RELOAD

draft-bryan-p2psip-reload-01
draft-lowekamp-p2psip-reload-security-01

Bruce Lowekamp
David Bryan
Jim Deverick
Marcia Zangrilli

What is RELOAD?

Evolved from dSIP

Implemented protocol

Security mechanism

NAT traversal support

Multiple DHT algorithms

Overview

Lightweight, extensible

- Fast routing
- Lightweight header
- TLV (based on STUN) used in body
- Minimal assumptions in base protocol
  - Method range reserved for DHT algorithms
  - Attribute range reserved for DHT and security
- NAT traversal support for applications (Open/Tunnel)

Pluggable DHTs

Base protocol does not specify which DHT, two written:

- Chord
- Bamboo

Must provide:

- isResponsible(ID)
- Build routing table
- DHT-specific attributes and methods

Message Structure

Fixed header

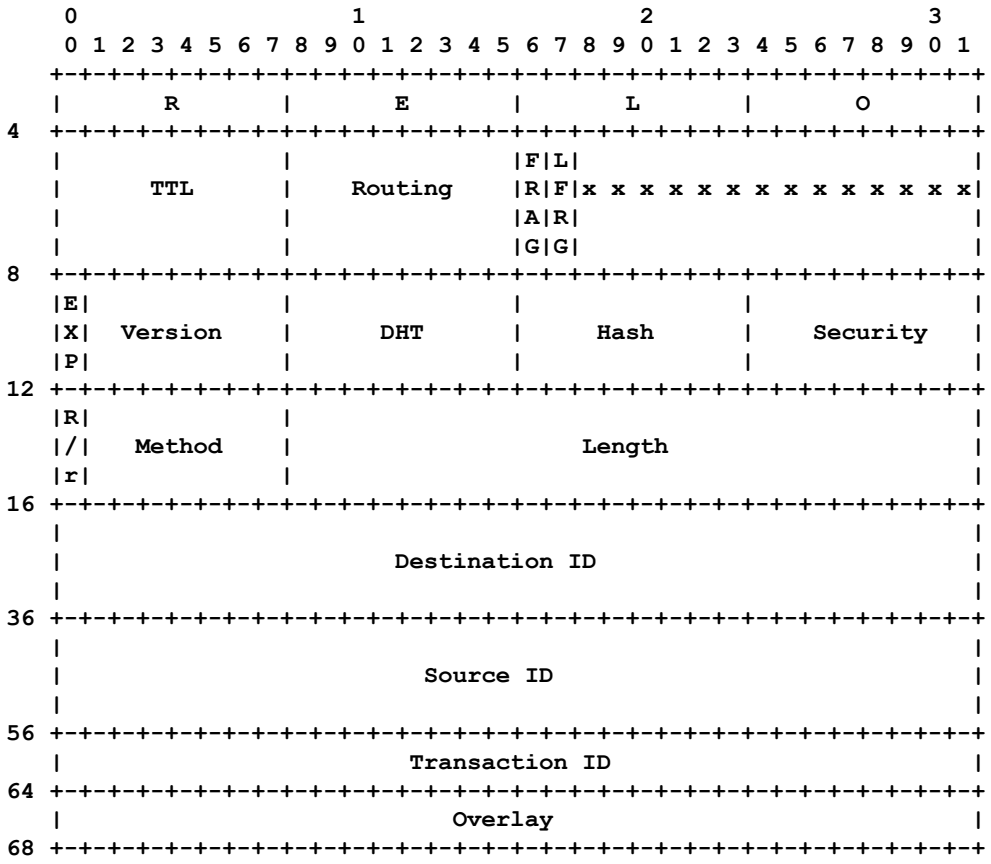
- Version compatibility
- State machine
- Route based on fixed length and offset

Body: attributes

- TLV-encoded
- Can occur multiple times
- “Types” can be recursive

Fragmentation supported

Header



Key Points:

