SHIM6 Protocol Drafts Overview

Geoff Huston, Marcelo Bagnulo, Erik Nordmark

The Multi6 Problem

- how to support IPv6 end-site configurations that have multiple external connections to support application-level session resiliency across connectivity failure events

- how to use IPv6 multi-addressing and connection-based address aggregates to avoid overloading the routing system with site-based specific address advertisements

The SHIM6 Approach

- host-based solution
  (rather than host / router interaction)
- network layer approach – per host pair
  (rather than transport – per session)
- discoverable negotiated capability
  (rather than a new protocol service)
- no new identifier space

Shim6

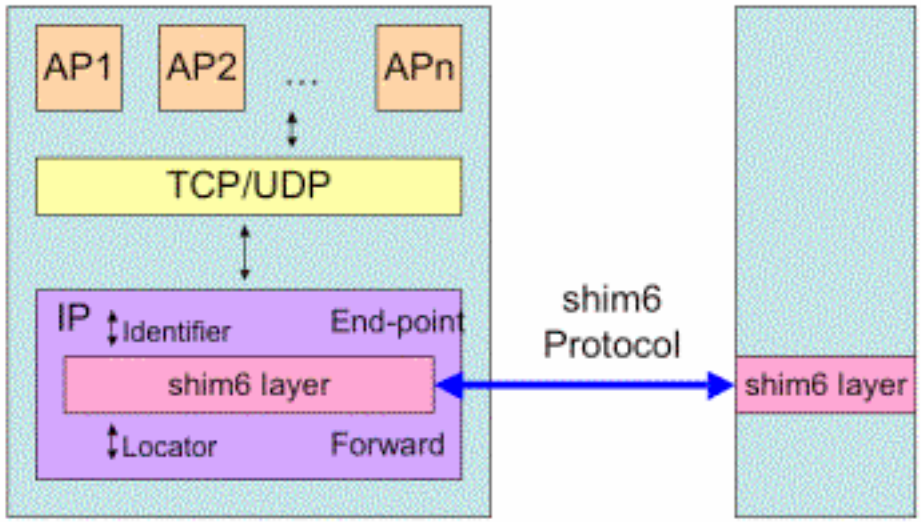
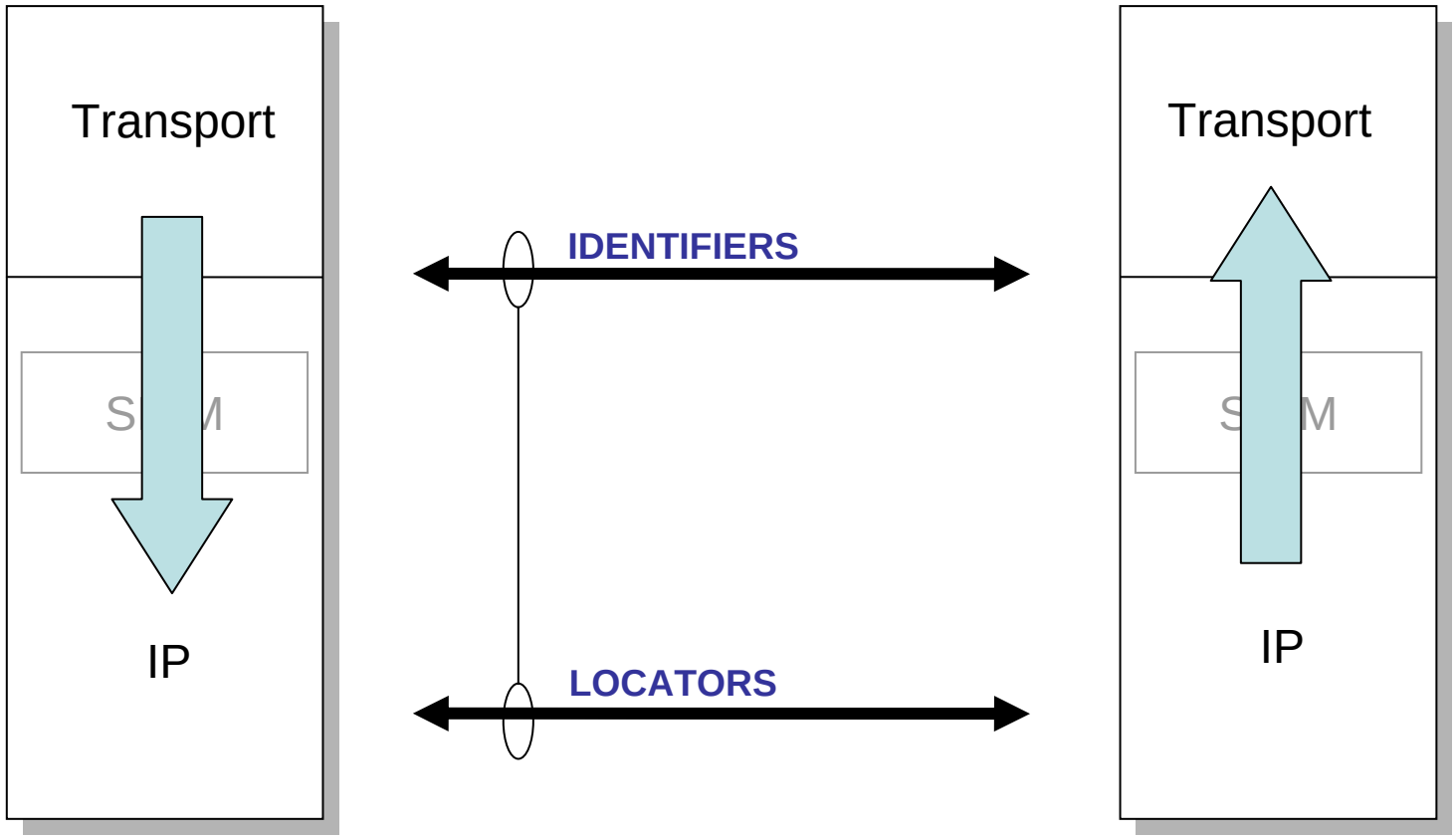


