Multiple Multi6 Approaches

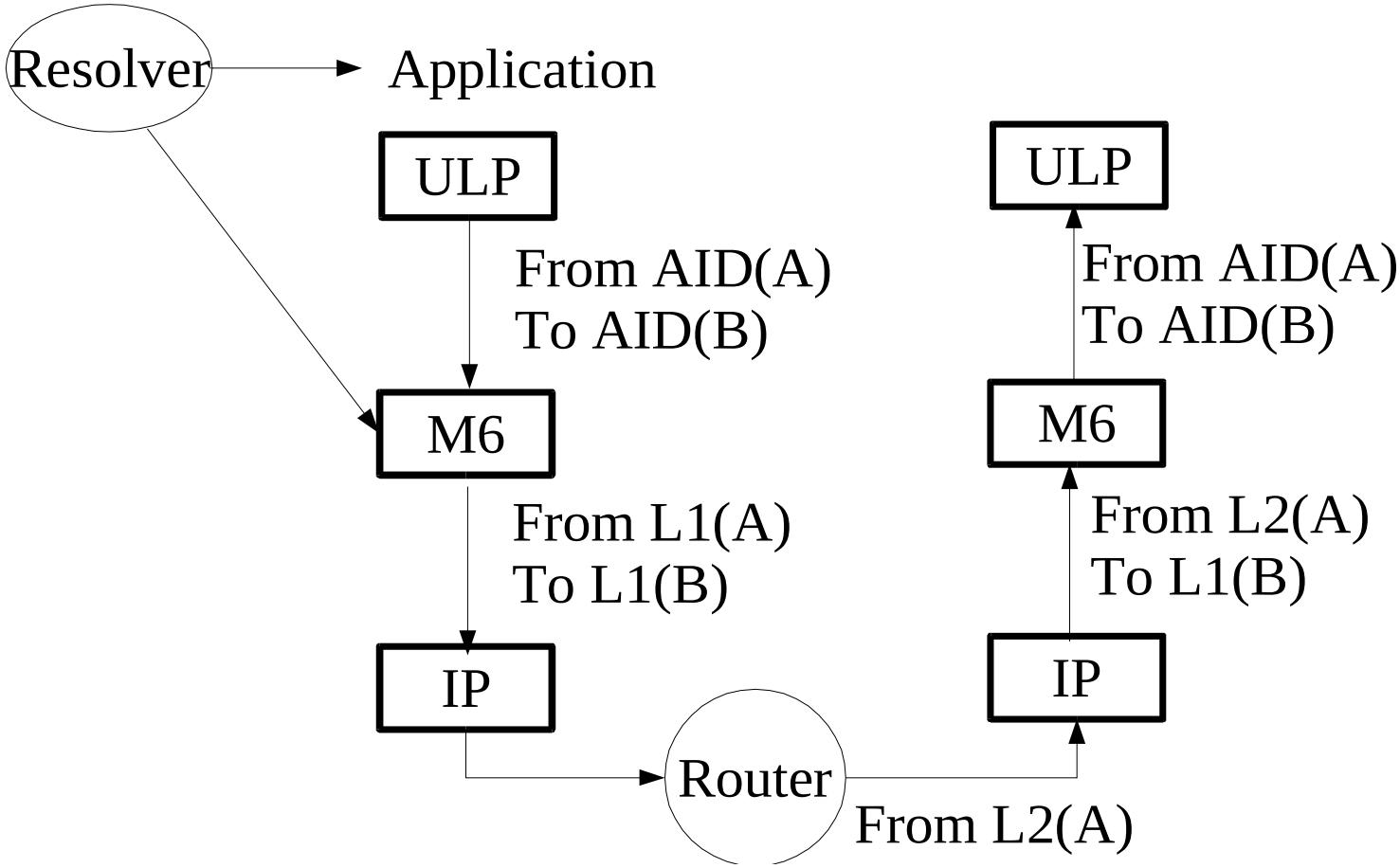
draft-nordmark-multi6-noid-01.txt
draft-nordmark-multi6-sim-01.txt
www.muada.com/drafts/draft-nordmark-multi6-cb64

Design Team Members (alphabetical order):
Iljitsch van Beijnum, Steve Bellovin, Brian Carpenter, Mike O'Dell, Sean Doran, Dave Katz, Tony Li, Erik Nordmark, and Pekka Savola

Commonality for NOID, SIM, CB64

- New shim layer between ULPs and IP layer
  - Actually below fragmentation, AH, ESP, destination options
  - Conceptually IPv6 extension header
- Application/ULP uses an ID – stable for a session or longer; we call this the AID
- Multihoming uses different locators over time
- Rewriting of source locators to detect changes
  - Returning packets to last received source locator
- Initiator uses DNS as today - more info retrieved

Common model



NOID concepts

- NO identifier in any packets
  - FQDN is what actually identifies a node
  - Set of locators are used on the wire
- ULP uses a single locator during communication
  - Different connections can use different locators for load spreading
- Shim layer can use different locators on the wire
  - Shim layer replaces AIDs by locators on xmit and the inverse on receipt
  - Receiver needs to find replacement state – context tag

NOID – DNS

- DNS reverse+forward used to prevent redirection attacks
  - That provides the locator set for a FQDN
  - Nodes in multihomed sites need FQDNs and reverse tree entry
  - Otherwise can only benefit from the peer being multihomed; not itself being multihomed
- DNS has locators in AAAA records plus new “M6-capable” RR type with no RDATA

