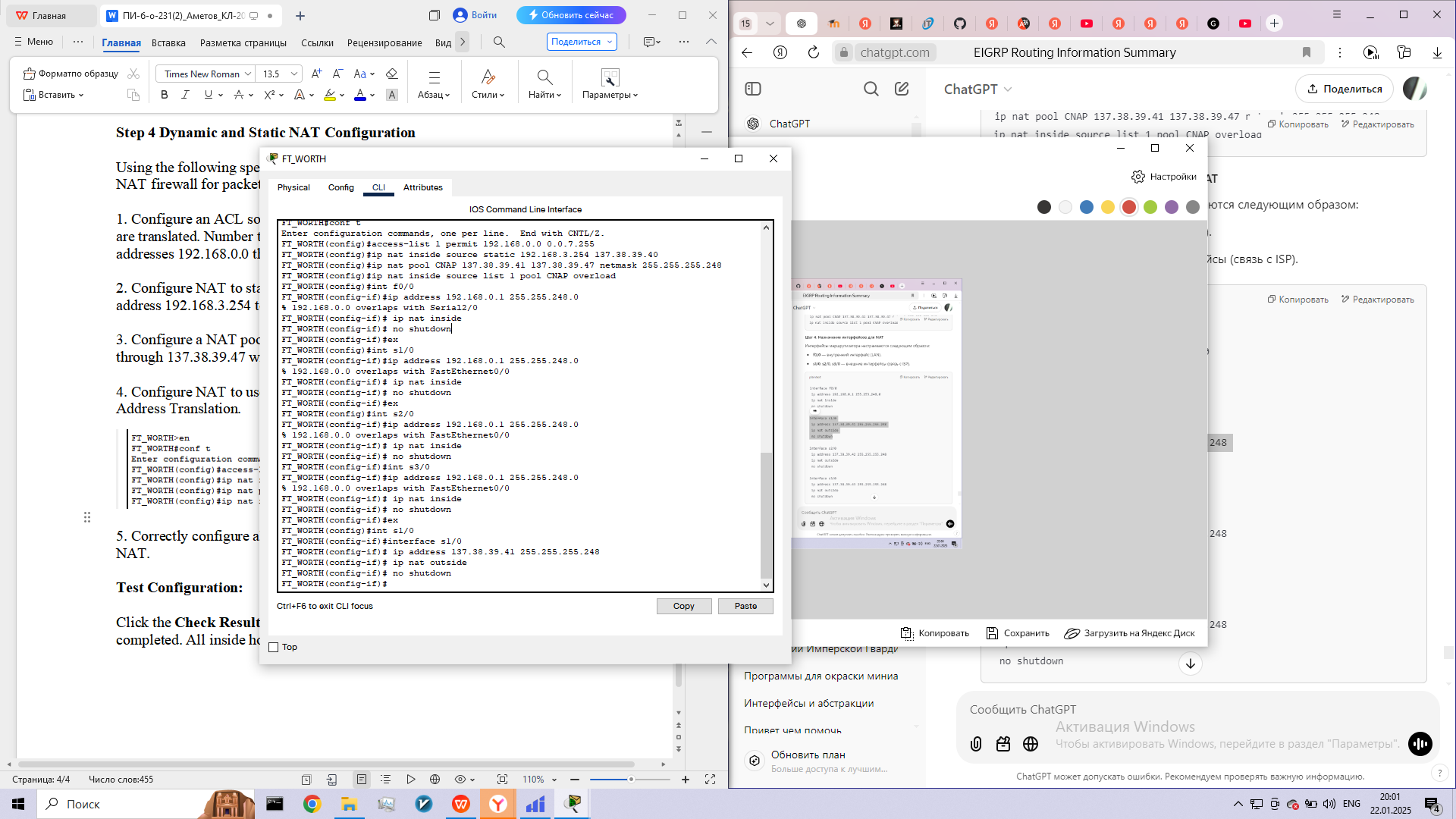
* Сокращение использования публичных IP-адресов.
* Повышение безопасности (внутренняя сеть скрыта).
* Упрощение подключения нескольких устройств в локальной сети к Интернету.

### Недостатки:

* Некоторые протоколы (например, SIP или FTP) могут работать хуже из-за модификации пакетов.
* Требуется дополнительная обработка пакетов, что может слегка увеличивать задержки.

**Step 4 Dynamic and Static NAT Configuration**  
  
Using the following specifications, configure the **FT\_WORTH** router as a NAT firewall for packets routed to and from **ISP**.  
  
1. Configure an ACL so that addresses in the 192.168.0.0/21 address space are translated. Number the ACL 1. The wildcard mask should cover addresses 192.168.0.0 through 192.168.7.255.  
  
2. Configure NAT to statically map the **Inside\_Public\_Webserver** IP address 192.168.3.254 to the public IP address 137.38.39.40.  
  
3. Configure a NAT pool named **CNAP** for the address range 137.38.39.41 through 137.38.39.47 with /29 mask.  
  
4. Configure NAT to use ACL 1 with the **CNAP** pool. Also, configure Port Address Translation.



5. Correctly configure all of the interfaces on **FT\_WORTH** to participate in NAT.  
  
**Test Configuration:**  
  
Click the **Check Results** icon to verify all assessed items are successfully completed. All inside hosts should now be able to ping **Internet\_Host**.

