**Network Address Translation**

Table of Contents

[Static NAT 3](#_Toc87293891)

[Dynamic NAT 4](#_Toc87293892)

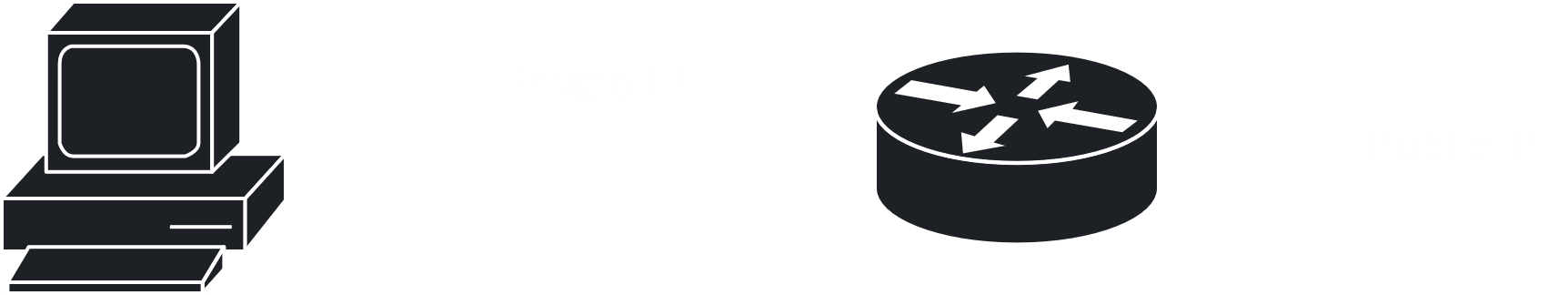
[Port Address Translation 5](#_Toc87293893)

The basic idea of **Network Address Translation** (NAT) is that a set of IP addresses for hosts in an **internal network** are translated to a different set of IP addresses that are exposed to the **global internet**. This allows us to use a small number of IP addresses, exposed globally, while still allowing a much larger number of IP addresses to be used internally. The mapping from local to global IPs is done using a **table** maintained by the router. Additionally, the global internet only ever becomes aware of the IP addresses that are exposed to it, not the ones used internally, which provides some security.

An example is the devices we use at home. We have several dozen devices connected to a Wi-Fi network at home, but our ISP only assigns us a single IP address. The router in our home uses NAT to internally assigned IP addresses for each of the devices we use and distribute different messages, which all arrive at the single, exposed IP address, to whichever internally assigned IP address the message belongs.

There are three types of NAT in Cisco devices, Static, Dynamic and Overloaded or Port Address Translation (PAT).

## Static NAT



In **Static NAT**, we use **one-to-one mapping** between a local and a global address. This basically just provides us with some security by hiding the private IP. It does not help with reducing the number of global IPs required.

Router(config)# **ip nat inside source static** *local\_ip global\_ip*

CLI

Once this is setup, we still need to specify an **inside** and an **outside interface**. Whatever host is connected to the inside interface will have their IP address translated to the global one and the resulting data will be sent out via the outside interface. We can have multiple inside and outside interfaces.

