An Architecture for Open Pluggable Edge Services (OPES)
draft-ietf-opes-architecture-02

Abbie Barbir   abbieb@nortelnetworks.com

Robin Chen   chen@research.att.com

Markus Hofmann   hofmann@bell-labs.com
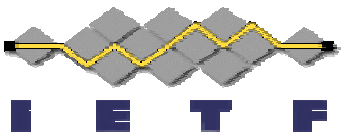
Hilarie Orman   ho@alum.mit.edu

Reinaldo Penno   rpenno@nortelnetworks.com

1

An Architecture for Open Pluggable Edge Services (OPES)
Summary

- **Presents architectural components**

- **Discuss IAB considerations**

  - **Trust, Security, tracing, etc..**

- **Issues**

- **Q&A**

draft-ietf-opes-architecture-02
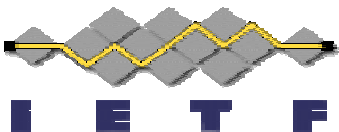
OPES Architecture

1. OPES Entities

- Applications that operates on a data flow between a data provider application and a data consumer application
  - A data dispatcher, which invokes an OPES service application based on OPES ruleset and application-specific knowledge

2. OPES Flows

- Cooperative undertaking between a data provider application, a data consumer application, zero or more OPES service applications, and zero or more data dispatchers
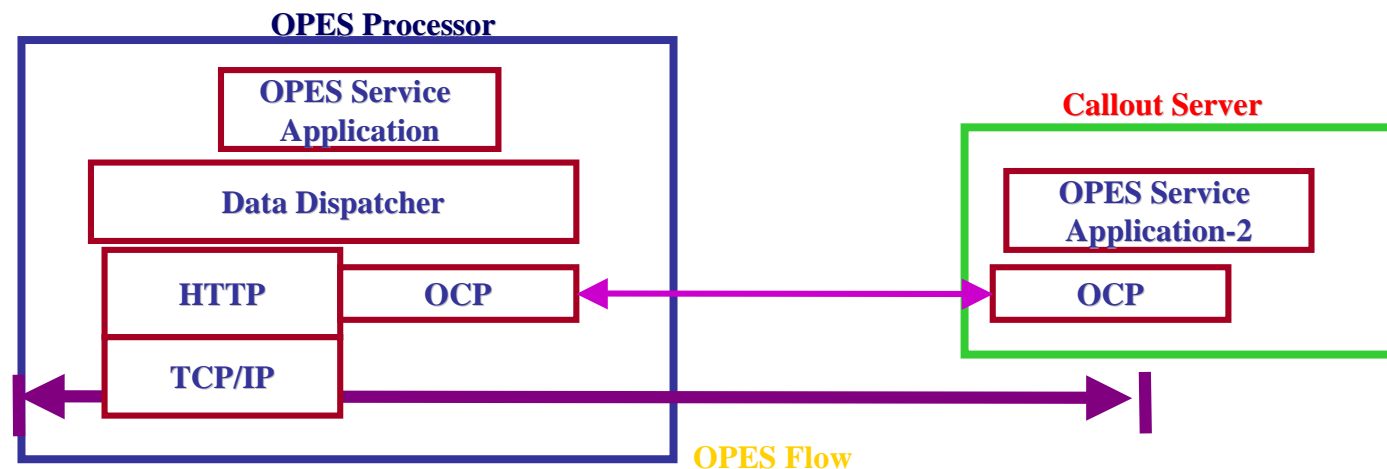
3. OPES Rules

- Determines which service applications will operate on a data stream
- All data filters are invoked for all data
- May invoke the services of Callout Servers

OPES Logical Implementation
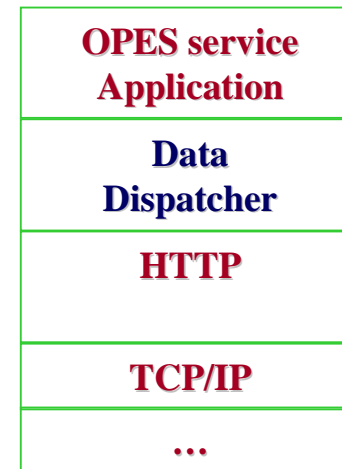
- **Architecture is independent of the protocol that is used by the OPES entities to exchange data**
  - **HTTP is the current example protocol to be used for realizing a data flow**

OPES service Application
Data Dispatcher
HTTP
TCP/IP
...

