

M³AAWG Technology Summary Carrier-Grade NAT

August 2024

The reference URL for this document is https://www.m3aawg.org/ts_CarrierGradeNat

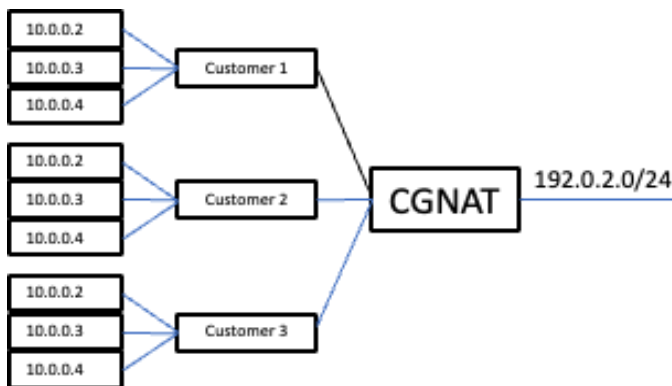
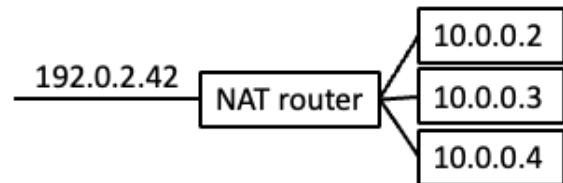
M³AAWG Technology Summary: Carrier-Grade NAT

The IP address shortage

Every device on the internet needs an IP address to identify it. Since the advent of always-on mobile and broadband, the supply of traditional IPv4 addresses has been exhausted. Larger IPv6 addresses are also available, but it will be many years until IPv6 is ubiquitous enough to replace IPv4.

What is NAT?

Network Address Translation, or NAT, allows all the computers on a network to have local private addresses, and to share an external IP address. Home networks invariably use NAT to let all the devices in the house share the router's external address.



Carrier-Grade NAT

Carrier-Grade NAT, or CGN, takes the same idea a step further: a group of ISP customers share a pool of external addresses at the ISP's router. With CGN, an ISP can put hundreds of customers behind a single external IP address, making the supply of external addresses go much farther. Consumer ISPs such as telephone and cable companies have used CGN since the early 2000s. Two levels of NAT (CGN in front of home NAT) are common.

Issues with CGN

- Servers need external addresses to allow clients to contact them; it is impractical to put servers behind CGN. Consumer ISPs generally block the ports that servers use (port 25 for mail, e.g.) so in practice this is rarely a problem for those consumer ISPs.

- CGN makes it more difficult to diagnose abuse and other problems, since third parties will report the external address, not the address of the offending device behind the CGN. CGNs have to keep detailed logs of the internal-to-external translation so that the ISP can tell which timestamp, external IP, and ports were used by which internal device in order to identify the device and resolve the problem.
- When a server receives multiple connections from a single IP address, it cannot assume those connections are related in any way. They may be from users that are neither physically nor organizationally near each other.

Further reading

RFC 6888, *Common Requirements for Carrier-Grade NATs (CGNs)*, <https://www.rfc-editor.org/rfc/rfc6888>
A Multi-perspective Analysis of Carrier-Grade NAT Deployment, <https://arxiv.org/abs/1605.05606>