



A World without IPv4 NAT

Tony Hain

alh-ietf@tndh.net

NAv6TF/ARIN XV IPv6 Conference

Orlando, Florida

April 17 – 21, 2005





Market perceived benefits of IPv4 NAT

draft-ietf-v6ops-nap-00.txt

<i>Function</i>	<i>IPv4</i>	<i>IPv6</i>
Simple Gateway	DHCP – single address upstream DHCP – limited number of individual devices downstream	DHCP-PD – arbitrary length customer prefix upstream SLAAC via RA downstream
Simple Security	Filtering side effect due to lack of translation state	Explicit Context Based Access Control (or Reflexive ACL)
Local usage tracking	NAT state table	Address uniqueness
End system privacy	NAT transforms device ID bits in the address	Temporary use privacy addresses
Topology hiding	NAT transforms subnet bits in the address	Untraceable addresses using IGP host routes /or MIPv6 tunnels for stationary
Addressing Autonomy	RFC 1918	RFC 3177 & ULA
Global Address Pool Conservation	RFC 1918	340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}) addresses
Renumbering and Multi-homing	Address translation at border	Preferred lifetime per prefix & Multiple addresses per interface



Simple Gateway

- Prefix delegation (DHCP-PD)
 - arbitrary length customer prefix via upstream dhcp request
- Stateless Address AutoConfiguratoon (SLAAC)
 - RA downstream to devices
- Default route upstream



Simple Security

- Explicit Context Based Access Control
 - The filtering side effect in a NAT due to lack of translation state does not provide predictable security
- RPF filtering
 - Only allow the DHCP-PD prefix out as a source



Local usage tracking

- Address uniqueness
 - Tracking of real address rather than random numbers from a chain of nested nat.



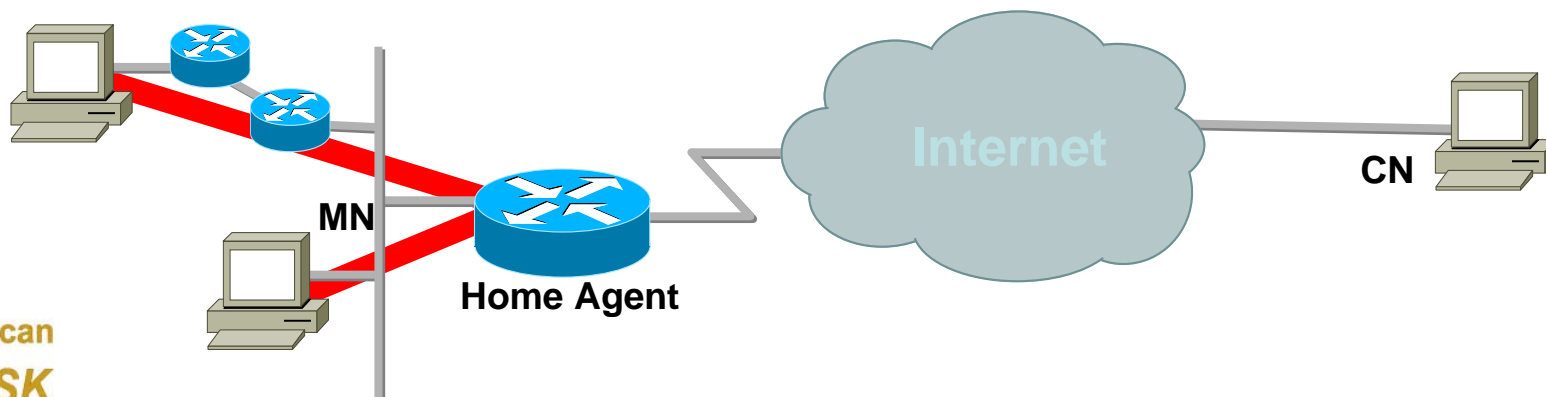
End system privacy

- Temporary use privacy addresses
 - Random 62 bit IID
 - Auto-generated for outbound connections
need to avoid ddns churn
 - Can be centrally managed for either in or out bound by running the algorithm on a DHCP server then remembering which mac the result is assigned to.



Topology hiding

- Untraceable addresses
 - IGP host routes
 - static topology-independent addresses
 - MIPv6 tunnels for stationary devices
 - Turn off route optimization, then have the potentially rack mounted server bind to a home agent at the edge of the corporate network.





Addressing Autonomy

- RFC 3177 with direct site allocation
- ULA (unique local addresses)
 - Multiple addresses per interface



Global Address Pool Conservation

- 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}) addresses
- 18,446,744,073,709,551,616 (18×10^{18}) subnets
- /4 (ie: $1/16^{\text{th}}$ of the total) is sufficient for /64 subnet per cubic meter, 1Km deep over the surface of the earth.
draft-hain-ipv6-pi-addr-07.txt



Renumbering and Multi-homing

- Preferred & valid lifetime per prefix
 - Set old as short preferred, valid through switch
 - Set new as long preferred, valid through switch
- Multiple addresses per interface
 - Controlled renumbering using both old & new
 - Multi-home with simultaneous use of prefixes