OPES Processor

OPES Service Application
Data Dispatcher

HTTP	OCP
TCP/IP	

Callout Server

OPES Service Application-2
OCP

OPES Flow

Interaction of OPES Entities

draft-ietf-opes-architecture-02

4

I E T F
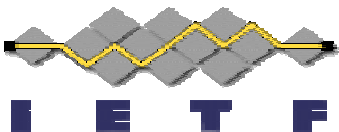
IAB Considerations

Addressed through various aspects of the architecture

Tracing Facility

- **in-band annotation**
- **Relation to IAB considerations**
  - **(3.1) Notification**
    - **May need Separate Document**
  - **(3.3) Non-blocking, (4.1) URI resolution, (4.2) Reference validity**

Security and Privacy Considerations

Trust Domains

- **Appropriate delegation of authority**
- **Callout protocol**
- **Various delegated Trust models**
- **Privacy**
- **Must advise primary parties of privacy policy and respect the policies of the primary parties**
- **End-to-end Integrity**
- **May use Digital signature techniques to allow third-party to verify**
- **Relation to IAB considerations**
  - **(3.1) Notification, (3.3) Non-blocking**
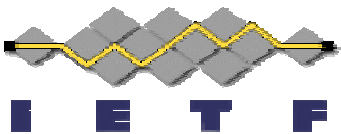 - **(4.2) Reference validity, (5.1) Privacy**
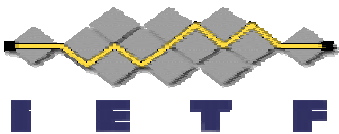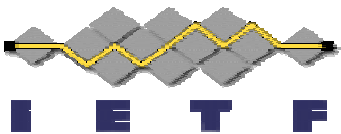
Issues

- **From the list**
  - **Agreed that architecture should allow for**
    - **Notification**
    - **tracing and**
    - **access to diagnostics**
  - **In-band versus out of band discussion**
  - **Details of how to achieve that in another draft**
- **No major issues with the architecture at this time**
- **Need to issue last call soon**
- **Provide feedback ASAP**
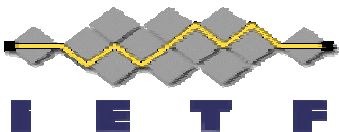
Q&A

Backup

IAB Considerations

Main IAB Issues

(2.1) One-party consent

- An OPES framework standardized in the IETF must require that the use of any OPES service be explicitly authorized by one of the application-layer end-hosts (that is, either the content provider or the client)

(2.2) IP-layer communications

- For an OPES framework standardized in the IETF, the OPES intermediary must be explicitly addressed at the IP layer by the end user

(3.1) Notification

- The overall OPES framework needs to assist content providers in detecting and responding to client-centric actions by OPES intermediaries that are deemed inappropriate by the content provider.

(3.2) Notification

- The overall OPES framework should assist end users in detecting the behavior of OPES intermediaries, potentially allowing them to identify imperfect or compromised intermediaries.

(3.3) Non-blocking

- If there exists a "non-OPES" version of content available from the content provider, the OPES architecture must not prevent users from retrieving this non-OPES" version from the content provider.
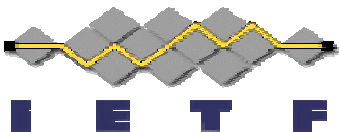
IAB Considerations

Main IAB Issues

(4.1) URI resolution

- OPES documentation must be clear in describing these services as being applied to the result of URI resolution, not as URI resolution itself.

