IAB
Architectural Consideration for OPES

Abbie Barbir abbieb@nortelnetworks.com

Design Team

IAB consideration (RFC 3238)

Brief Review of Some Issue

IP-layer communications

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

- Make that mandatory (first HOP)
  - How about NAT/Firewall issues
- Do we need to consider chained
  - OPES intermediaries
  - Callout Servers

IAB consideration (RFC 3238)

Data integrity with client-centric OPES services on responses

Notification

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

Tracing and Error detection

- Our interpretation is that OPES services should, in so far as possible, make it easy to debug problems

- We defined explicit transformation notification as consisting of two parts:

1. “via headers” to include OPES intermediaries and callout servers
2. Comments or embedded naming conventions with the meaning “OPES service A transformed this element"

- We ruled out automated semantic error detection,
  - e.g., checking images for damage by broken compression methods, malformed tags, etc.

Open Issues

- How can an origin server be made aware/trace errors caused by an OPES intermediary, and
- How can an origin server specify bypass of OPES services?
- How can the OPES architecture not prevent users from retrieving "non-OPES" version from the content provider?
- For example, an OPES intermediary might insert a reference to an image into an HTML page;
  - if it get the URL wrong, who will get notified about the error and how will they trace it to the faulty intermediary?
- **Basically, we need input/help**

Possible Approaches

1. HTTP Extensions
   - Nasty (Yuk …Not Again…)
2. Special OPES Headers in HTTP
   - Less Nasty ???????
3. Authoring Tool
4. Separate OPES Signaling Protocol
5. Try W3C for Error Reporting
6. Give UP …….

The architecture document

1. It needs substantial revision to include
   - content path "traceroute",
   - HTTP “via header” extensions,
   - error notifications,
   - bypass provisions,
   - confidentiality and integrity

2. We need volunteers who have time to discuss and review the architecture

Q&A