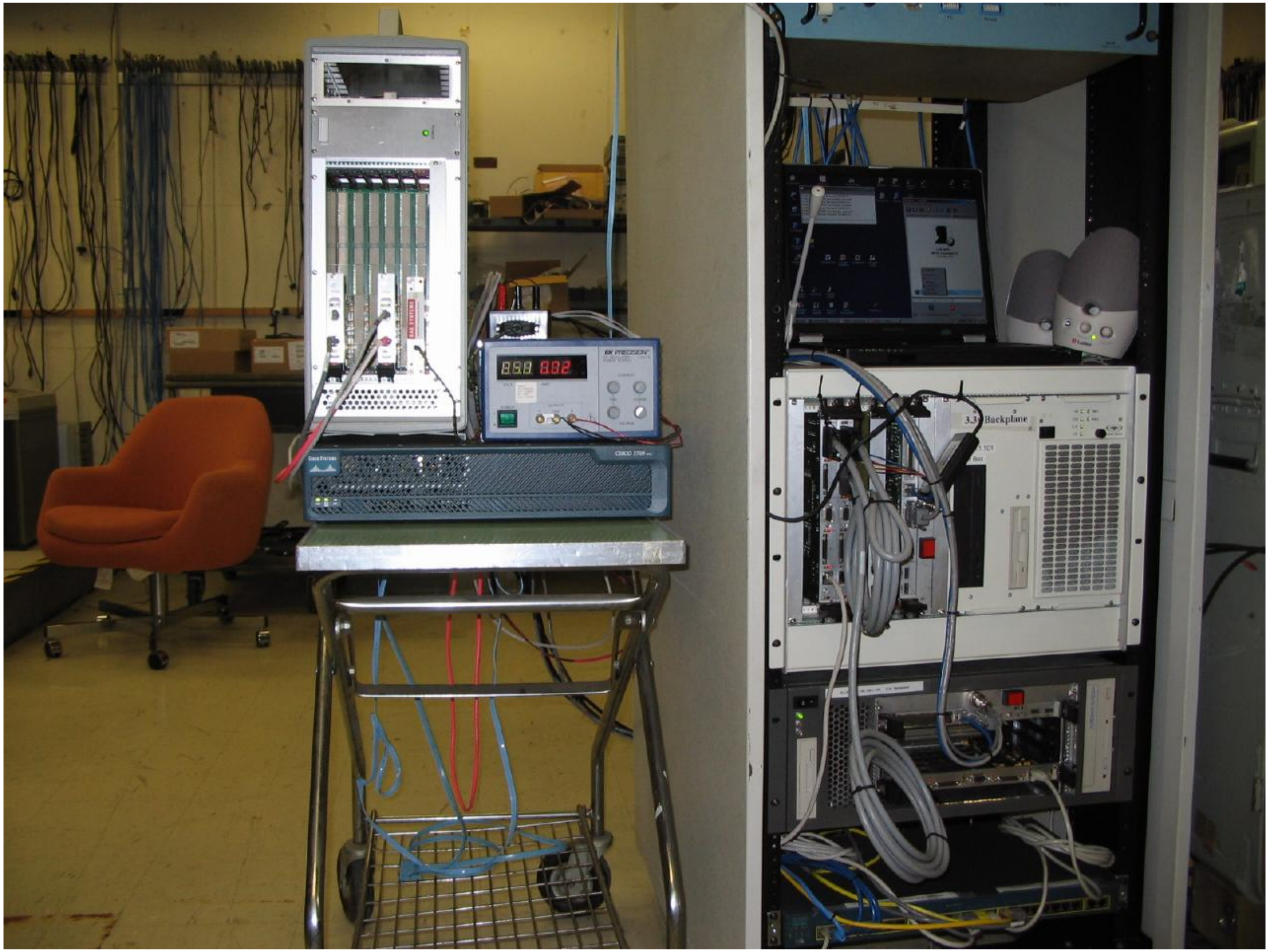
GSFC Flight Network Summary
Space Internet Workshop #5

Dave Israel/GSFC Code 567
Jane Marquart/GSFC Code 582
Greg Menke/GSFC RSC Code 582
Mike Lin/GSFC Code 561

Cisco Embedded Space Router

- Space Act Agreement between Cisco and GSFC, 2004
- GSFC and Cisco base-lined requirements
- Cisco designed and implemented an IOS on a BAE Systems Rad750; called "SQR" (Space Qualified Router)
  - Clock not specified, somewhere between 133 and 166mhz
  - 128Mb RAM
  - Running experimental 12.3 IOS w/ K9 advanced security option
  - Two commercial dual 10/100/1g Ethernet devices on the CPCI backplane, giving the SQR four Ethernet ports, appearing in IOS as conventional Gigabit Ethernet devices.
  - No onboard flash boot, firmware loaded from auxiliary system.
- GSFC tested router in flight software lab in April 2005
- Demos in June 2005