NOID packet formats

- No packet overhead for data packets
  - Using flowid plus nextheader values (see draft)
- Conceptually an extension header
  - Its conceptual precence says sender is M6 aware
  - Contains a context tag to indicate replacement context
  - Contain a “rewrite ok” bit for routers
- New (ICMPv6) packets for handshake
  - Context request, reply, confirm
  - Unknown context error

NOID – walkthrogh (1)

- Client looks up AAAA and “M6 capable” in DNS
  - Verifies reverse lookup locators->FQDN
- ULP sends packet; M6 creates state with flowid
- Receiver doesn't find state for locators + flowid
  - Pass to ULP; locators not rewritten by routers
  - Don't create state
  - Send context request message
- 3-way context message exchange provides flow labels to both ends (one flow label for each direction)

NOID – walkthrogh (2)

- After 3-way context message exchange responder can start verifying locators
  - Reverse lookup AID to get FQDN
  - Lookup FQDN to get locator set (AAAA RR set)
  - Reverse lookup each locator before it is used to send packets (prevent 3rd party DoS)
- Once the locator set is known, host can accept received packet from any locator in set
- Send to last received source locator (if verified)

NOID Basic capabilities

3.1.1 Redundancy	Yes, on top of routing
3.1.2 Load Sharing	Yes, per “connection”
3.1.3 Performance	Using BGP
3.1.4 Policy	Border router locator rewriting
3.1.5 Simplicity	Sure
3.1.6 Transport Survivability	Failover during “connections” Timeliness?
3.1.7 Impact on DNS	New “M6 capable” RR type
3.1.8 Packet Filtering	In addition, locator rewriting

NOID Additional capabilities

3.2.1 Scalability	No more routes in DFZ
3.2.2 Impact on Routers	Optional locator rewriting
3.2.3 Impact on Hosts	Compatible
3.2.4 Host-Routing interaction	Locator rewriting plus existing prefix deprecation
3.2.5 Operations & Management	Sure
3.2.6 Cooperation between Transit Providers	Need correct exit when not “rewrite ok”
3.2.7 Multiple Solutions?	What?
4 Security Considerations	multi6-threats-00.txt

SIM concepts

- 128 bit identifier which is a hash of a public key
  - Akin to identifier used in HIP; stable over time
  - Hosts create these autonomously
- ULPs uses the above identifiers
  - API can handle ID as well as current IP addresses
- Shim layer maps between the ID and the locators used on the wire
  - Shim layer replaces IDs by locators on xmit and the inverse on receipt
  - Receiver needs to find replacement state – context tag

SIM – Public Key

- DNS has locators in AAAA records plus new ID RR type which contains the identifier
- Public key crypto to prevent redirection attacks
  - Similar to CGA technique in SEND WG
  - Does not require a PKI of any sort
  - Not needed until locators change
    - Perhaps possible to avoid it in that case as well
  - Best case: needed only when two nodes claim the same ID

SIM packet formats

- A new M6 extension header for data packets
  - Two nexthdr values; one means “rewrite ok”
  - Precence of ext header says sender is M6 aware
  - Contains a 32 to 40-bit context tag
  - Checksum + nexthdr value
- New (ICMPv6 or M6?) packets for handshake
  - Context request, reply, confirm
  - Challenge request and response
  - Unknown context error

SIM – walkthrogh (1)

- Client looks up AAAA and ID in DNS
  - Checks that ID used with one set of locators
- ULP sends packet to M6 layer
  - Triggers context creation exchange
  - Sender picks its context tag
- 3-way context message exchange establishes context state at both ends
  - ID + locator sets, context tags allocated by receiver
  - Locators are not yet verified (except the ones used to establish the communication)

SIM – walkthrogh (2)

- Find context using only context tag – no locator
- After 3-way context message learn and verify locators
  - When new locator arrives in source address field
  - Trigger challenge request/response exchange
  - In draft this involves public key signatures
- Send to last received source locator (if verified)
- Beyond draft:
  - Explicitly exchange list of locators up front
  - Weaker verification based on hash chains possible

SIM Basic capabilities

3.1.1 Redundancy	Yes, on top of routing
3.1.2 Load Sharing	Yes, per “connection”
3.1.3 Performance	Using BGP
3.1.4 Policy	Border router locator rewriting
3.1.5 Simplicity	Sure
3.1.6 Transport Survivability	Failover during “connections” Timeliness?
3.1.7 Impact on DNS	New ID RR type
3.1.8 Packet Filtering	In addition, locator rewriting

SIM Additional capabilities

3.2.1 Scalability	No more routes in DFZ
3.2.2 Impact on Routers	Optional locator rewriting
3.2.3 Impact on Hosts	Compatible
3.2.4 Host-Routing interaction	Locator rewriting plus existing prefix deprecation
3.2.5 Operations & Management	Sure
3.2.6 Cooperation between Transit Providers	Need correct exit when not “rewrite ok” - always set?
3.2.7 Multiple Solutions?	What?
4 Security Considerations	multi6-threats-00.txt

CB64

- Draft didn't make it to I-D directory in time
- Middle ground between NOID and SIM
- IP addresses with 64 bit hash of public key
- Public key, as in SIM approach, is used to prevent redirection attacks
- Otherwise the NOID approach is taken
- Note: IP addresses containing 64 bit hashes of public keys might be covered by IPR

High-level choices

- Introduce a new ID namespace as in SIM/HIP?
  - Or use multiple addresses?
  - Or some notion of designated addresses plus more short-lived ones?
  - This relates to what applications might want to see
- Using DNS (or some other 3rd party infrastructure) for verification?
  - Or public key crypto?
  - Or emphemeral Ids with no proof who “owns” an ID?
  - Able to use locators not in the DNS? Local locators?