УДК 621.391

МЕТОДЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ В МЕЖСЕТЕВЫХ ЭКРАНАХ

М.Н. БОБОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 13 октября 2009

Технология трансляция сетевых адресов (Network Address Translation (NAT)) осуществляется на межсетевом экране, стоящем на границе между внутренней сетью, и внешней сетью. Перед посылкой пакетов во внешнюю сеть, NAT транслирует внутренние локальные адреса в глобальные уникальные IP-адреса и наоборот. Эта технология осуществляется для скрытия внутренних адресов своей сети, чтобы не дать злоумышленнику возможности получить информацию о структуре и масштабах сети, а также о структуре и интенсивности исходящего и входящего трафиков.

Ключевые слова: межсетевой экран (МСЭ), локальный и глобальные адреса, внутренние и внешне адреса, таблица NAT.

Введение

МСЭ осуществляющий трансляцию адресов, должен иметь, по меньшей мере, один внутренний и один внешний интерфейс [1]. В обычных условиях NAT конфигурируется на МСЭ, являющемся для данной локальной сети выходом в глобальную сеть. Когда пакет покидает внутреннюю сеть, NAT транслирует локальный адрес источника в глобальный уникальный адрес. Когда пакет входит в локальную сеть, NAT транслирует глобальный адрес назначения в локальный адрес. Если существует более одной выходной точки в глобальную сеть, то все устройства, работающие с NAT, должны иметь идентичные таблицы трансляции. Если программное обеспечение не может транслировать адрес, оно блокирует пакет и посылает сообщение источнику протоколом ICMP “хост не доступен” [2].

МСЭ, на котором NAT сконфигурирован, не должен передавать наружу информацию о внутренней сети. Тем не менее, данные о маршрутизации, получаемые извне (из внешней сети), могут передаваться в локальную сеть.

Трансляция внутреннего адреса источника

Используется для преобразования внутренних адресов в глобальные адреса при связи с внешними сетями. Включает в себя статическую или динамическую трансляцию:

- *Статическая трансляция* устанавливает взаимно-однозначное соответствие между внутренними локальными адресами и внутренними глобальными адресами. Статическая трансляция полезна, когда внутренний хост должен быть доступен извне по фиксированному адресу.

- *Динамическая трансляция* устанавливает соответствие между внутренними локальными адресами и пулом глобальных адресов.

На рис. 1 показан МСЭ, транслирующий адрес источника при переходе пакета из внутренней сети во внешнюю сеть.

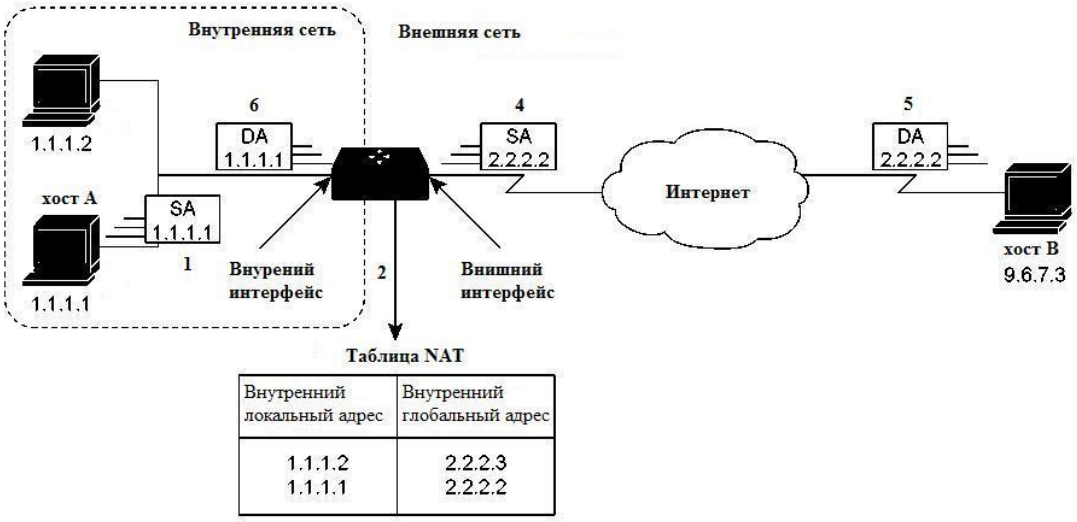

Рис. 1. Трансляция внутренних адресов: SA ≡ Адрес источника (Source Address);
DA ≡ Адрес назначения (Destination Address)

Статический метод трансляции.