Figure 1: shim6 architecture

From http://www.shim6.org

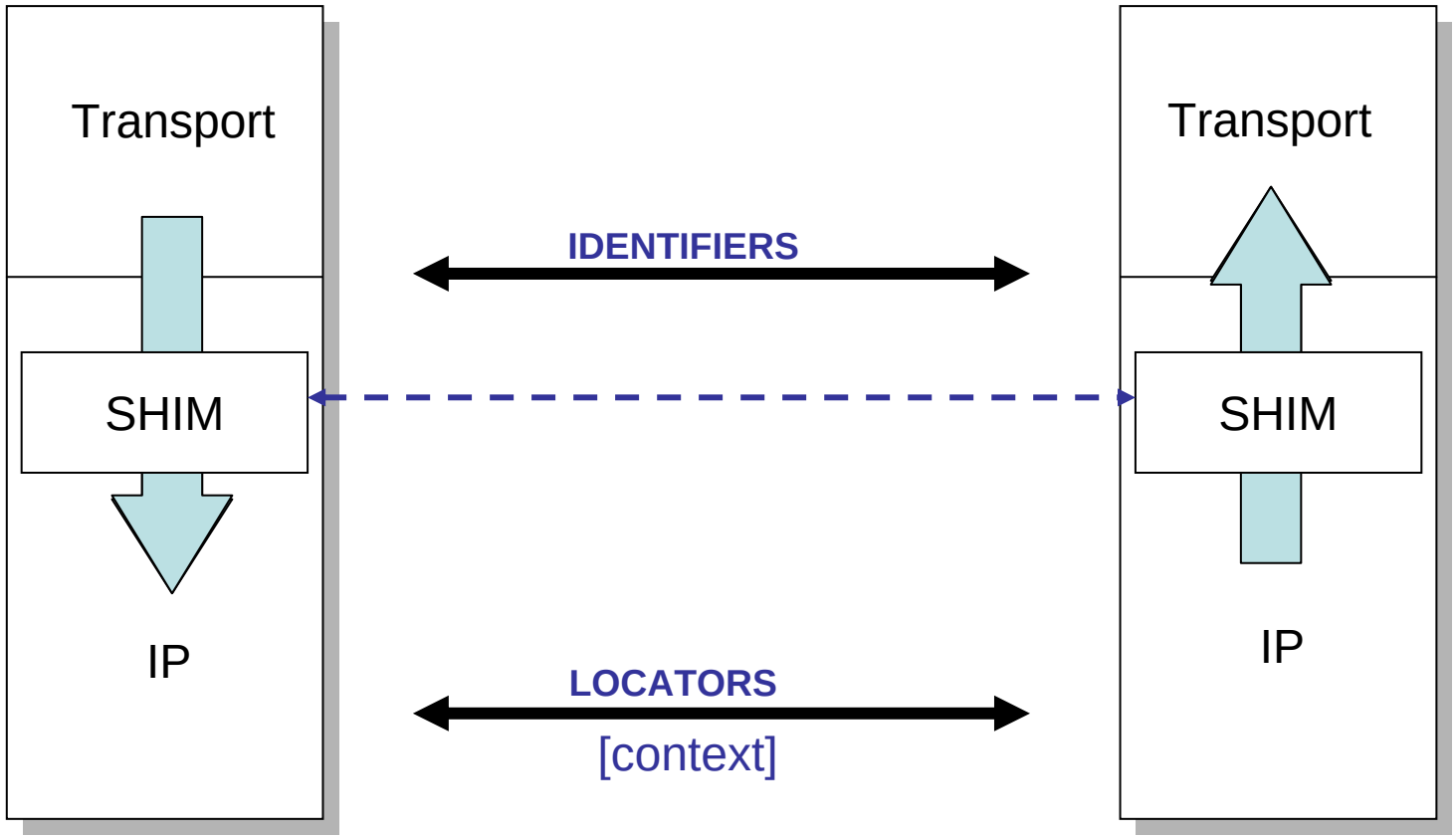
Initial Contact

No SHIM state active
Locator Selection using RFC3484
Locators and Identifiers are Equivalent



