INTAREA
Internet-Draft
Intended status: Informational
Expires: 4 October 2025

D. McLarty
Independent

2 April 2025

NAT Sub Address Protocol
draft-mclarty-nat-sub-address-protocol-00

Abstract

This document defines the NAT Sub-Address Protocol (NATSAP), a Layer 5 encapsulation protocol designed to facilitate seamless bidirectional communication with devices behind Carrier-Grade NAT (CG NAT). NATSAP introduces dynamic sub-addresses assigned by the NAT router, which external clients can use alongside the public IP to route traffic back to internal devices without requiring traditional port forwarding. This document also defines the Dynamic Sub-Address Assignment Protocol (DSAAP), to facilitate the acquiring of a NATSAP Sub-Address.

The protocol offers backward compatibility with existing IPv4 infrastructure, efficient DNS-based service discovery, and simple, stateless mapping. By encapsulating application-layer traffic, NATSAP enables direct communication with devices behind NATs using a standardized socket notation and DNS records.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://Daniel-McLarty.github.io/NAT-Sub-Address-Protocol/draft-mclarty-nat-sub-address-protocol.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-mclarty-nat-sub-address-protocol/.

Discussion of this document takes place on the INTAREA Working Group mailing list (mailto:int-area@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/int-area/. Subscribe at https://www.ietf.org/mailman/listinfo/int-area/.

Source for this draft and an issue tracker can be found at https://github.com/Daniel-McLarty/NAT-Sub-Address-Protocol.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The proliferation of Carrier-Grade NAT (CG NAT) in IPv4 networks has made it increasingly difficult for devices behind NATs to host services. Traditional NAT traversal techniques, such as port forwarding, STUN, TURN, and UPnP, are cumbersome, inconsistent, and difficult to automate.

NATSAP addresses this issue by introducing:

* Dynamic sub-addresses, automatically assigned by the NAT router using DSAAP.

* Encapsulation at Layer 5, allowing transparent traversal of NAT devices.

* DNS integration for seamless service discovery.

* Backward compatibility with existing network infrastructure.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

* *NATSAP*: NAT Sub-Address Protocol

* *DSAAP*: Dynamic Sub-Address Assignment Protocol

* *CG NAT*: Carrier-Grade Network Address Translation

* *Sub-Address*: A unique 32-bit identifier assigned by the NAT router to an internal device.

* *NATSAP Table*: A mapping table in the NAT router that associates sub-addresses with internal IPs.

3. Protocol Overview

3.1. Protocol Flow

1. Client Initialization (DSAAP)

    * When a device connects to the CG NAT network, it sends a DSAAP request to the gateway router.

    * The NAT router responds with a DSAAP reply, assigning a 32-bit sub-address to the client.

    * The client stores the sub-address and uses it for external communication.

2. Service Advertising (DNS)

    * The client updates the NATSAP TXT record in DNS with its current sub-address.

    * Example DNS record:

A: example.com → 192.0.2.20 TXT: _natsap.example.com → "example.com, ABCD-1234"

1. Third-Party Client Connection

    * The external client resolves the public IP via the A record.

    * It looks up the _natsap TXT record for the sub-address.

    * It forms the NATSAP socket: natsap://192.0.2.20[ABCD-1234]:443

2. NATSAP Encapsulation

    * The external client encapsulates its application-layer traffic inside a NATSAP packet.

    * The CG NAT router receives the packet, extracts the sub-address, and performs a table lookup to route the traffic to the appropriate internal device.

    * The router forwards the traffic to the internal client.

    * The internal client de-encapsulates the NATSAP packet and treats the application-layer traffic like normal.

* The internal client then sends a standard reply to the external client.

* If the external client has to send new traffic to the internal client the external client will build a new NATSAP packet.

4. NATSAP Header Format

Field Name	Description
Version (8 bits)	NATSAP protocol version (e.g., 0x01).
Flags (8 bits)	Reserved for future use.
Destination Sub-Address (32 bits)	The Sub-Address of the server.
Encapsulated Data Length (16 bits)	Length of the encapsulated payload in bytes.
Encapsulated Data (variable)	The original datagram traffic (e.g., https)

Table 1

5. DNS Integration

NATSAP uses DNS TXT records for service discovery.

5.1. DNS Record Format

* A record: The public IP of the CG NAT router.

* TXT record:

  - Name: _natsap.FQDN

  - Value: "FQDN, sub-address"

5.2. Example DNS Records

A: example.com → 192.0.2.20 TXT: _natsap.example.com → "example.com, ABCD-1234" Clients use the A record to find the public IP and the TXT record to retrieve the sub-address.

6. Socket Addressing Scheme

NATSAP defines a new URI format for addressing services:

natsap://<public-ip>[<sub-address>]:<original-port>

Example URI: natsap://192.0.2.20[ABCD-1234]:443

7. Dynamic Sub-Address Assignment Protocol (DSAAP)

TODO DSAAP

8. Security Considerations

8.1. Sub-Address Privacy

* Sub-addresses are public, similar to ports.
* Applications should use existing encryption protocols (e.g., TLS) for security.

9. Backward Compatibility

NATSAP is backward-compatible with existing IPv4 infrastructure:

* No modifications to Layer 3 or Layer 4 protocols are required.
* Non-NATSAP routers will simply drop unrecognized NATSAP packets.
* Services using traditional ports remain unaffected.

9.1. Rate Limiting

* The CG NAT router should rate-limit DSAAP requests to prevent abuse.

9.2. Expiration and Reuse

* Sub-addresses should have a lease time to prevent stale mappings.
* Routers should implement keep-alive mechanisms to verify active clients.

10. IANA Considerations

IANA may need to register both a TCP and UDP port to NATSAP. IANA may need to register a UDP port to DSAAP.

11. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgments

TODO acknowledge.

Author’s Address

Daniel McLarty
Independent
Email: daniel@mclarty.tech