В соответствии с рис. 1, трансляция внутренних адресов источника статическим методом включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает пакет от хоста 1.1.1.1, читает информацию из заголовка и сверяется со своей NAT-таблицей.
3. Если входа трансляции не существует в таблице, МСЭ блокирует пакет.
4. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
5. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).
6. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.
7. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятый.

Алгоритм этого механизма представлен на рис. 2.

Динамический метод трансляции.

Трансляция внутренних адресов источника динамическим методом включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется со своей NAT-таблицей.
3. Если вход трансляции не существует в таблице, МСЭ определяет, что адрес источника 1.1.1.1 должен транслироваться динамически, выбирает легальный глобальный адрес из пула динамических адресов и создает вход в таблице трансляции. Этот тип входа называется *простым входом*.
4. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
5. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).
6. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.
7. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

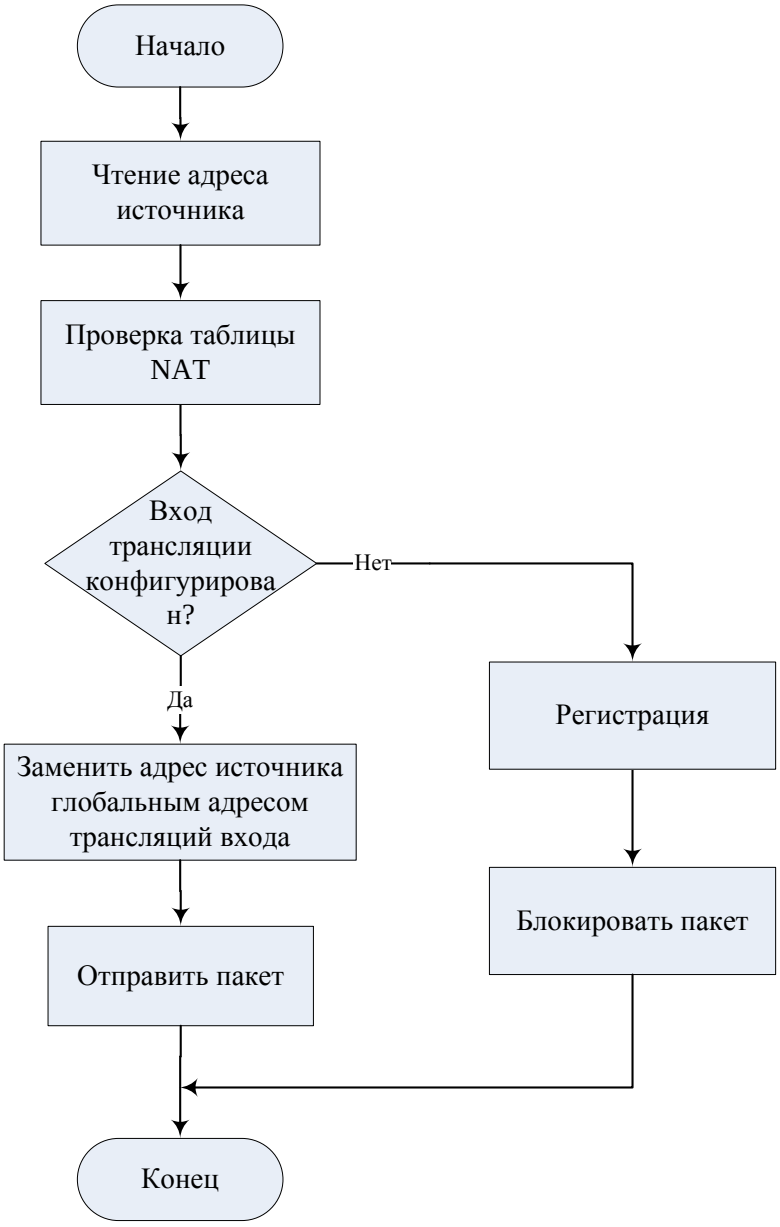

Рис. 2. Алгоритм трансляции внутреннего адреса источника статическим методом

Смешанный метод трансляции.

