BACKGROUND

Address Depletion—The world ran out of IPv4 addresses. IPv6, with its *huge* addresses was the ultimate solution, but in the meantime, having many organizations internally reuse the same "private" addresses bought a lot of time.

Private Addresses—non-routable and never assigned to "real" destinations.

Class	Private Networks	CIDR Mask (each)	Qty of Nets
A	10.0.0.0	/8	1
B	172.16.0.0 - 172.15.0.0	/16	16
C	192.168.0.0 - 192.168.255.0	/24	256

NAT (Network Address Translation)—The process of translating internal private addresses on the fly to fewer "public" (real) addresses for traffic that uses the outside internet.

CIDR (Classless Inter-Domain Routing)—Ignore the A, B, and C address classes so you can

- Allocate smaller chunks of addresses, decreasing waste
- Summarize blocks of contiguous addresses into "supernets" (the opposite of subnets) and reduce the size of routing tables. Basically, you're saying in the routing table "all of these addresses are somewhere in that same direction." Exceptions are handled automatically because routing uses the most specific match.

TERMINOLOGY

Inside/Outside—The physical location/identity of the source computer

Local/Global—The address space being used. Local addresses are the private ones used on the internal network; Global addresses are public addresses used by the internet at large.

These terms pair up to give us the following labels in Cisco's "show" commands

Term	Meaning
Inside Local	The private IP address of our internal computer, e.g. 192.168.1.3
Inside Global	The public address that our internal computer's packets receive during NAT translation. This is what the rest of the world sees and is enough to get responses routed to our site. Once there, NAT translates this address back to the matching inside local address for internal delivery to the actual computer.
Outside Local	Not used when NAT translates source addresses. For us, it'll always match the outside global address, below.
Outside Global	The public address of the computer outside our company, somewhere on the internet, that our inside computer is trying to reach. This would be the destination address of outbound packets and simply doesn't change.

STATIC NAT

Good for public servers that need both an internal private address and a public internet address for the rest of the world. As a packet leaves an organization's internal network, its source IP address is changed from the private address used by the originating computer (inside local address) to a public address (inside global) from the pool of addresses the company owns according to a static 1:1 mapping that is configured on the router. That public address can't be used by any other internal computer.

When packets arrive from the outside addressed to that inside global address, the router replaces the destination address with the matching inside local address before forwarding the packet into the internal network.

```
R6(config)# interface gi0/0
R6(config-if)# description TO ISP
R6(config-if)# ip address 203.0.113.50 255.255.255.240
                    Our ISP has sold us the 14 addresses in 203.0.113.48/28 they are using 203.0.113.49 as our gateway.
R6(config-if)# ip nat outside

*Oct 18 03:07:04.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
                    Don't worry about this; an NVI is a "NAT Virtual Interface," part of the router's internal processing.
R6(config-if)# no shut
*Oct 18 03:07:27.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
R6(config-if)# interface gi0/1
R6(config-if)# ip address 192.168.0.1 255.255.255.0
R6(config-if)# ip nat inside
R6(config-if)# no shutdown
*Oct 18 03:10:07.843: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
R6(config-if)# exit
R6(config)# ip nat inside source static 192.168.0.2 203.0.113.51
                    Our web server. Internally, it's 192.168.0.2. The world sees it at 203.0.113.51
R6(config)# ip nat inside source static 192.168.0.3 203.0.113.52
                    Our mail server
```

Verification & Troubleshooting

```
R6# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 203.0.113.50       192.168.0.2        ---                ---
--- 203.0.113.51       192.168.0.3        ---                ---
```

DYNAMIC NAT

As a packet passes through the edge router to the internet, its source address is translated on-the-fly to one in a pool of public addresses controlled by the enterprise. A note of this translation is made by the router so that it can recognize responses and translate their destination address back to the original.

The translation can expire when packets haven't flowed for a while (configurable). You don't need as many inside global addresses in the pool as you have internal hosts, you just have enough to accommodate the number that speak to the outside world at once (plus timeout).

Configuration—The main difference is that you'll create a pool of available global addresses and an ACL that defines which inside local addresses should be translated as they exit your LAN. With our same interfaces, we just add the ACL, address pool, and our modified NAT statement.

Gi 0/0	Gi 0/1
interface GigabitEthernet0/0 description TO ISP ip address 203.0.113.50 255.255.255.240 ip nat outside	interface GigabitEthernet0/1 description LAN ip address 192.168.0.1 255.255.255.0 ip nat inside

```
ip access-list standard NAT_INSIDE_HOSTS
 remark Matching hosts will have their address translated
 permit 192.168.0.0 0.0.0.255
!
ip nat pool MY_NAT_POOL 203.0.113.51 203.0.113.62 netmask 255.255.255.240
```

IOS uses the netmask to check that the beginning address (203.0.113.51) and ending address (203.0.113.62) are in the same subnet when you enter the command.

12 External addresses means the 13th inside host will need to wait for a translation to expire

```
ip nat inside source list NAT_INSIDE_HOSTS pool MY_NAT_POOL
```

We can see a shorthand version of our definition without looking at the running-config:

```
R6# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 0  Misses: 0
```

The Hits & Misses counters refer to the NAT translation table. A packet from a fresh internal host that required a new translation entry is considered a miss. The next time (within timeout) that a packet from that same internal host needed translating, its local address would be found in the table (a hit) and translated to the same global address from the pool as before.