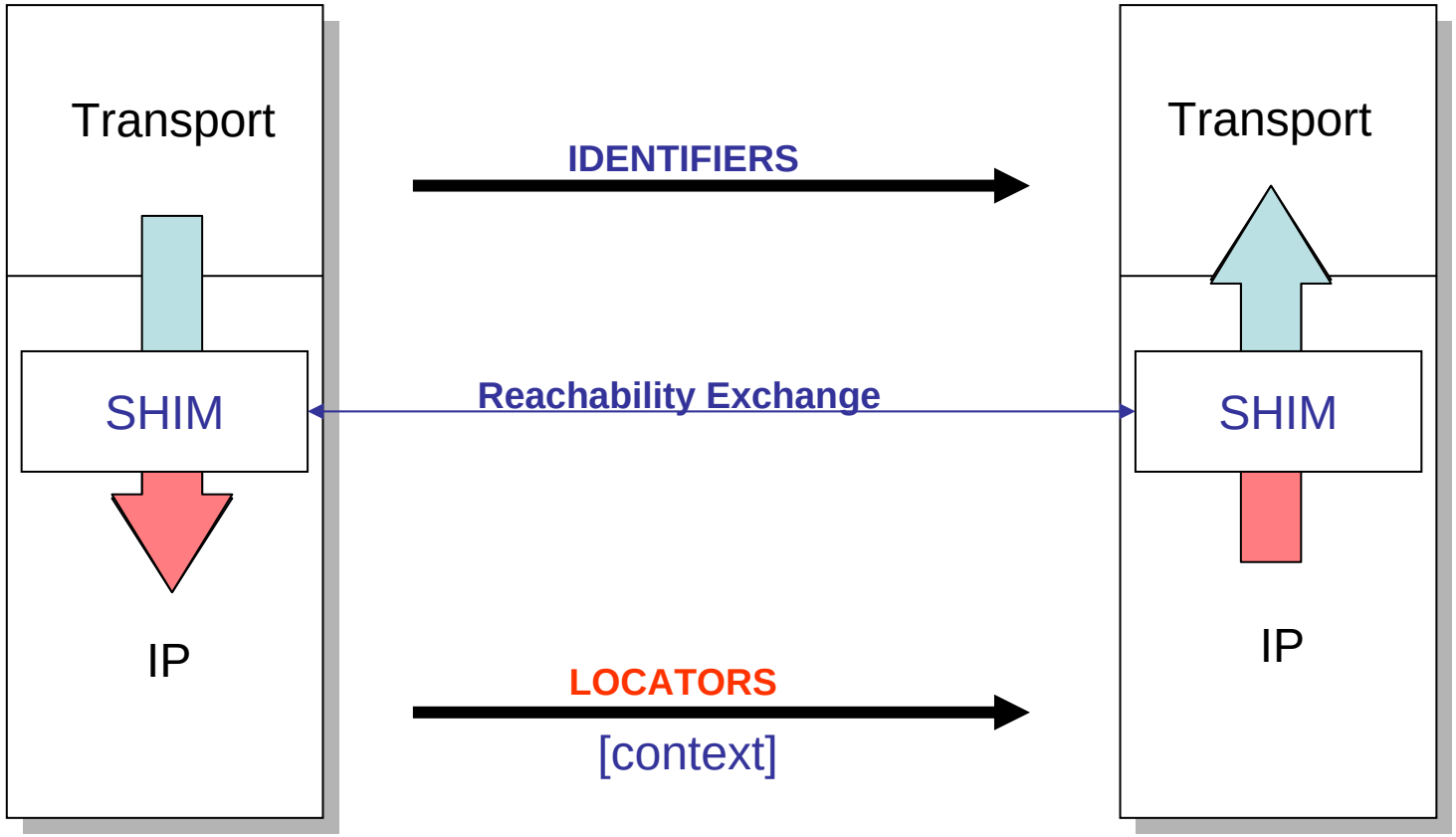
SHIM6 Activation

SHIM active
Current Locator Sets exchanged
Locators and Identifiers are Equivalent



SHIM6 Locator Failure and Recovery

Detect locator failure
Explore for functioning locator pair
Use new locator pair – preserve identifier pair



SHIM6 Control Elements

- initial handshake (4-way) and locator set exchange
- locator list updates
- explicit locator switch request
- keepalive
- reachability probe exchange
- No-Context error exchange

SHIM6 Proto Issues

- Interaction with IPSEC BITW
  - Case where IPSEC is applied at the interface
  - Solution: implement part of shim6 proto in the BITW
- Is this an extension to SHIM6 decoders allowing variable Shim6 / IPsec header processing depending on header ordering?
  - It is possible to put shim6 on top of IPSec, maybe suboptimal (IKE for each locator pair)
    - IPSec Transport mode vs. IPSec Tunnel mode
    - This is not IPSec security for shim6 signalling

SHIM6 Proto Issues

- Provide shim6 security based on IPSec SAs
  - Option 1: use certificates with ULIDs in them
    - How do you issue this certificates
      - Address autoconf, DHCP,
    - Revocation
  - Option 2: use pre-existent IPSec trust relationships
    - Still need to change IPSec so that SAs are dynamically created when a locator pair changes
    - This is functionally what mobike does…

SHIM6 Proto Issues

- Support for multiple ULID security mechanisms
  - Already have HBA, CGA HBA/CGA hybrids
  - Is the protocol spec already sufficiently modular wrt ULID security?
  - Do we need to support other security mechanisms
    - DNS
    - SSL certificates
  - Do we need to support different security for client and server?
