

# CDNI Framework

B. Davie, L. Peterson et al.



# Objective of Framework

- ▶ Address the question “how do all the pieces fit together?”
  - Think of a frame providing the structure to which the other pieces get attached
  - Describes how all the CDNI components and additional out-of-scope components (e.g. inter CDN acquisition, request interface) combine to deliver full CDNI solution



# Objective of Framework (2)

- ▶ Illustrate key design tradeoffs
  - E.g. HTTP- versus DNS-based redirection
  - E.g. Recursive versus iterative request routing
- ▶ Leave details of interface specifications (Request Routing, Control, Metadata, Logging) to other documents

# Message Flow examples

- ▶ Series of examples to illustrate:
  - The “big picture” of how operations proceed to distribute content, metadata and control information
  - The key information that needs to be exchanged
  - Different request routing styles, including recursive and iterative
  - Various ways the Request Routing, Metadata and Control interfaces may be used
  - How certain agreements/conventions between providers may assist interoperation
    - E.g. naming conventions for acquisition nodes
- ▶ Not prescriptive
  - Next rev will clarify this and draw conclusions from examples

# Message Flow Details

- ▶ Read the draft :-)
- ▶ It's been noted that we have a lot of detail on domain names, DNS operation, and HTTP redirection
- ▶ The names illustrate the type of things that will either need to be configured or exchanged in protocols to be defined
- ▶ The use of DNS- and HTTP-based redirection needs to get documented somewhere
  - The request interface is “out of scope” for CDNI in the sense that no new mechanisms are to be defined


# Deployment Scenarios

- ▶ Illustration of how various deployments may be supported
  - Mesh of CDNs
  - CSP uses CDNI to interact with CDN(s)
  - CDN Exchange
- ▶ Not exhaustive
- ▶ Show some examples of useful subsetting of the CDNI interfaces

# Trust Model and Security Issues

- ▶ Identify trust & security issues that are **unique to interconnected** CDNs
- ▶ Key issue: (non-)transitivity of trust
  - CSP trusts uCDN who trusts dCDN but CSP doesn't trust dCDN
  - “Trust but verify” covers some cases
    - E.g. 3<sup>rd</sup> party monitoring of end-end performance
    - But, if problems are found, may be harder to pinpoint the culprit in a chain of CDNs
  - Detailed interface specs should tackle this
- ▶ Single CDN access control methods must also work in CDNI (e.g. URL signing)
- ▶ Avoiding open proxy behavior

# Next Steps (1)

- ▶ Add interface definitions
  - ▶ More discussion of design tradeoffs
    - e.g. what info belongs in which interface, etc.
  - ▶ Draw conclusions from the examples
    - e.g. point out where existing machinery already does job
  - ▶ More security considerations
  - ▶ Deal with all the mailing list comments
  - ▶ Say more about relationship to ALTO, choosing among multiple dCDN candidates
- 



# Next steps (2)

- ▶ Get another round of discussion on list
- ▶ Consider if next rev is a good candidate for the WG framework doc