DNMTT -- NASPI WG
Feb 20, 2013

An InterNut Looks at NASPInet

Bob Braden
USC Information Sciences Institute
Marina del Rey, CA

- Last month was the 30th anniversary of the Internet.
- Is the Internet experience relevant to the design of NASPInet?
- Needless re-inventing the wheel would be costly.

Internet Protocol Suite (IPS): Guiding Principles

1. Interoperability is essential
2. Don’t over-optimize
3. Keep it as simple as possible (but no simpler)
4. Obey End-to-End principle whenever possible
5. Use distributed control

1. Interoperability

- **Specify enough** (but not more) so two conforming implementations will interoperate correctly, out of the box.
  - Allow multiple vendors
  - Allow innovative implementations
- IETF Standardization rules: require at least 2 independent interoperable implementations.

… Interoperability

- Before you accept any NASPInet proposal: “show us the bits on the wire.”
- So vendor A and vendor B can interoperate with different implementations.
- Comment: exposure of final NASPInet design in the IETF might save a lot of trouble in the long run.

2. Don’t Over-optimize

- **Be willing to sacrifice some efficiency to gain flexibility & uniformity**
  - The problem will change
  - The technology will rapidly evolve
- *Eg “We can develop our own internetwork layer protocol that will be more efficient that IP [for our specific case].”*
  - **BAD IDEA!!**

NASPInet Example

- Two quite different NASPInet functions:
  1. Delivery of PMU data streams
  2. Closed loop control
- Could build two different NASPInets, one optimized for each function.
- *Probably* a BAD IDEA (but not certain).

3. Simplicity

- Simplicity ~ elegance in protocol design
- Complexity goes with:
  - ugliness
  - unmaintainability
  - non-interoperability
- Unfortunately, all protocols tend to accrete features … !

4. End-to-End Principle

- Converse of the telephone system --
  - Phones: smart network, dumb terminals
  - Internet: smart terminals, dumb network
- Dumb network adaptable to new applications
  - Minimal function in internetwork: => IP
  - No per-flow state in routers

… End-to-End Principle

- Those who would violate the E2E principle have to make a strong case in the IETF.
  - IP multicast violates E2E principle
  - RSVP and Integrated Service violate E2E principle
  - GridStat violates E2E principle

5. Distributed Control

- Avoid single points of failure
- Avoid implosion points

- Example:
  - GridStat does pub/sub centrally
  - IP MC, RSVP do pub/sub in distributed fashion

Untrue Rumors about the IPS

- IPS cannot stream real-time data
  - See VoIP, Skype
- IPS has no QoS mechanisms
  - See Diff Service, Integrated Service
- IPS cannot bound E2E latency
  - See Guaranteed Service under Int Serv
- IPS cannot do resource reservation
  - See RSVP

Fact: Limited deployment

- Backbone providers typically provide only basic best-effort service
- But some corporate intranets provide IP MC, diff-serv, int-serv, resource reservations, …

Some Common Fallacies

- The IPS* cannot stream real time data
  - Have you used Skype or VoIP lately?
- The IPS has no QoS provisions
  - See Differentiated Services, Integrated Services
- The IPS cannot provide bounded E2E delay
  - See Guaranteed Service under Integrated Services
- The Internet cannot do resource reservations
  - See RSVP

**Internet Protocol Suite*

Important Issues

In packet switching, important issues include:

- Naming and Addressing
- Congestion
- Fragmentation
    - Why aren't you worried about fragmentation?
- Buffering
- Store-and-forward delays

Naming and Addressing

- 61850 requires a 128 bit unique name for every hardware box.
- A new name space => questions
  - Who allocates names?
  - How partition bits for distributed allocation?
    - Suggest: Use convenient /n notation from IP addr
- Need new DNS-like directory service to map these hardware IDs to IP addresses.

- But if every box already has 128 bit unique IP address, do we really need a new name space at all?

NASPInet

- Will be a (more or less) crisply defined **subset of the Internet.**
  - Completely isolated network? Never happen --
  - "Backdoor" Internet connections inevitable.
- Built on Internet protocol suite (IPS):
  - IP at internetwork layer
  - Some transport protocol (UDP, TCP, SCTP …)
- That positions NASPInet in:
  - the Application layer (eg IP MC)
  -- or in middleware layer (eg GridStat)

The Isolation Myth

- "If we build a new network isolated from the Internet, we can get precisely the service we need and avoid many security problems"
- It never works
  - E.g., need Internet back doors for management, configuration, diagnosis, …
  - Even with only one 300 baud modem connection, bad guys can get in and take over.

Proposed NASPInet-P Architectures

- IP MC – Myrda et al
  - Network layer MC, TA* at dest
- Chained PDCs
  - App layer or network layer MC
  - TA at intermediate PDCs and dest
- GridStat -- Bakken et al
  - Middleware approach

**Time align*

- Can we choose one of these?
- *Must* we choose one?
- What input do we need to choose wisely?

Some Opinions

- We are underestimating the rapidity of evolution in communication software and hardware
  - Transformers can last 50 years, but specifying a 15 year lifetime for NASPInet seems foolish
- Should think of a PG as a set of functions, not as a device.
- PG currently has too many functions, is too complex, in fact.

More Opinions

- The “Data Bus” is an unfortunate and misleading metaphor. Should be cloud.

- Maybe we are underestimating the ability of application builders to accommodate lost/delayed data.
  - Buffering is cheap
  - Physical system has lots of inertia

Danger Areas for NASPInet

- NASPInet dynamics will be similar to Internet's
- Rapid technology change
- Changing problem space
  - See: "An Internet-Inspired Electricity Grid", IEEE Spectrum, 12-14, Jan 2013.
- Success disaster

Robust, Interoperable Implementation

- Postel Principle: “Be conservative in what you send and liberal in what you receive.” [RFC1122]

Thank You