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT_INSIDE_HOSTS pool MY_NAT_POOL refcount 0
 pool MY NAT POOL: netmask 255.255.255.240
        start 203.0.113.51 end 203.0.113.62
        type generic, total addresses 12, allocated 0 (0%), misses 0
```

This "misses" counter refers to the number of times historically that all the global addresses in the pool had been allocated and a host couldn't be translated.

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

You can clear one or all dynamic translations from the table without waiting for them to timeout. To blow away all of them, use an asterisk (*).

```
R6# clear ip nat translation *
```

The *debug* option can issue a syslog message every time a packet is translated.

```
edge# debug ip nat
IP NAT debugging is on
```

PAT (OVERLOADING NAT)

PAT (Port Address Translation)—allows you to shrink the inside global address pool, even to just one public address, by adding the inside host's TCP or UDP *port number* to the mapping table. This allows many uses of the same global address to still be unique entries in the translation table. If a different inside host is already using the same source port number, that inside port number can even be translated to a new random one to keep things unique on the outside. This relies on the fact that even though destination ports can determine which service is being contacted, source ports are generally unimportant and often already random.

```
edge# show ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
tcp 69.12.233.218:49159   192.168.2.109:49159   17.249.60.19:443      17.249.60.19:443
tcp 69.12.233.218:49197   192.168.2.109:49197   23.5.219.228:80       23.5.219.228:80
tcp 69.12.233.218:49243   192.168.2.109:49243   23.5.219.228:80       23.5.219.228:80
tcp 69.12.233.218:49246   192.168.2.109:49246   54.230.119.218:80     54.230.119.218:80
tcp 69.12.233.218:49247   192.168.2.109:49247   54.230.119.218:80     54.230.119.218:80
udp 69.12.233.218:49990   192.168.3.53:49990    50.116.23.211:53      50.116.23.211:53
udp 69.12.233.218:50123   192.168.3.53:50123    50.116.23.211:53      50.116.23.211:53
udp 69.12.233.218:50186   192.168.3.53:50186    50.116.23.211:53      50.116.23.211:53
udp 69.12.233.218:50323   192.168.3.53:50323    50.116.23.211:53      50.116.23.211:53
udp 69.12.233.218:50567   192.168.3.53:50567    50.116.23.211:53      50.116.23.211:53
```

These last 5 UDP entries are upstream queries from the DNS server for addresses it didn't already know.

```
edge# show ip nat statistics
Total active translations: 118 (7 static, 111 dynamic; 118 extended)
Peak translations: 2275, occurred 7w0d ago
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0.2, FastEthernet0/0.3, FastEthernet0/0.22
Hits: 1007205536  Misses: 0
CEF Translated packets: 995938707, CEF Punted packets: 11189830
Expired translations: 9592209
Dynamic mappings:
-- Inside Source
[Id: 3] access-list PAT_LIST interface FastEthernet0/1 refcount 111

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Configuration—if you have more than one global address, just add the word "overload" to the configuration used for dynamic NAT. If you only need one address, you can reuse the address of world-facing interface.

```
ip nat inside source list NAT_INSIDE_HOSTS pool MY_NAT_POOL overload
ip nat inside source list NAT_INSIDE_HOSTS interface Gi0/0 overload
```

UPSHOT & PERSPECTIVE

You really just have NAT and the optional ability to overload the global address(es) by using port numbers (PAT). The global (public) addresses come from a pool that you define with a start and end address, while an ACL defines which local (private) addresses should be translated as their packets leave. Such translations can only happen with conversations initiated from within the LAN and when they do, the router keeps track of them so it can know whom to give the responses to. It delivers the responses by reversing the translation back to a local address. Static NAT is nothing more than manually adding a permanent entry to the translation table, with or without overloading. Since static entries are in place before the conversation starts, they allow outside entities to begin the conversation, which is good for public-facing servers in your LAN.

TROUBLESHOOTING

You'll need traffic hitting the "inside" interface for NAT to act on—hard when prototyping in a lab. Also, all the normal problems with routing, port security, filtering ACLs, etc. can keep traffic from invoking NAT.

Common Problems	Diagnosis & Symptoms
inside & outside interfaces reversed ("ip nat inside" command on the wrong interface)	`show ip nat statistics` *Interfaces listed near top* Only packets entering an "inside" interface get translated.
(Static NAT) addresses reversed	The local address comes first, then the global. You can remember this because the command starts with "ip nat inside…"
(Dynamic NAT) ACL doesn't match [all] of the necessary inside local addresses	

(Dynamic NAT without overload) Not enough global addresses in the pool.
 	
Of course if the pool is way too small, maybe PAT was intended and the overload keyword is missing.
	`show ip nat statistics`
	Look for a growing second "misses" counter
	`show ip nat translations`
	Compare list length to the size of the pool

PAT missing the "overload" keyword.	Each address in the pool will only be available to one outbound host. For all other hosts, it looks like "the internet is down."
Filtering ACL on a NAT interface	Order of operations on an interface: • Inbound—ACLs before NAT • Outbound—NAT before ACLs Remember that ACLs are on the interlace; NAT is internal to the router.