Cisco Embedded System Router



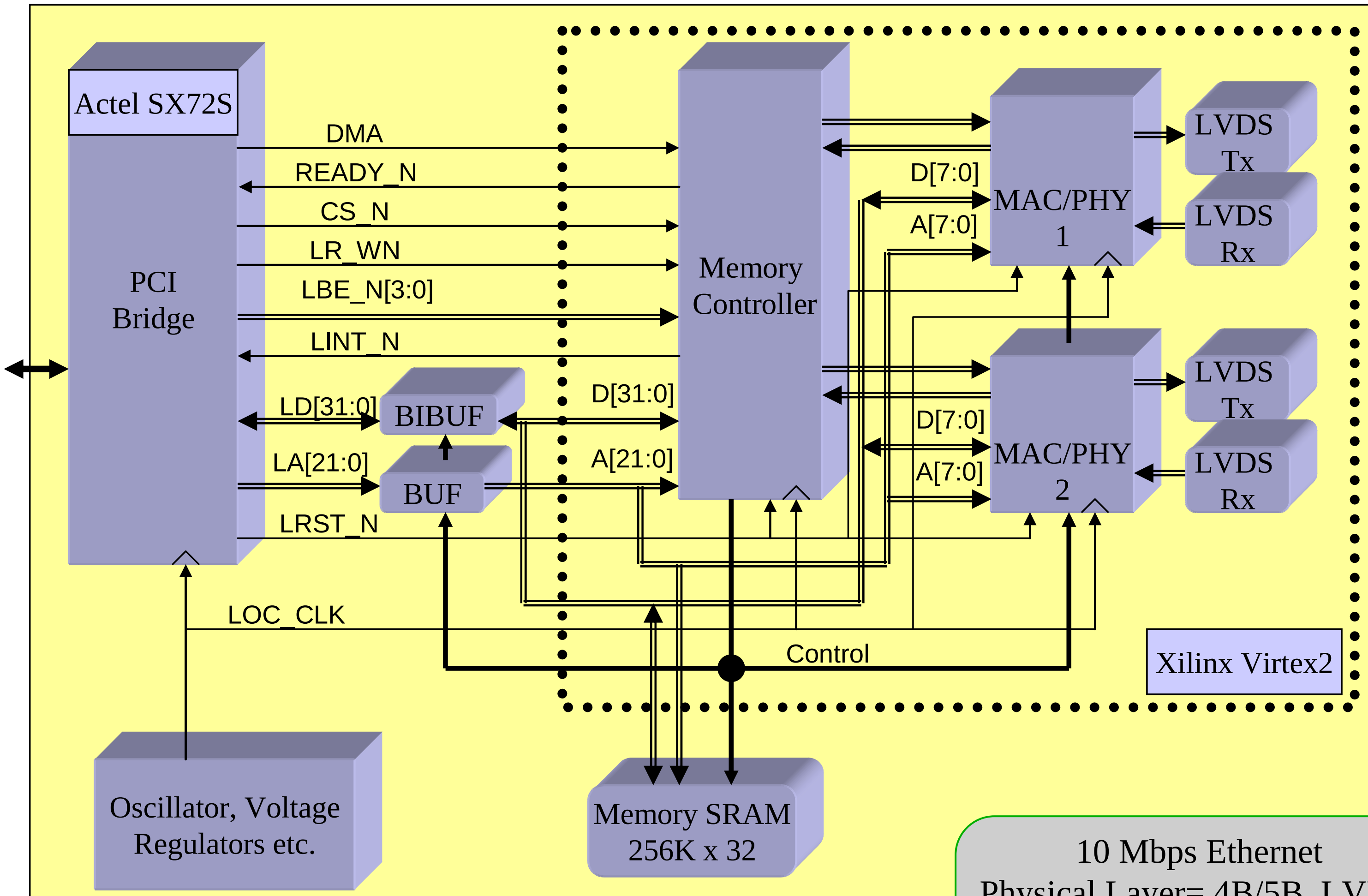
GSFC NIC and Switch

- Developed by Code 561 (Mike Lin) under ESTO funding
- Supports 10/100 Mbit Ethernet over twisted pair using a 12.5/125 Mbit DS Link encoded LVDS physical layer
- Media converter connects LVDS Flight Ethernet to 10/100-base TX
- NIC
  - 2 independent instances of a commercial MAC core per NIC.
  - Two external LVDS Ethernet interfaces & one selectable 10baseT RJ45 interface per NIC. MAC's are standard, PHY redeveloped to use LVDS.
  - NIC configured as a 6U CPCI card; 32 bit, 3.3v, 33mhz, bus mastering.
  - Supports full duplex 10/100 Mbit Ethernet
  - FPGA's chosen to provide a path to a rad-hard flight implementation
- Switch
  - 12 port, 10mb LVDS Ethernet
  - Fixed MAC address table (to reduce gate count)
  - Supports Broadcast and Pause (to meet GPM network requirements)