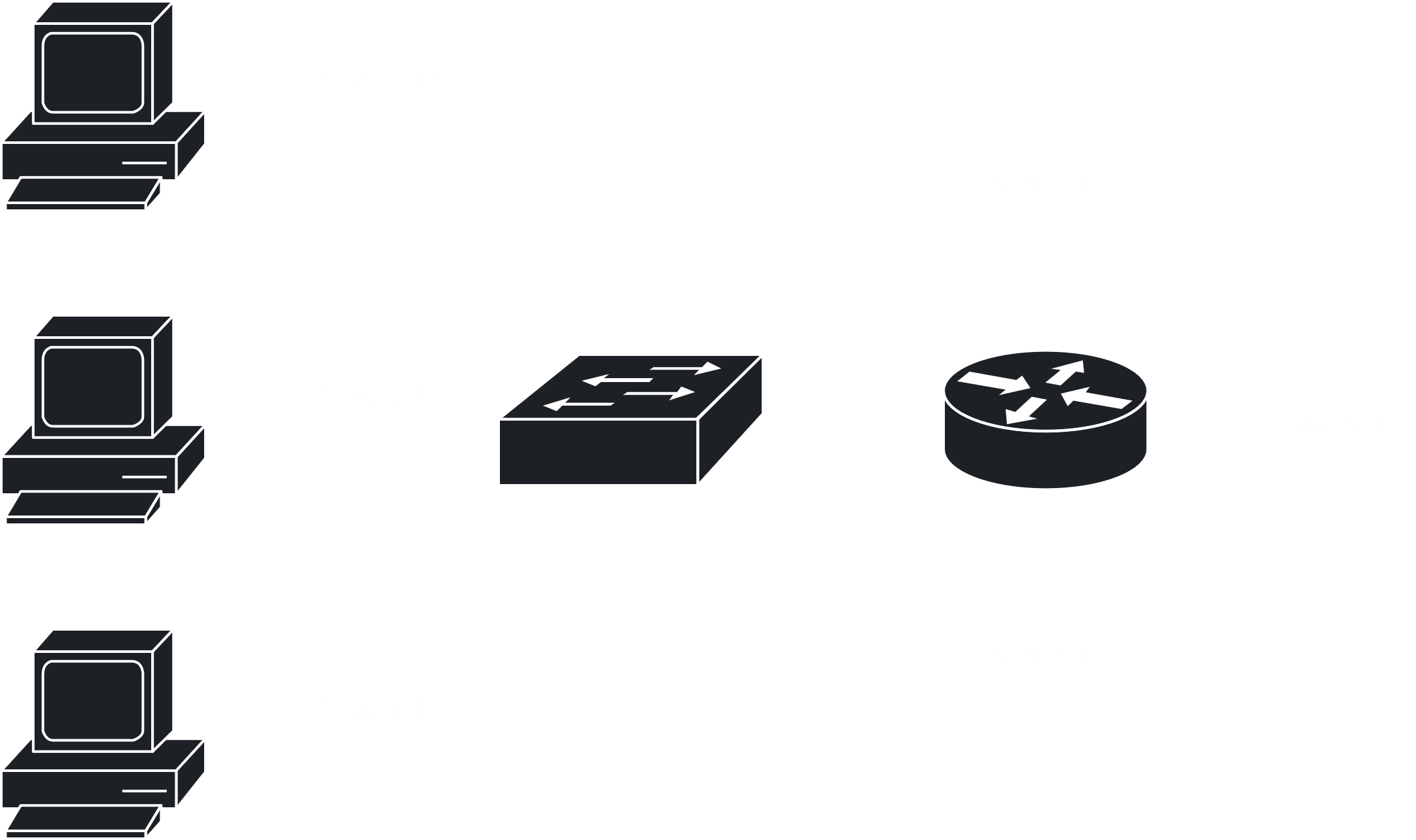
Router(config-if)# **ip nat inside**

CLI

Router(config-if)# **ip nat outside**

CLI

## Dynamic NAT



In **Dynamic NAT**, a **pool** of global addresses is available. Whenever a local address requires a connection to the internet, one of the IP addresses from the pool is selected. When not in use, the global IP addresses is released into the pool again.

To configure Dynamic NAT, we first to need to create an **access list** which permits the local addresses to be translated.

R1(config)# **access-list** *access\_list\_num* **permit** *local\_network\_addr subnet\_mask*

CLI

Next, we specify the pool of global addresses. This must be a **continuous range**.

Router(config)# **ip nat pool** *pool\_name start\_ip end\_ip* **netmask** *subnet\_mask*

