APAM

IAB Strawman

Architectural Principles and Methods

(a.k.a. Apple Pie and Motherhood)

Brian E. Carpenter

CERN/IAB

July 1995

1. General Design Issues

1.1 There should be one, and only one, protocol at the Internet level (but perhaps two versions for an extended period during transition). There can be many protocols at other levels.

1.2 End-to-end functions can best be realised by end-to-end protocols. [End-To-End Arguments in System Design, J.H. Saltzer, D.P.Reed, D.D.Clark, ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288]

1.3 All designs must fit into the Internet security architecture.

1.4 All designs must scale readily to very many nodes per site and to many millions of sites.

1.5 Heterogeneity is inevitable and must be supported by design.

1.6 Keep it simple. When in doubt during design, choose the simplest solution.

1.7 Avoid options and parameters whenever possible. If there are several ways of doing the same thing, choose one. Any options and parameters should be configured or negotiated dynamically rather than manually.

1.8 Be strict when sending and tolerant when receiving. When in doubt, discard faulty input silently.

1.9 Be parsimonious with unsolicited packets, especially multicasts and broadcasts. (IPv6 eliminates broadcast by design.)

1.10 Circular dependencies must be avoided.

For example, routing should not depend on DNS.

1.11 Objects should be self decribing (include type and size). Only type codes and other magic numbers assigned by IANA may be used.

1.12 All specifications should use the same terminology and notation, and the same bit- and byte-order convention.

1.13 Running code before standardization.

2. Name and address issues

2.1 Avoid any design that requires addresses to be hard coded or stored on non-volatile storage (except of course where this is an essential requirement as in a name server or configuration server). In general, user applications should use names rather than addresses.

2.2 A single naming structure should be used.

2.3 All names should be case-independent???

2.4 Addresses must be unambiguous (unique within any scope where they may appear).

2.5 Upper layer protocols must be able to identify end-points unambiguously. (In practice this means that addresses must be the same at start and finish of transmission???)

3. External Issues

3.1 Prefer unpatented technology, but if the best technology is patented and is available to all at reasonable terms, then incorporation of patented technology is acceptable.

3.2 The existence of export controls on some aspects of Internet technology is only of secondary importance in choosing which technology to adopt into the standards.

3.3 Any implementation which does not include all of the required components cannot claim conformance with the standard.

3.4 Designs should be "internationally user-friendly"

4. Confidentiality and Authentication

4.1 Confidentiality and Authentication are Good Things

4.2 Confidentiality is the responsibility of end users and must be implemented in the protocols used by the end users. (I.e. users should not depend on the confidentiality of the carriers.)

4.3 Wherever a cryptographic algorithm is called for in a protocol, the protocol should be designed to permit alternative algorithms to be used.

4.4 In choosing algorithms, the algorithm should be one which is widely regarded as strong enough to serve the purpose.