

# XIA: An Evolvable, Expressive, and Secure Internet Architecture

## Multiple Principal Communication Types

### What is a principal type?

A principal type is a set of identifiers and the semantics of communicating with one of these IDs. Specific semantics allow endpoints to directly express the *intent* of a packet. Varying semantics are achieved through type-specific *per-hop processing*.

### Example Principal Types

We introduce the host, service, and content principals. New types can be added in the future to provide native network support for new modes of communication, making XIA networks *evolvable*.



Host



Service  
e.g., search



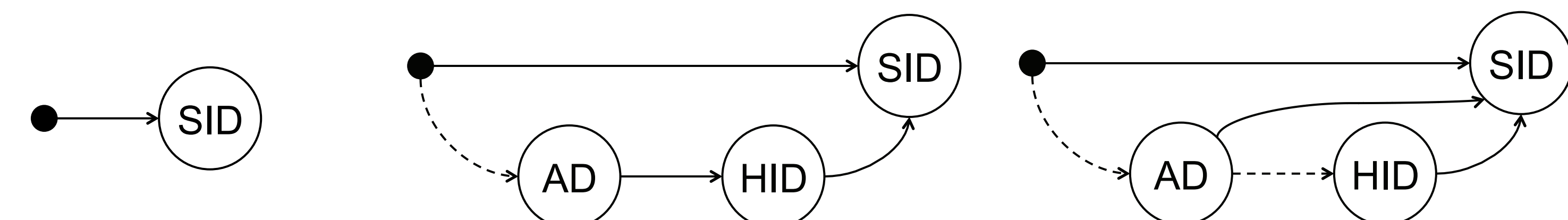
Content  
e.g., a photo

## Flexible Addressing

Addresses in XIA are represented as *directed acyclic graphs* (DAGs), which allows for graceful implementations of mechanisms like *fallbacks*, *iterative refinement*, and *session binding*.

### Example: Fallbacks and Iterative Refinement

- Provide *backwards compatible* paths
- Facilitate *endpoint evolution*
- Allow *incremental deployment* in the network



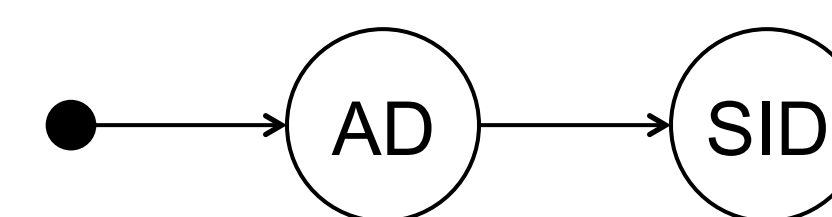
**A Simple DAG.** This simple DAG expresses only the sender's primary intent: to send a message to a service with ID 'SID.'

**Fallback.** The primary intent is still to route to SID, but if a router doesn't support services, it can fall back to AD and host-based routing.

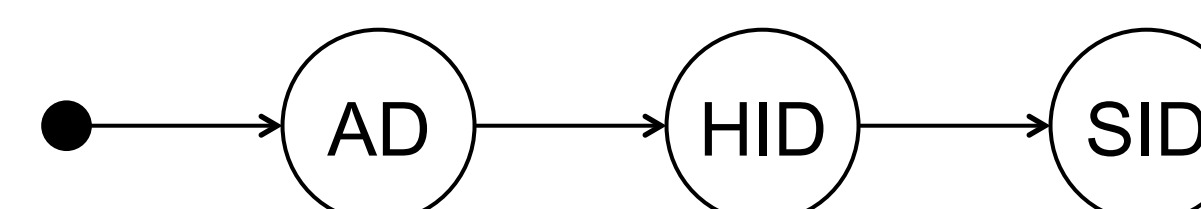
**Iterative Refinement.** Now any node can route directly to the final intent if able, but otherwise falls back to AD or HID.

### Example: Session Binding

Some communication sessions must be bound to a particular server (e.g., an online banking session).



The initial packet in such a session might be destined to any node providing service SID.



The node replies with a bound source address specifying which host serviced the request, to which the client sends all subsequent packets.

## Intrinsically Secure Identifiers

- IP is hard to secure, as security was not a first-order consideration in its design
- XIA aims to build into the architecture a means for bootstrapping secure communication
- The exact meaning of "secure communication" varies by principal type



#### Hosts

Host IDs (HIDs) are the hash of a host's public key

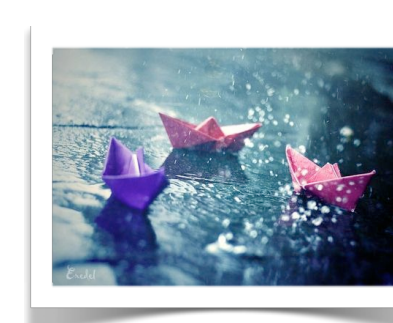
$$\text{HID} = \text{hash}(\text{PUB})$$



#### Services

Service IDs (SIDs) are the hash of a certifying authority's public key

$$\text{SID} = \text{hash}(\text{CERT})$$



#### Content

Content IDs (CIDs) are the hash of the content itself

$$\text{CID} = \text{hash}(\text{Content})$$

A prototype implementation of XIA is publicly available at [www.cs.cmu.edu/~xia](http://www.cs.cmu.edu/~xia)