(4.2) Reference validity

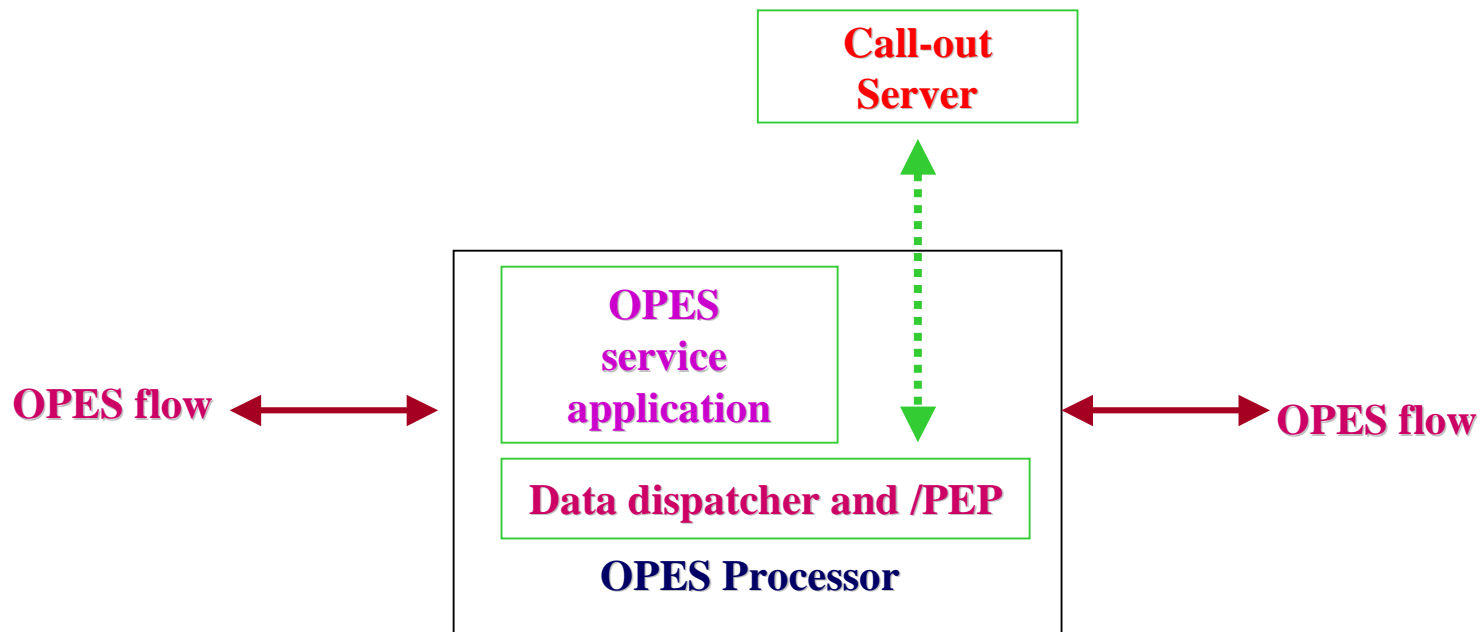- All proposed services must define their impact on inter- and intra-document reference validity

(4.3) Any services that cannot be achieved while respecting the above two considerations may be reviewed as potential requirements for Internet application addressing architecture extensions, but must not be undertaken as ad hoc fixes.

(5.1) Privacy

- The overall OPES framework must provide for mechanisms for end users to determine the privacy policies of OPES intermediaries.
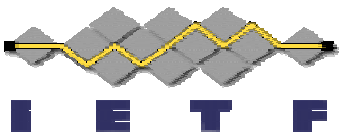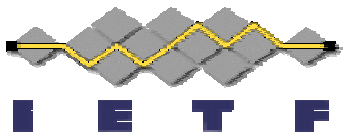
Data Dispatcher Logical View

