Поддержка протокола NAT

Лаштанов И.Г.

Знакомство с NAT

NAT позволяет преобразовывать для входящего и исходящего трафика Интернета частные IP-адреса в открытые IP-адреса Интернета. Это предотвращает передачу трафика непосредственно во внутреннюю сеть, одновременно снижая затраты времени и средств пользователя на получение и поддержку диапазона открытых адресов.

Протокол Microsoft Windows 2000 NAT позволяет компьютерам небольшой сети совместно использовать одно соединение Интернетом, имеющее только один IP-адрес. Компьютер, на котором установлен протокол NAT, может работать в качестве транслятора сетевых адресов, упрошенного сервера DHCP, прокси-сервера DNS и прокси-сервера WINS. Протокол NAT позволяет компьютерам разделять один или несколько зарегистрированных открытых IP-адресов, увеличивая пространство доступных для выделения открытых адресов.

Основы NAT

Протокол NAT в Windows 2000 позволит вам настроить домашнюю сеть или сеть небольшого офиса для совместного использования одного подключения к Интернету. Ниже перечислены составляющие NAT.

- **Компонент трансляции.** Маршрутизатор Windows 2000 с поддержкой NAT (далее — NAT-компьютер) выступает в качестве преобразователя сетевых адресов, транслирующего IP-адреса и номера портов пакетов TCP/UDP, передаваемых между частной сетью и Интернетом.
- **Компонент адресации.** NAT-компьютер передает другим компьютерам домашней сети сведения о конфигурации IP-адреса. Компонент адресации — это упрошенный сервер DHCP, выделяющий IP-адрес, маску подсети, шлюз по умолчанию и IP-адрес DNS-сервера. Для автоматического получения конфигурационных сведений IP-адреса компьютеры домашней сети следует настроить в качестве клиентов DHCP. По умолчанию компьютеры с Windows XP, Windows 2000, Windows NT, Windows 95 и Windows 98 являются клиентами DHCP.
- **Компонент разрешения имен.** NAT-компьютер становится для остальных компьютеров домашней сети DNS-сервером. При получении запросов на разрешение имен NAT-компьютер передает их находящемуся в Интернете DNS-серверу, для работы с которым он сконфигурирован, и возвращает ответ компьютеру домашней сети.

Маршрутизируемые и транслируемые соединения с Интернетом

Существует два вида подключения к Интернету: маршрутизируемое и транслируемое. При планировании маршрутизируемого соединения вам надо получить у своего поставщика услуг Интернета диапазон IP-адресов, который будет использоваться во внутренней части нашей сети; кроме того, поставщик даст вам IP-адрес DNS-сервера, который вы и будете применять. Вы можете назначить компьютерам статические IP-адреса или воспользоваться DHCP-сервером.

Маршрутизатор Windows 2000 следует настроить на работу с сетевым адаптером внутренней сети. Кроме того, для маршрутизатора необходимо создать подключение к Интернету.

Транслируемый доступ (с использованием NAT) значительно безопаснее, поскольку адреса частной сети полностью скрываются от Интернета. NAT-компьютер, разделяемый соединением, преобразует все адреса Интернета в адреса частной сети и наоборот. Не забывайте, однако, что NAT-компьютер не способен транслировать всю полезную информацию. Это связано с тем, что некоторые приложения используют IP-адреса в других полях, помимо стандартных полей заголовка TCP/IP.

С NAT не работают следующие протоколы:

- Kerbcros;
- IP Security Protocol (IPSec).

Поддержка протоколом NAT выделения адресов DHCP-сервером позволяет всем DHCP-клиентам в сети автоматически получить от NAT-компьютера IP-адрес, маску подсети, шлюз по умолчанию и адрес DNS-сервера. Если в сети имеются компьютеры без поддержки DHCP, настройте для них статические IP-адреса.

Общие и частные адреса

Если ваша интрасеть не подключена к Интернету, вы вправе внедрить любую схему IP-адресации. Если вам требуется прямое (через маршрутизатор) или косвенное (через прокси-сервер или транслятор) соединение с Интернетом, стоит использовать общие и частные адреса.

Общие адреса

Общие адреса присваиваются центром InterNIC и состоят из сетевых идентификаторов, которые основаны на классах, или блоков адресов, которые основаны на протоколе Claseless Inter-Domain Routing (CIDR-блоки) и гарантированно являются глобально уникальными и Интернете. Если назначаются общие адреса, в Интернет-маршрутизаторы заносятся маршруты, чтобы трафик к общим адресам достигал конечной точки. Интернет-трафик к конечным общим адресам достигает своего места назначения.

Частные адреса

Каждому IP-узлу требуется IP-адрес, являющийся в данной IP-сети уникальным. В случае с Интернетом каждому IP-узлу сети, подключенной к Интернету, необходим IP-адрес, являющийся в Интернете глобально уникальным. С развитием Интернета подключающимся к нему организациям требовалось все больше общих адресов — для каждого из узлов их интрасетей. Это привело к тому, что диапазон доступных общих адресов значительно сократился.