Трансляция внутренних адресов источника смешанным методом, включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется со своей NAT-таблицей.

a. Если статический вход трансляции был сконфигурирован, МСЭ следует на шаг 3.

b. Если вход трансляции не существует в таблице, МСЭ определяет, что адрес источника 1.1.1.1 должен транслироваться динамическим методом, выбирает легальный глобальный адрес из пула динамических адресов и создает вход в таблице трансляции. Этот тип входа называется *простым входом*.

3. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
4. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).

5. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.

6. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

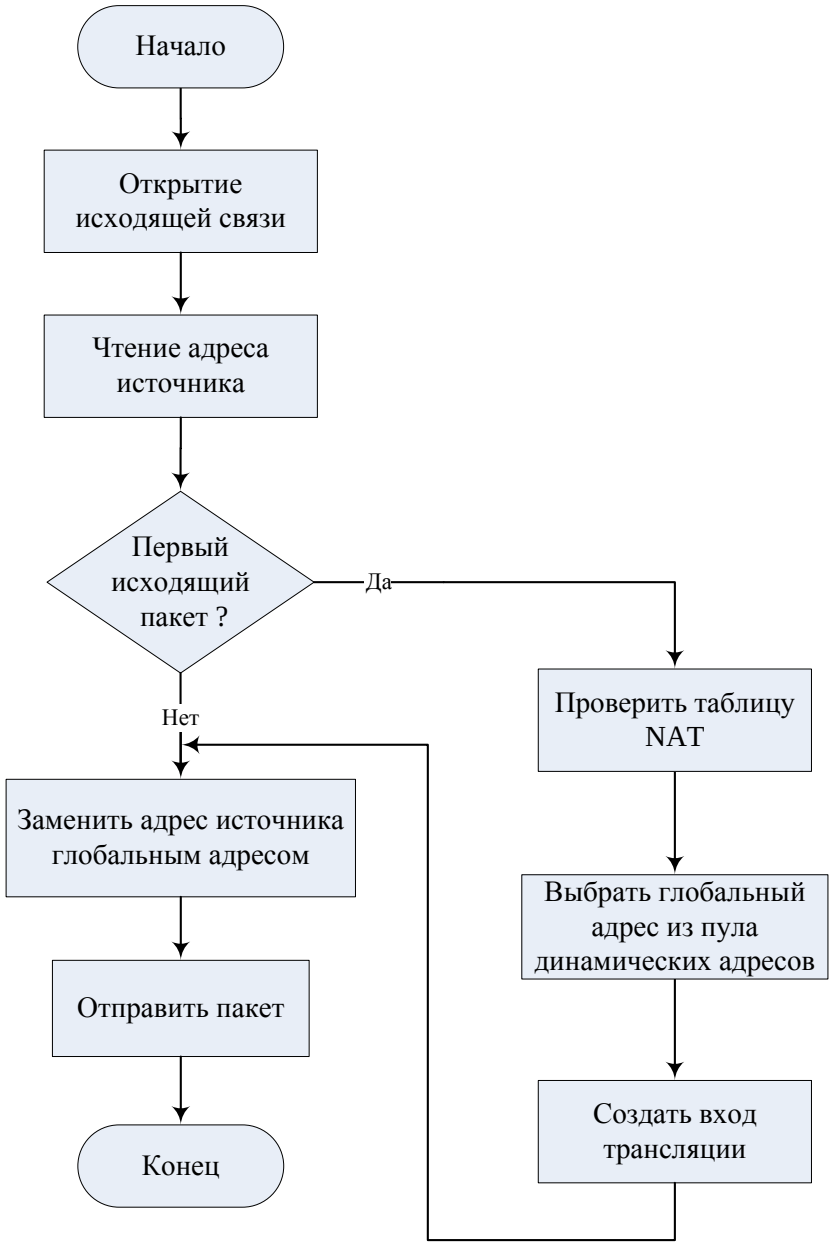

Рис. 3. Алгоритм трансляции внутреннего адреса источника динамическим методом

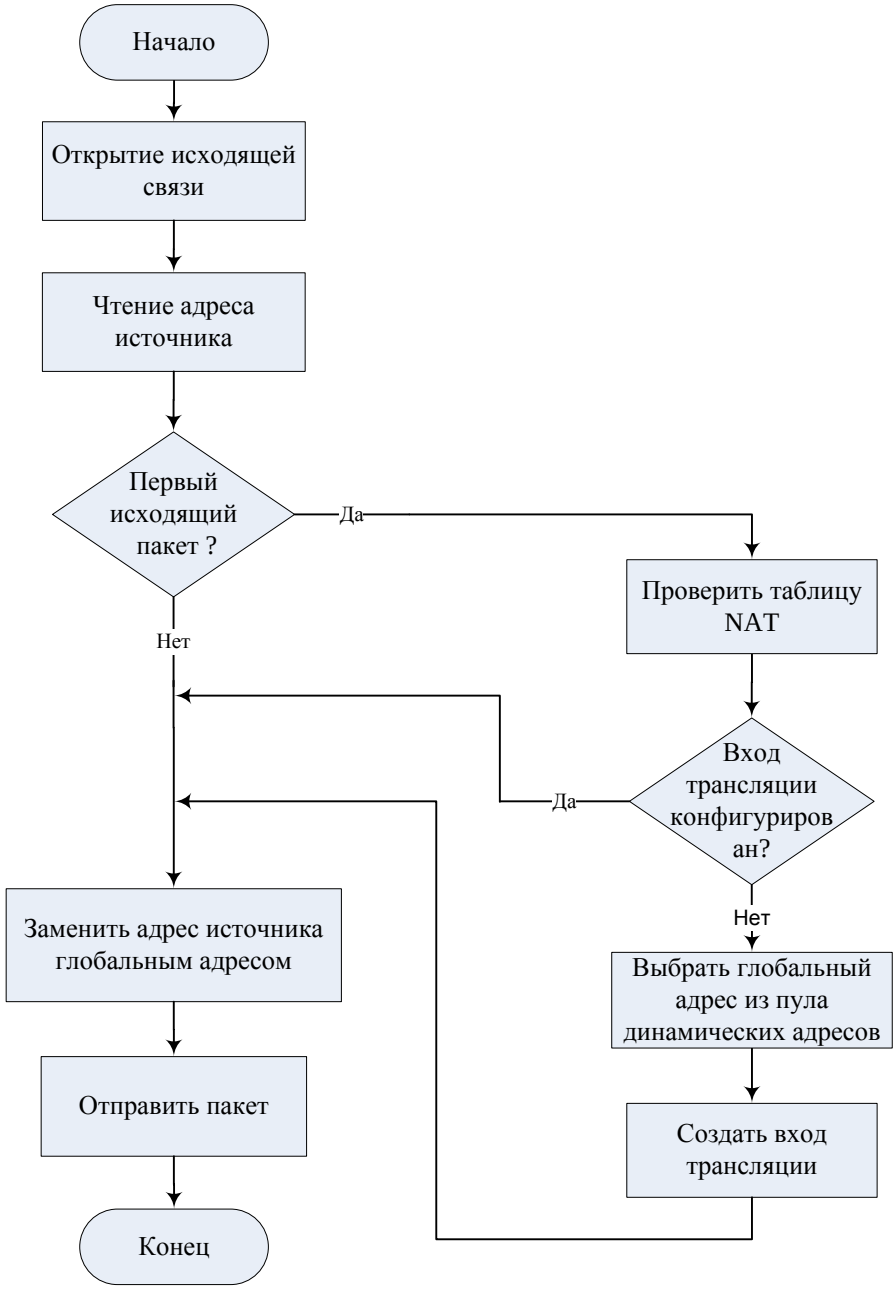

Рис. 4. Алгоритм трансляции внутреннего адреса источника смешанным методом

Совмещение внутренних глобальных адресов

Данный режим трансляции (режим совмещения) позволяет сэкономить адреса в пуле внутренних глобальных адресов путем настройки МСЭ на использование одного глобального адреса для нескольких локальных адресов. Когда такой режим сконфигурирован, МСЭ имеет достаточно информации от протоколов верхних уровней (например, номера портов TCP или UDP) для трансляции глобального адреса обратно в нужный локальный адрес. Когда нескольким локальным адресам ставится в соответствие один глобальный адрес, номера портов TCP или UDP каждого внутреннего хоста позволяют различать их локальные адреса [3].

Рис. 5 иллюстрирует механизм трансляции адресов, когда один внутренний глобальный адрес представляет несколько внутренних локальных адресов. Номер порта TCP играет роль отличительного признака.

