NAT64

Overview

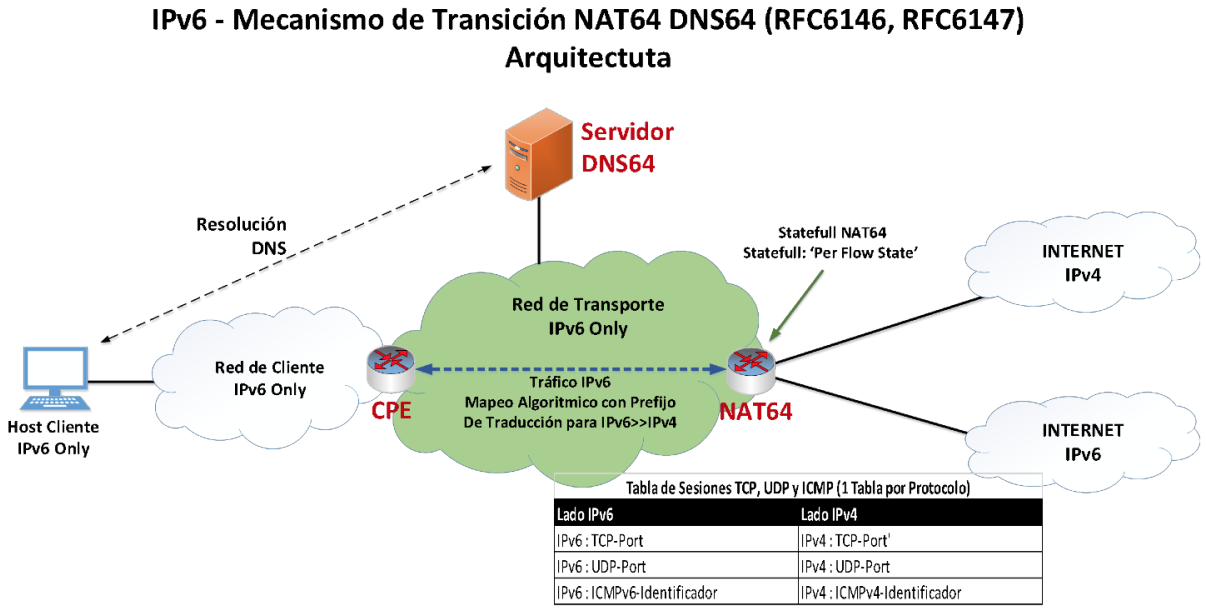
This mechanism is based on the deployment of stateful NAT64 on the edge of the ISP's network and is formally standardized in IETF RFC6146 (2011). The accompanying DNS64 mechanism is defined in RFC6147 (2011).

NAT64 was especially designed to allow IPv6-only clients and hosts to establish outbound connections to servers on the IPv6-only Internet. In other words, it was specifically designed for IPv6-only clients. It solves the problem of IPv6-only clients wishing to connect to IPv4-only servers and for which there are no AAAA records in the DNS.

For example, an IPv6-only host will not be able to connect to 'https://www.server.net' if this domain name only has an A Record. This is because an IPv6-only host has no way to establish connections to IPv4 hosts. So, NAT64 allows the IPv6-only host to perform an algorithmic translation from IPv4 to IPv6 using either DNS64 or a literal translation of IPv4 and IPv6. The IPv6-only host then translates the destination IP address from IPv4 to IPv6 and tries to establish a connection to the translated IPv6 address relying on the stateful NAT64 translation performed at the edge.

