

Applying the Lessons of Internet Services to Space Systems

James Cutler

*Space Systems Development Laboratory
Software Infrastructures Group
Stanford University*

GSAW 2002

■ Motivation

- Reducing missions operations costs
- Increasing mission yield and capabilities

■ Long term objectives

- Provide baseline satellite infrastructure to make science data *more accessible* and enable experiments to have *wider impact*
- Make this infrastructure *robust and affordable*

Primary Technical Approach:

- *A recovery-oriented COTS ground station*
- *Develop a loose federation of networked "virtual ground stations"*

Space Parallel: COTS and the Internet

- COTS *opportunities* are well known
 - Lower barriers to entry (rapid prototyping and standards)
 - Components ride the cost/performance curves
- Set against these are the *challenges* of COTS
 - Not designed for mission-critical applications
 - Complex behaviors, not always well known or understood
- Internet systems have some experience building reliable systems from unreliable parts:
 - RAID, Internet routing substrate (IP), Cluster-based Internet servers
- Similarities between space and Internet system:
 - Need for high reliability
 - Automatic management of transient failures
 - Rapid prototyping, short schedules, time pressure
- Key: *system-wide* availability, robustness, security

Internet services programmed with a "bunker mentality"

- Preserve fault isolation boundaries
 - Containment--exploit natural isolation boundaries to contain faults (clusters, virtual machines)
- Explicitly encapsulate state
 - Protection—all state in a well-known, protected place (HTTP)
- Separate data format from implementation
 - Versatility—data exchange is independent of transport (HTML over HTTP, WAP, etc.)
- Orthogonal checks and monitors
 - Reliability—component level and end-to-end checks
- Design for restartability
 - Recovery—improving availability through lower MTTR and rejuvenation

Recovery-Oriented Computing



- Our design philosophy is *recovery-oriented* computing (ROC)
 - ROC emphasizes *recovery* from failures rather than purely failure-avoidance

- Motivation—even the most robust systems still fail due to:
 - human operator error
 - transient or permanent hardware failure
 - software anomalies resulting from "Heisenbugs" or software aging

- ROC techniques
 - Redundancy—to mask failures
 - Small recovery units—to recover quickly
 - On-line testing—verify functionality and recovery mechanisms
 - System-aided diagnosis—reduce human operator latency/errors
 - Undo-able systems—roll back to recover from human errors

- Partnering with Prof David Patterson from U.C. Berkeley

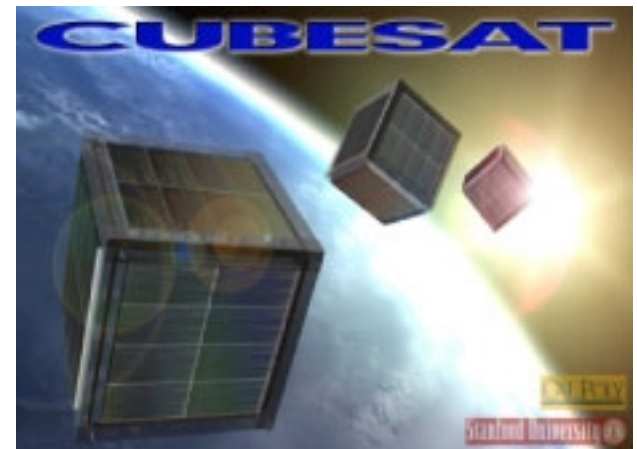
Examples of Our COTS Space Systems



- Global university ground stations built from amateur radio equipment
 - Linux/Windows commodity PCs
 - Data speeds $\leq 38.4\text{kbps}$
 - Cost $< \$10,000$

- Small satellite support of existing and future missions
 - Stanford's OPAL and Sapphire: 2+ years in orbit
 - University nanosatellite program
 - Cubesat program: 10-20 satellites a year

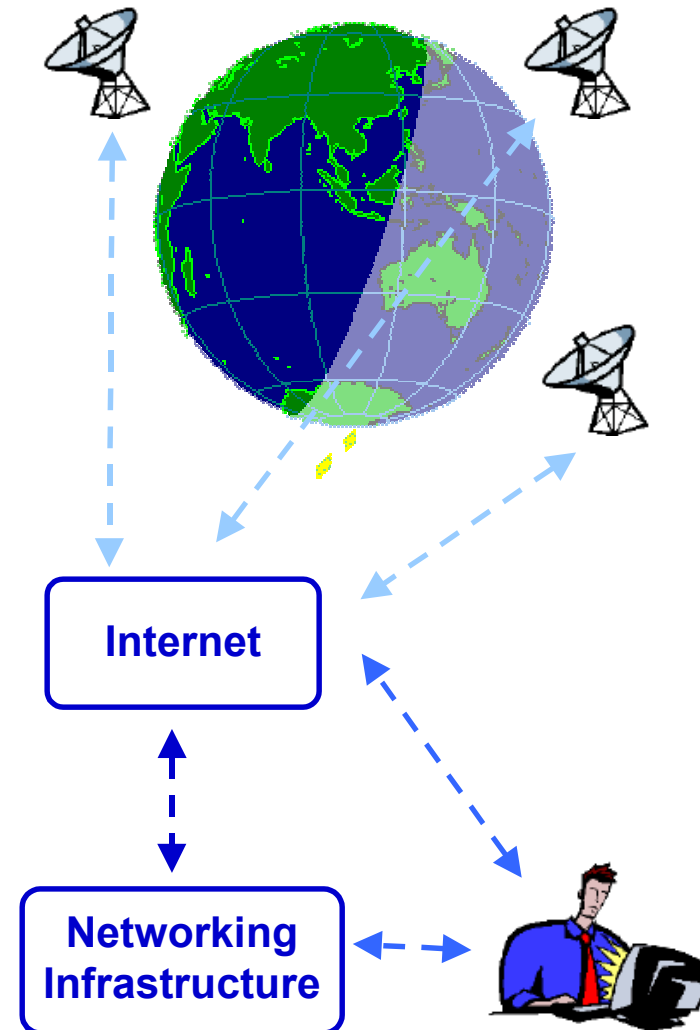
- Fertile research testbed
 - End-to-end IP accessible spacecraft
 - Software/DSP radios
 - Reconfigurable computing



Infrastructure: Federated Ground Station Network



- 100's or 1000's of ground stations in different administrative domains
- Facilities can dynamically join and leave the federation
 - Collection of autonomous entities
- Ability to designate subset of GS's as a "team"
 - team collaboratively solves a high-level task (e.g. "track this spacecraft")
 - path and node redundancy within team to deal with partial failures
- team and individual nodes addressable as "virtual GS"
 - Today: IP-based access to GS's and spacecraft data
 - Future: enable machines to do the access



- Developing a single-node, ROC ground station
 - Automated basic fault detection and recovery
 - Mixed-initiative, hierarchical command and control language
 - Virtual ground station concept for GS composition
- Supporting current satellites mission (Opal and Sapphire) and future satellite missions (Cubesats and University Nanosatellite missions).
- Extending ROC concepts to federated ground station network (FGN)
- More information online at
 - Ground station systems--<http://swig.stanford.edu/>
 - ROC philosophy--<http://roc.cs.berkeley.edu/>
 - Satellites systems--<http://ssdl.stanford.edu/>