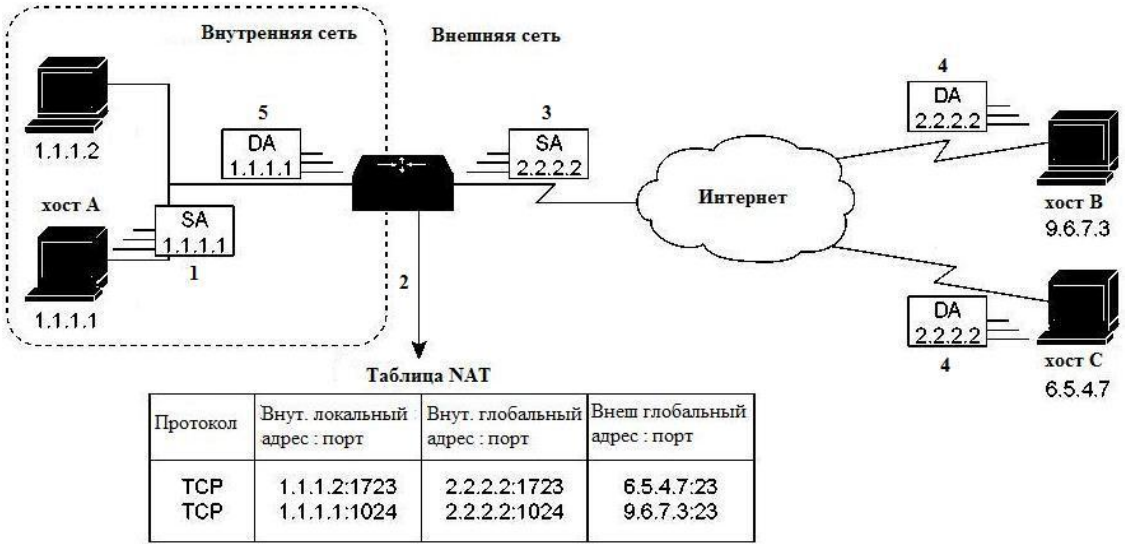

Таблица NAT

Протокол	Внут. локальный адрес : порт	Внут. глобальный адрес : порт	Внеш глобальный адрес : порт
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

Рис. 5. Перегрузка глобальных адресов в NAT

В данном режиме трансляции внутренних глобальных адресов, как показано на рис. 5, хост B и хост C представляют, что они взаимодействует с одном хостом по адресу 2.2.2.2. Реально, они сообщаются с разными хостами в виду отличия номеров портов. МСЭ реализует этот механизм следующими шагами [4, 5]:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется своей NAT-таблицей.

a. Если вход трансляции в таблице не существует, МСЭ транслирует внутренний локальный адрес 1.1.1.1 в легальный глобальный адрес. Если совмещение адресов разрешено и другая трансляция является активной, то МСЭ использует тот же глобальный адрес для создания входа и сохраняет информацию, необходимую для обратной трансляции. Этот тип входа называется *расширенным входом.*

3. МСЭ заменяет локальный адрес источника 1.1.1.1 на выбранный глобальный адрес и отправляет пакет.
4. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес 2.2.2.2.
5. Когда МСЭ получает пакет с глобальным адресом, он проверяет NAT-таблицу, используя в качестве ключа тип протокола, внутренний глобальный адрес и номер порта, транслирует адрес во внутренний локальный адрес 1.1.1.1 и направляет пакет хосту 1.1.1.1.
6. Хост 1.1.1.1 получает пакет и продолжает сетевой обмен. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

Алгоритм этого механизма представлен на рис. 6.