Call-out
Server

OPES flow

OPES
service
application

Data dispatcher and /PEP

OPES Processor

OPES flow

I E T F

An OPES flow

Consumer administrative domain

Provider administrative domain

Data Consumer

OPES Processor

OPES Processor

Data Provider

Data Consumer Application
HTTP
TCP/IP

OPES Service Application
HTTP
TCP/IP

OPES Service Application
HTTP
TCP/IP

Data Provider Application
HTTP
TCP/IP

OPES Flow

I E T F
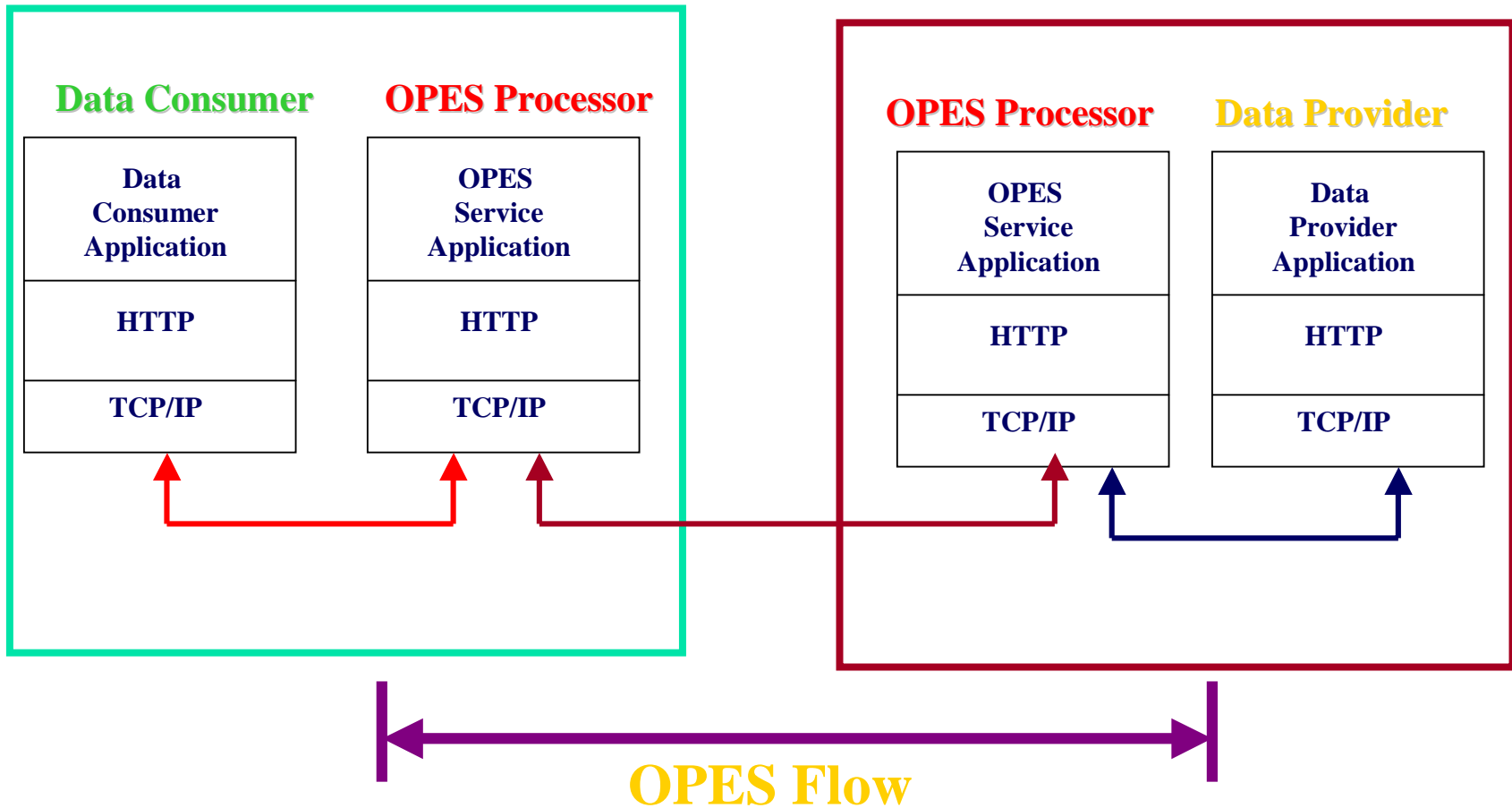
An OPES flow with Callout servers

Data Dispatcher

Callout Server

Callout Server

OPES Callout Server Protocol OCP
Lower Layers Protocols
…..