The DNS64 component allows synthesizing AAAA records from A records in a DNS server. The DNS64 function is deployed on a DNSv6 server with the functional extension for DNS64 enabled. With the use of DNS64, IPv6-only clients do not require any adaptations or additional applications. DNS64 operates asynchronously and fully decoupled from NAT64. The configuration of the prefixes and the translation scheme used in DNS64 and NAT64 must match. Despite performing an important function, DNS64 is optional and may be omitted. In this case, IPv6-only clients must perform the NAT46 translation manually. NAT64 uses an IPv6-only transport network, which means that this network is more efficient and simpler, as the operator's network manages and operates a single protocol stack. The NAT64 component deploys the stateful IPv6 to IPv4 translation function. NAT64 uses an IPv4 address pool (at least one public IPv4 address) for NAT and IP traffic to the IPv4-only Internet. NAT64 devices will have at least two interfaces: an interface on the operator's IPv6-only network and an interface to connect to the IPv6 Internet. NAT64 supports TCP, UDP and ICMP protocol connections. NAT64 even supports protocols compatible with NAT traversal, such as ICE (RFC5245). NAT64 matches the 'client-server' model and only resolves outgoing connections from IPv6-only clients to IPv4-only servers. NAT64 can even support the possibility of filtering on the edge device that performs IPv6 to IPv4 NAT The algorithmic mapping translation, in both the IPv6-only client and the NAT64, it is performed as defined in RFC 6052 (2010). While any translation prefix scheme may be used, typically the well-known prefix 64:ff9b::/96 is used. Finally, an interesting detail of stateless NAT46

translation in the IPv6-only client (manually) or via DNS64, and the NAT64 translation at the edge is that, in the IPv6-only client, only the connection's IPv6 destination address is translated, while in NAT64, stateful NAPT46 is performed and both source and destination IPv6 addresses are translated. A working routed path must exist between the IPv6-only client and the NAT64 router.



Technical Characteristics

NAT64 is a transition mechanism especially designed for IPv6-only clients. It solves the problem that arises when IPv6-only clients need to establish outgoing connections (TCP, UDP or ICMP) from an IPv6 host to IPv4-only servers on the Internet. It is often described as a transition mechanism for datacenters, servers and hosts in IPv6-only configuration. It is based on algorithmic mapping translation and does not use encapsulation. Instead, it uses an IPv6-only transport network.

NAT64 is based on algorithmic mapping translation (details). NAT64 does not use IPv4 in IPv6 encapsulation techniques. Instead, for both NAT46 and NAT64, it utilizes a translation technique that uses algorithmic mapping to map IPv4 addresses to the corresponding IPv6 addresses. RFC6052 (2010) defines the operational details of this algorithmic mapping. The table below (source: RFC6052, Section 2.2) illustrates the algorithmic mapping process for IPv4 to IPv6 translation (and vice versa):

IPv4-Embedded IPv6 Address Format											
PL	0 - 31	32-39	40-47	48-55	56-63	64-71	72-79	80-87	88-95	96-103	104-127
32	prefix	v4(32)				u	suffix				
40	prefix		v4(24)			u	v4(8)	suffix			
48	prefix			v4(16)		u	v4(16)	suffix			
56	prefix				v4(8)	u	v4(24)	suffix			
64	prefix					u	v4(32)				suffix
96	prefix (tipico: 64:ff9b::/96)									v4(32)	

Examples of algorithmic mapping

Example & Text Representation		
IPv6 Prefix	IPv4	IPv4-Embedded IPv6 Address
2001:db8::/32	192.168.2.33	2001:db8:c000:221::
2001:db8:100::/40	192.168.2.33	2001:db8:1c0:2:21::
2001:db8:122::/48	192.168.2.33	2001:db8:122:c000:2:2100::
2001:db8:122:300::/56	192.168.2.33	2001:db8:122:3c0:0:221::
2001:db8:122:344::/64	192.168.2.33	2001:db8:122:344:c0:2:2100::
2001:db8:db8:122:344::/96	192.168.2.33	2001:db8:122:344::192.0.2.33

Although NAT64 allows the use of any /32, /40, /48, /54, /64 or /96 translation prefix, the most commonly used is the well-known prefix **64:ff9b::/96**.

NAT works over an IPv6-only transport network. NAT64 uses IPv6-only between the CLAT and the PLAT. The use of IPv6-only in the transport network provides for greater efficiency and better performance in the core network and L3 switching of the operator (ISP), even more so given that it does not use packet encapsulation. An IPv6-only transport network also allows the operator to deploy traffic engineering and QoS techniques to optimize traffic, service and network management.