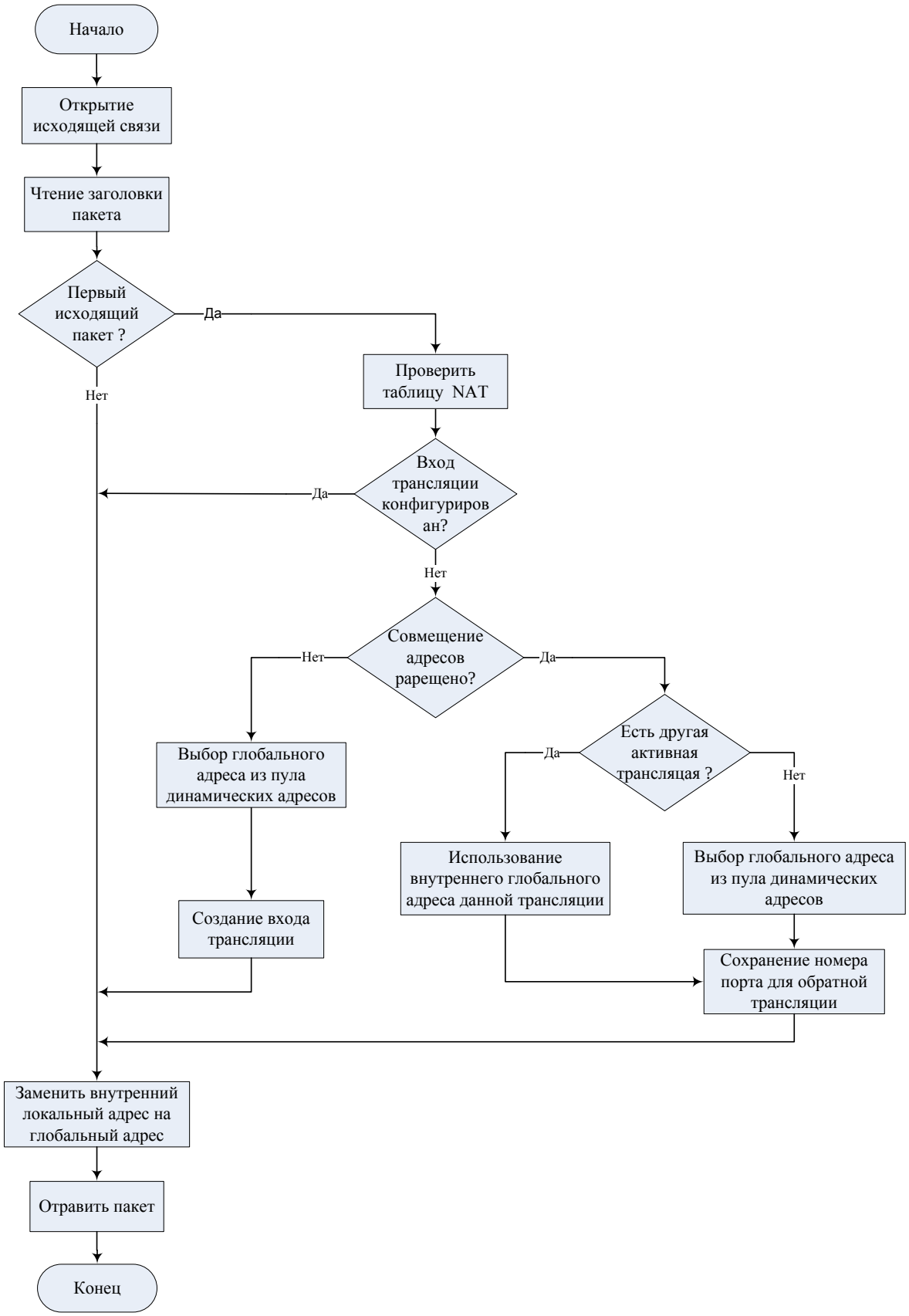

Рис. 6. Алгоритм совмещения внутренних глобальных адресов

Заключение

Технология трансляции сетевых адресов является одним из самых эффективных механизмов используемых для скрытия структуры и масштабов сети, а также структуры и интенсивности исходящего и входящего трафиков. Она является также частью последовательности операций, выполняемых МСЭ для обеспечения безопасности внутренней сети от всех типов атак.

METHODS OF USING NETWORK ADDRESS TRANSLATION (NAT) TECHNOLOGY IN FIREWALLS

M.N. BOBOF

Abstract

Network Address Translation applied to the firewall which positioning between the internal and external networks. When a packet is leaving the trusted (internal) network, NAT translates the local source address to a global unique address and vice versa. This technology applied to secure trusted network's internal addresses to prevent unauthorized user from gathering information about the structure of internal network and the intensity of the incoming and outgoing traffic.

Литература

1. *Олифер В.Г.*, *Олифер Н.А*. Компьютерные сети, принципы, технологии, протоколы // П., 2007.
2. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // Cisco press, Second Edition, 2008.
3. *Ray Blair, Arvind Durai*. Cisco Secure Firewall Services Module (FWSM) // Cisco press, Second Edition, 2009.
4. RFC 1631 – The IP Network Address Translator (NAT).
5. RFC 2663 – IP Network Address Translator (NAT) Terminology and Considerations.