IAB Architectural and Policy Considerations for OPES

Edited by: Sally Floyd and Leslie Daigle

OPES BOF
December 10, 2001
Salt Lake City IETF

The IAB document on OPES:

- It is a recommendation to the IESG.

- If the IESG accepts an OPES charter referring to the IAB draft, then the individuals working on OPES have to address the issues in the draft in their work.

- The IAB draft does not have answers, it mostly describes issues that should be addressed.

- Somewhat like ”Security Considerations”: the WG has to convincing argue that the issues have been addressed, and this will be considered when a document comes up for IESG Last Call.

Related past work in the IETF:

- RFC 3135: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations

- RFC 3135 has sections on:
Security Implications, Fate Sharing, End-to-end Reliability,
End-to-end Failure Diagnostics, Asymmetric Routing,
Mobile Hosts, Scalability, and Other Implications of Using PEPs.

- “we believe that ... PEPs should be used only in specific environments and circumstances where end-to-end mechanisms providing similar performance enhancements are not available.”

- “the choice of employing PEP functionality should be under the control of the end user ...”

IAB Considerations for OPES:

(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.

IAB Considerations for OPES:

(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.

IAB Considerations for OPES:

(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 for OPES:

(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.

IAB Considerations for OPES:

(5.1) **Privacy**: The overall OPES framework must provide for mechanisms for end users to determine the privacy policies of OPES intermediaries.

[This does not mean that the mechanisms for this would be developed in the OPES WG, or even in the IETF.]

The IAB Plenary on Thursday

- A more general discussion of the architectural issues.