NATing
Network Address Translation

To be
Presented to
St. Louis Unix Users Group
TBD, 2018
By
David Forrest

Who am I?

David Forrest graduated from Oregon State University in BA, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7, Raspbian, Mint, and Chrome on various local and cloud machines.

What is “NATing”

- This red slide and the following 15 to the next red are a prologue “background” and will be largely skipped (TL;DR) in the actual presentation.
- This prologue to V6 addressing is an aside largely from Julia Evans site: https://drawings.jvns.ca/nat/ and wikipedia.
- Local addressing is routable only locally and can be “NATed” in the IPv4 system to use a public routable v4 site address (no longer available from the agreed regional international registries, RIRs,) to be shared by those lucky enough to own them.
- This prologue presentation will attempt to cover the local functions needed to implement the “sharing”.

NATing and breeches

We have had over 20 years of delaying the necessity of using IPv6 as we have effectively used NATing on IPv4. But IPv4 is now out of public addresses and ISPs have resorted to re-NATing previously NATed connections, Carrier Grade Nat (CGN). This has caused significant congestion in some carrier configurations along with schemes to filter some bogus networks.

My Thoughts on NAT

All of the confusion/complexities on NAT (although some believe it gives them “safety through routing”) leads me to conclude that the new paradigm of IPv6 properly excludes such except in prefix NATing necessary for those using the “Unique (Universal) Local Address” scheme available in IPv6. IPv6 allows enough addresses to give safe and effective firewall routing control throughout our assigned internet addresses.

What is a MAC Address?

A MAC address is a unique identifier for network interfaces. It is a 48-bit number (12 hexadecimal characters). They can either be written in either of these formats:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

What is an ODI ?

An OUI {Organizationally Unique Identifier} is a 24-bit number that uniquely identifies a vendor or manufacturer. They are purchased and assigned by the IEEE. The OUI is basically the first three octets of a MAC address. For example, these are examples of OUI:

00:00:0A -- this is owned by Omron

00-0D-4B -- this is owned by Roku, LLCar

And maybe not even NPT

IPv6-to-IPv6 Network Prefix Translation (**NPTv6**) is an experimental specification for IPv6 to achieve the address-independence at the network edge, given by network address translation (NAT) in IPv4. It has fewer architectural problems than traditional IPv4 NAT; it is for example stateless and preserves the reachability attributed to the end-to-end principal. However, the method still lacks solutions to translate embedded IPv6 addresses, for example in IPsec, and requires a more complex nameserver setup (split-horizon DNS).

NAT Summary

- IPv6 NAT is not needed for address sharing, but may be for other situations.
- In IPv4 networks, we solved the shortage of addresses by using NAT to share one public IP address between many hosts. In IPv6, we have no address shortage and do not need to share IP addresses any more. For other uses of NAT, work is still going on to figure out how to solve these – but we will propably end up using NAT66 in some situations in our networks. By learning how the use of NAT and private address space breaks the network architecture and adds costs to projects like VoIP and causes additional delays in the network we will not add these by default when building IPv6 networks.

The State of a Connection!

- In IPv4 we used the state of the connection, “Established, Related, or New - a SYN packet that has not been ACKed ” to determine if this is a valid connection packet. Many things could interfere and level 1 (transit) errors have to have been properly satisfied before we get to assembling a valid packet. That procedure used the address, port, and checksum data in the header verify the state of the connection packet that may be composed of several different individual transmitted records.

The port is the key

- The port and/or address data can be used in firewall rules to control how the connection packet is handled. There are over 65,000 possible ports and an ipv4 customer has usually only one address of a possible 256 in a /24. This lets an ISP aggregate them in their transmission within their network as a natted address connection. That’s where the rubber meets the road. Carrier-grade NAT is not necessary in stateless IPv6.

It’s really 128 bits!

- The routing, subnet, and interface together is the IPv6 address. When an internet “Socket” is established (connected), it is similar to a hard wired connection.
- A network socket is an internal endpoint for sending or receiving data within a node on a computer network. Concretely, it is a representation of this endpoint in networking software (protocol stack), such as an entry in a table (listing communication protocol, destination, status, etc.), and is a form of system resource.

Socket

- The term socket is analogous to physical female connectors, communication between two nodes through a channel being visualized as a cable with two male connectors plugging into sockets at each node. Similarly, the term port (another term for a female connector) is used for external endpoints at a node, and the term socket is also used for an internal endpoint of local inter-process communication (IPC) (not over a network). However, the analogy is strained, as network communication need not be one-to-one or have a dedicated communication channel.

Fin

- And that's it, folks!
- I'm open and interested in questions (?)

Thanks,