Middleboxes: NATs

In this lesson, we'll study Network Address Translation!

We'll cover the following

Introduction

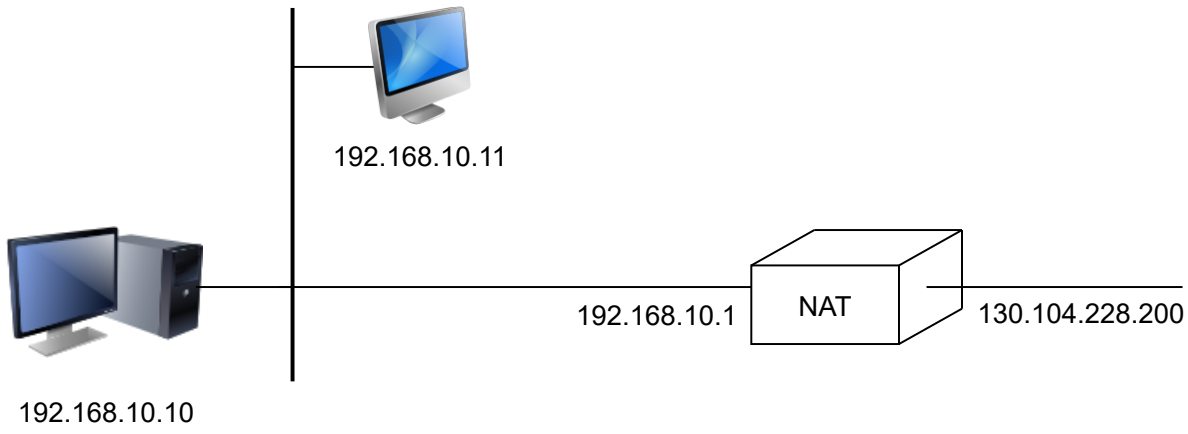
Network Address Translation (NAT) was proposed as a short term solution to deal with the expected shortage of IPv4 addresses in the late 1980s to early 1990s. Combined with CIDR, NAT helped to significantly slow down the consumption of IPv4 addresses. A NAT is a middlebox that interconnects two networks that are using IPv4 addresses from different addressing spaces. Usually, one of these addressing spaces is the public Internet while the other is using a private IPv4 address. Unlike a router, when a NAT box forwards traffic, it modifies the IP addresses in the IP header, as will be described shortly.

Broadband Access Routers

A very common deployment of NAT is in broadband access routers as shown in the figure below. The broadband access router interconnects a home network, either WiFi or Ethernet-based, and the global Internet via one ISP.

A single IPv4 address is allocated to the broadband access router and network address translation allows **all of the hosts** attached to the home network **to**

address translation allows **all of the hosts** attached to the home network **to share a single public IPv4 address**.



A simple NAT with one public IPv4 address

Enterprise Networks

The second type of deployment is in enterprise networks. In this case, the NAT functionality is installed on a border router of the enterprise. A private IPv4 address is assigned to each enterprise host while the border router manages a **pool containing several public IPv4 addresses**.

> **Note**: In typical home usage scenarios, only one public IP address is available to the NAT. However, in enterprise settings, a public IP address pool may also be configured on the NAT box.

Sending a Message over a NAT

The simplest NAT is a middlebox a mapping between a private IP address and a public IP address. To understand its operation, let's assume that a NAT has just booted.

Sending a Message

- When the NAT receives the first packet from source **S** in the internal network which is destined to the public Internet, it creates a mapping between internal address **S** and the first address of its pool of public addresses (P1).
- Then, it translates the received packet so that it can be sent to the public Internet. This translation is performed as followed:
    i. The source address of the packet (S) is replaced by the mapped

public address (P1)

ii. The checksum of the IP header is incrementally updated as its content has changed

iii. If the packet carried a TCP or UDP segment, the transport layer checksum found in the included segment must also be updated as it is computed over the segment and a pseudo-header that includes the source and destination addresses.

Receiving a Message

- When a packet destined to **P1** is received from the public Internet, the NAT consults its mapping table to find **S**.
- The received packet is translated and forwarded in the internal network.

This works **as long as the pool of public IP addresses of the NAT does not become empty**. In this case, a mapping must be removed from the mapping table to allow a packet from a new host to be translated. This **garbage collection** can be implemented by adding to each entry in the mapping table a timestamp that contains the last utilization time of a mapping entry. This timestamp is updated each time the corresponding entry is used. Then, the garbage collection algorithm can remove the oldest mapping entry in the table.

Disadvantages of NATs

NAT allows many hosts to share one or a few public IPv4 addresses. However, using NAT has two important drawbacks.

1. First, it's not easily possible for external hosts to open TCP connections with hosts that are behind a NAT. Some consider this to be a benefit from a security perspective. However, a NAT should not be confused with a firewall, as there are some techniques to traverse NATs.
2. Second, NAT breaks the end-to-end transparency of the network and transport layers.

Quick Quiz!

1

Suppose several end systems including a web server is behind a NAT. Will external clients be able to initiate connections with it?

A) Yes

B) Most likely not

COMPLETED 0%

1 of 3

In the next lesson, we'll have an introduction to routing in IP networks!