Частные адреса

Компьютерам внутри организации, не нуждающимся в прямом доступе к Интернету, необходимы IP-адреса, отличные от уже присвоенных общих адресов, Для решения этой проблемы разработчики Интернета зарезервировали часть пространства IP-адресов и назвали это пространство пространством частных адресов. Частные IP-адреса никогда не присваиваются в качестве общих. Поскольку пространства частных и общих адресов не пересекаются, частные адреса никогда не дублируют общие адреса. RFC 1918 определяет следующие диапазоны IP-адресов:

- 10.0.0.0—10.255.255.255 — частная сеть с IP-адресом 10.0.0.0 — сетевой идентификатор класса А, допускающий использование действительных IP-адресов из диапазона 10.0.0.1 —10.255.255.254. У частной сети 10.0.0.0 имеется 24 разряда для обозначения узла, которые можно использовать для внедрения в организации любой схемы подсетей;
- 172.16.0.0—172.31.255.255 — частная сеть с адресом 172.16.0.0 интерпретируется как блок из 16 сетевых идентификаторов класса В или как 20-разрядное присваиваемое пространство адресов (20 разрядов для обозначения узла), которое можно использовать для внедрения и организации любой схемы подсетей. Частная сеть 172.16,0.0 допускает использование действительных IP-адресов из диапазона 172.16.0.1 — 172.31.255.254;
- (92.168.0.0—192.168.255.255 - частная сеть 192.168.0.0/16 интерпретируется как блок из 256 сетевых идентификаторов класса С или как 16-разрядное присваиваемое пространство адресов (16 разрядов для обозначения узла), которое можно использовать для внедрения в организации любой схемы подсетей. Частная сеть 192.168.0.0 допускает использование действительных I P-адресов из диапазона 192.168.0.1 — 192.168.255.254.

Принципы работы NAT

Транслятор сетевых адресов — определенный в стандарте RFC 1631 IP-маршрутизатор, способный в процессе передачи пакетов транслировать их IP-адреса и номера портов TCP/UDP.

Рассмотрим небольшую сеть из нескольких компьютеров, подключающихся к Интернету. В обычной ситуации компании потребовалось бы получить у поставщика услуг Интернета для каждого из этих компьютеров общий IP-адрес. Протокол NAT позволяет реализовать в сети компании схему частной адресации (см. RFC 1597) и привязать частные адреса компьютеров к одному или нескольким общим IP-адресам, полученным у поставщика услуг Интернета. Например, интрасеть небольшой компании реализована как частная сеть с адресом 10.0.0.0, и поставщик услуг Интернета выделил фирме общий IP-адрес 198.200.200.1. NAT привязывает (статически или динамически) все используемые в сети 10.0.0.0 частные IP-адреса к общему IP-адресу 198.200.200.1.

Статическая и динамическая привязка адресов

Протокол NAT использует статическую или динамическую привязку адресов. При статической привязке трафик всегда направляется в определенное место. Весь входящий и исходящий трафик определенного сегмента частной сети можно привязать к определенному месту в Интернете. Например, чтобы установить Web-сервер на одном из компьютеров частной сети, вы создаете статическую привязку общего IP-адреса (порт номер 80 протокола TCP) к частному IP-адресу (порт номер 80 протокола TCP).

Динамические привязки создаются, если пользователи частной сети обмениваются информацией с узлами Интернета. Служба NAT автоматически добавляет эти привязки в свою таблицу привязок и обновляет их при каждом обращении. Не применяемые динамические привязки по истечении определенного времени удаляются из таблицы привязок проекций NAT после заданного периода времени. Тайм-аут привязки для TCP-подключений по умолчанию составляет 24 часа. Для трафика UDP тайм-аут равняется 1 минуте.

Корректное преобразование полей заголовков

По умолчанию NAT преобразовывает IP-адреса и порты TCP/UDP. При этом в IP-дейтаграмму вносятся определенные изменения, которые требуют модификации и корректировки следующих полей заголовков IP. TCP и UDP:

- исходного IP-адреса;
- контрольной суммы TCP, UDP и IP;
- исходного порта.

Если информация об IP-адресах и портах содержится только в заголовках IP и TCP/UDP, как например, в протоколе HTTP или трафике WWW, прикладной протокол может транслироваться прозрачно. Впрочем, некоторые приложения и протоколы записывают информацию об IP-адресах и портах в собственные заголовки. Например, протокол FTP хранит в заголовке FTP для команды порта FTP десятичную нотацию IP-адреса. При некорректном преобразовании адреса протоколом NAT иногда возникают проблемы связи. Кроме того, н случае с FTP IP-адрес хранится в десятичной нотации, и поэтому преобразованный IP-адрес в заголовке FTP может иметь иной размер. В связи с этим во избегание потери данных служба NAT должна также изменять порядковые номера TCP.