  - Do we need error messages to express no support for a sec mechanism? See key length section…
- DoS attacks based on exhausting the 2^47 context tag space
  - Would the 4-way handshake enough to protect this?

SHIM6 Proto Issues

- About forking
  - The whole point of shim6 is to make locator transparent to ULP, then why forking?
  - Examples of apps using forking
  - Transport Area AD request for support for different transports
- Allowing a shim6 host to continue using a renumbered prefix may create confusion and security issues
  - Proposal: remove recommendation about keeping shim6 context even if the prefix was renumbered
- Shim6 protocol should define minimum CGA key length?
  - What would be the minimum length?
  - Do we need to define an error message for different security mechanisms/key lengths? Currently ICMP parameter problem in the UPDATE case and silent discard in I2/R2 case
- Define the BROKEN flag

SHIM6 HBA Issues

- IPR Concerns
  - IPR statements on CGA with potential HBA relevance have been clarified to the WG
- Use of protocol structures that are compatible with CGA
  - Is this acceptable to the WG?
- IANA Considerations
  - Is “CGA Extension Type” a new IANA registry?
    - RFC 4581 creates the CGA Extension type registry
- Security Considerations
  - Is the “Interaction with ISPEC” section finished?
  - Is the “SHA-1 Dependency” section finished?
    - draft-bagnulo-multiple-hash-cga-00
- SECDIR review: added motivation, overview and threat model section
- Other Issues?

SHIM6 Failure Detection Issues

- Have all the identified issues been addresses in the -06 version of this draft?

Shim6 WG Last Call

- Is the WG ready to pass these 3 base drafts to the IESG for publication as Proposed Standard?