- Nothing else needed to route
- Two lines confirm compatibility
- Method and TID for routing and processing

Message Attributes and Types

Body consists entirely of TLV attributes

Nested attributes are allowed

- Peer-Info contains Peer-ID, Name, and IP-Port information

Same structures used for different attributes

- Both Source-Info and Redirect use the Peer-Info structure

Using Signatures

Three forms of security

- None, HMAC, Certificates

Signatures are used to

- Ensure end-to-end message integrity
- Ensure integrity of components
  - no transitive trust

Signature applies to all previous attributes at the same level or below

- entire message
- single Peer-Info

What Signatures Protect

Certificates granted on enrollment

- Authorize a range of PeerIDs
- Authorize particular resources

Signatures remain with peer and resource data

A subversive peer

- Cannot choose PeerID
- Can drop messages
- Can return Not Found
- Can return unexpired but replaced registrations

Most attacks handled by replication and parallel searches

What a message looks like

```
Version: 0x01
Method: 0x11
DHT: 0x0
Security: 0x03
Hash: 0x0
Source ID: 463ac413c4
Destination ID: a6c5927a45
-------Attributes-------
SOURCE-INFO:
   PEER-ID: 463ac413c4
   PEER-IP-PORT: 10.4.1.2:5060
   PEER-CERT: 23d634...
   PEER-EXPIRATION: 300
   PEER-SIGNATURE:
       TIMESTAMP: 946702799
       DIGEST: 00acf2…
…
```

```
RESOURCE:
   RESOURCE-INFO.KEY: alice@example.com
   RESOURCE-INFO.BODY:
      RESOURCE-INFO.BODY.ENTRY: sip:alice@10.4.1.2:5060
      RESOURCE-INFO.BODY.EXPIRATION: 300
      RESOURCE-INFO.BODY.PARAMETER:
         RESOURCE-INFO.BODY.PARAMETER.KEY: type
         RESOURCE-INFO.BODY.PARAMETER.OP: 0x1
         RESOURCE-INFO.BODY.PARAMETER.VALUE: voice
      RESOURCE-INFO.BODY.PEER-INFO:
         PEER-ID: 463AC413C4
      RESOURCE-INFO.BODY.SIGNATURE:
         TIMESTAMP: 946702799
         DIGEST: 3037e...
   RESOURCE-INFO.BODY
      RESOURCE-INFO.BODY.ENTRY: mailto:alice@example.com
      RESOURCE-INFO.BODY.EXPIRATION: 24000
      RESOURCE-INFO.BODY.PARAMETER:
         RESOURCE-INFO.BODY.PARAMETER.KEY: type
         RESOURCE-INFO.BODY.PARAMETER.OP: 0x1
         RESOURCE-INFO.BODY.PARAMETER.VALUE: voicemail
      RESOURCE-INFO.BODY.SIGNATURE:
         TIMESTAMP: 946702799
         DIGEST: 5f271b1...
   RESOURCE-INFO.BODY
      RESOURCE-INFO.BODY.CERTIFICATE: 23d634...
SIGNATURE
   TIMESTAMP: 946702799
   DIGEST: f7a155b0…
```

NAT Traversal

TRANSPORT-OPEN

- Use overlay for control connection for ICE
- SDP determines type of connection
  - open to other encodings

TRANSPORT-TUNNEL

- Route messages across overlay
- SIP, RELOAD, etc
- Solution for peers joining from behind NATs and secured client protocol

Peer-Info

PEER-INFO:

- PEER-ID
- PEER-NAME
- PEER-IP-PORT
- PEER-EXPIRATION
- PEER-CERTIFICATE
- PEER-SIGNATURE

Resource-Info

RESOURCE-INFO:

- KEY
- BODY
  - ENTRY
  - PARAMETER
  - EXPIRATION
  - SIGNATURE
  - PEER-INFO
  - CERTIFICATE