OPES Callout Server Protocol OCP
Lower Layers Protocols
…

OPES Callout Server Protocol OCP
Lower Layers Protocols
…
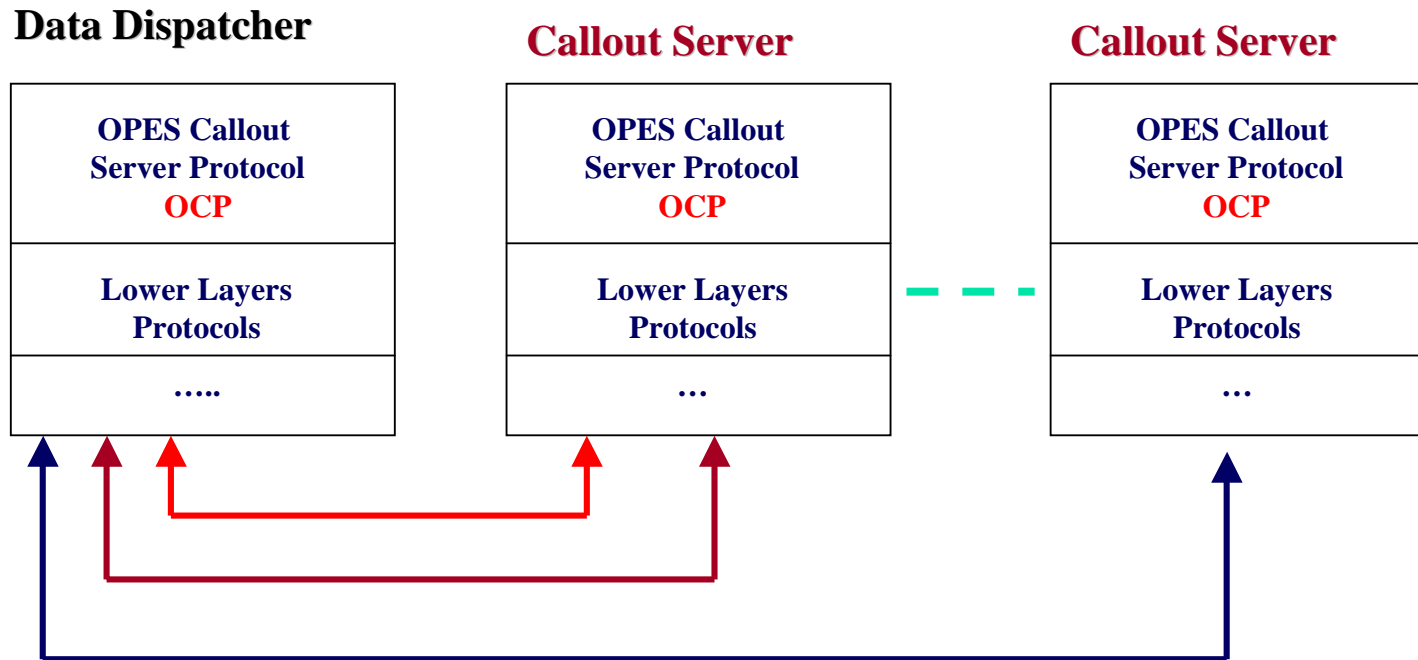
OCP is application-agnostic
- **Unaware of the semantics of the encapsulated application protocol**
  - **Must incorporate a service aware vectoring capability**
  - **Parses the data flow according to the ruleset and**
- **Delivers the data to the OPES service application that can be local or remote**

draft-ietf-opes-architecture-02