CLI

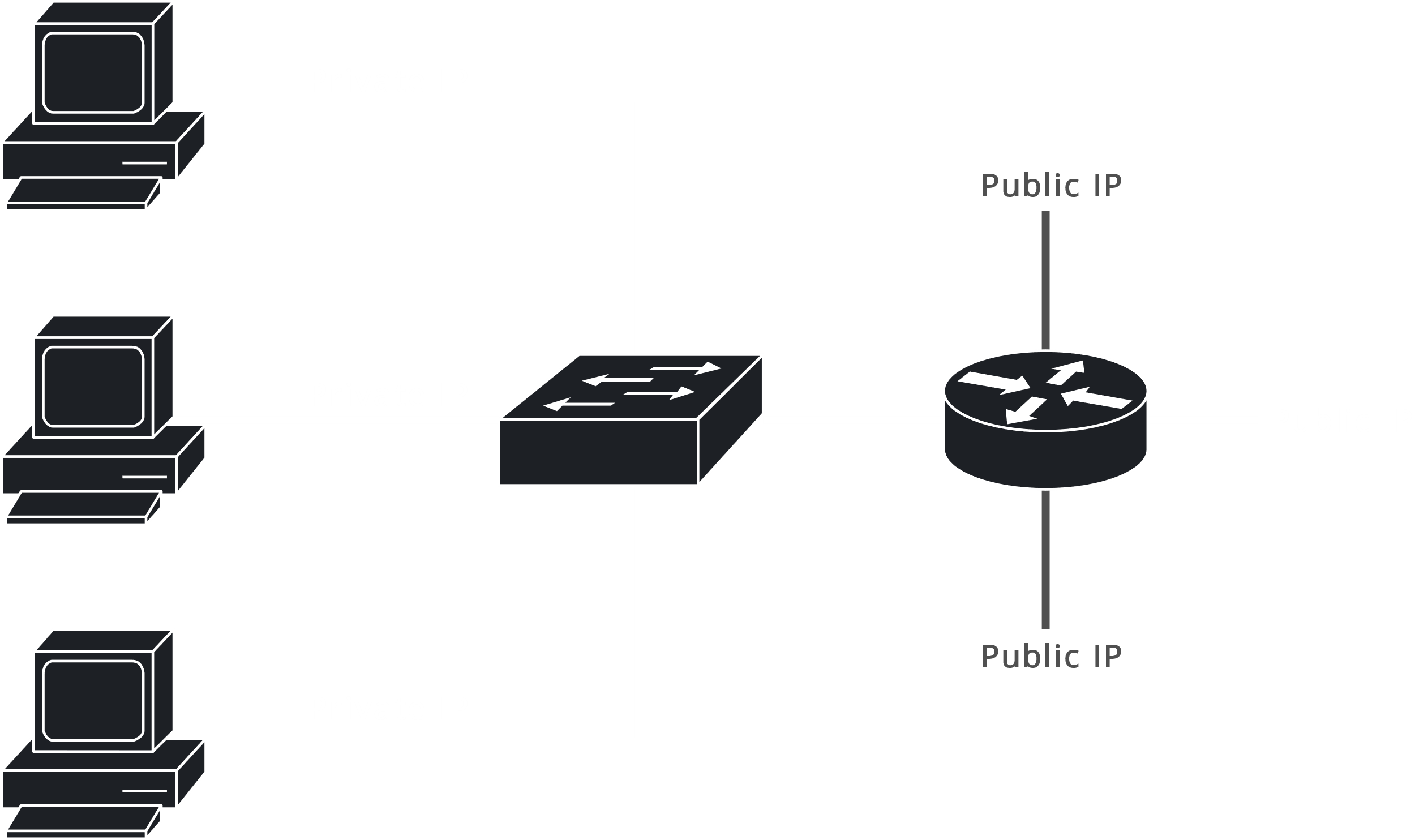
Next, we connect the pool to the access list.

Router(config)# **ip nat inside source list** *access\_list\_num* **pool** *pool\_name*

CLI

Finally, we specify the inside and outside interfaces, as above.

## Port Address Translation



In Dynamic NAT, in the worst case, we may need as may global IP addresses as we have local ones, which makes the thing pointless. In **Port Address Translation** (PAT), **multiple local addresses** are mapped to a **single global one**. TCP or UDP port information is used to separate out which data comes from or goes to which internal host. Note that we still have multiple global addresses available, but we keep using the same one until it is no longer possible to assign a different port number for each device using the global address. Although this can theoretically happen, practically, it does not.

The configuration of PAT is the same as Dynamic NAT, except for a small change in the command connecting the pool and the access list.

Router(config)# **ip nat inside source list** *acc\_list\_num* **pool** *pool\_name* **overload**

CLI