NAT64 supports TCP, UDP and ICMP traffic. NAT64 supports TCP, UDP and ICMP connections. It does not support protocols such as IPSec or multicast. It fully matches the client-server service model and is designed for outbound connections from IPv6-only devices and hosts on the ISP's network. It does not define a solution for incoming connections from the IPv4 Internet to IPv6-only hosts. In other words, NAT64 does not fully match the peer-to-peer model on which the Internet is based.

Advantages:

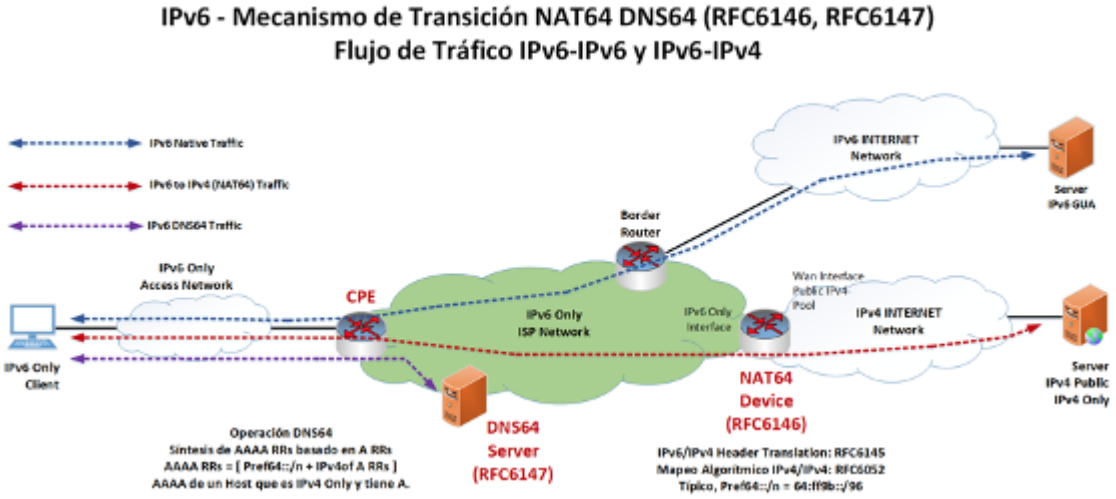
- Does not require modifications or additional applications or protocols on IPv6-only clients.
- Does not use encapsulation.

- IPv6-only transport network: high efficiency and performance, single protocol stack and management.
- Promotes the deployment of IPv6-only client devices and hosts.
- Native IPv6 traffic is neither translated nor encapsulated.
- Allows traffic engineering and QoS in the operator's network.
- Matches the client-server model and allows outgoing connections from IPv6-only local binding.
- Allows load balancing through the simultaneous use of several NAT64 and several translation prefix schemes.
- Allows multiple IPv6-only clients (e.g. IPv6-only datacenters) to share the use of one or more public IPv4 addresses to connect to the IPv4-only Internet.

Disadvantages

- Does not resolve incoming connections from the IPv4 Internet.
- Limited to TCP, UDP and ICMP.
- If used, the DNS64 component (although it operates asynchronously) must be configured with the same prefix and translation scheme as the one used in NAT64.
- Applications that require local binding in IPv4 (IPv4 using API sockets) will fail, as will any application that requires native IPv4 in the IPv6-only client.

Detailed Architecture and Diagram



- Native IPv6 traffic is not handled by the NAT64 mechanism.
- IPv6 to IPv4 traffic is handled by the NAT64 mechanism and can optionally use DNS64.
- Location of the DNS64 service:

- On the same device where NAT64 is deployed.
- On a DNS64 server that is part of the ISP's network.
- On a DNS64 server that is external to the ISP's network (public DNS64).
- On a DNS64 server in the ISP's Cloud.

· In turn, the NAT64 service may also be located as follows:

- NAT64 in the ISP's network.
- NAT64 that is external to the ISP's network (third-party or public NAT64).
- NAT64 in the ISP's Cloud.

NAT64 and Upstream Traffic