NIC Breadboard

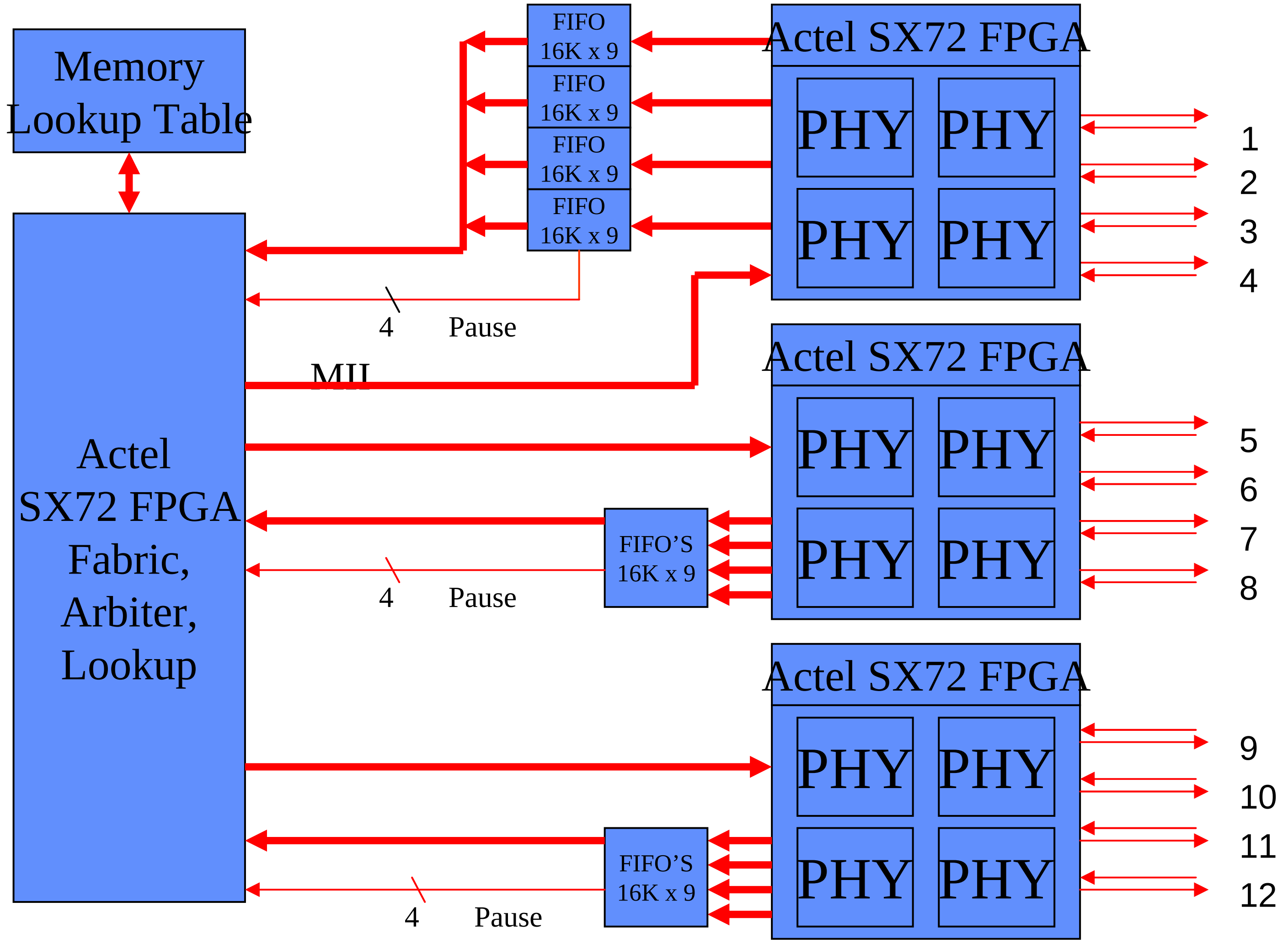
Standard 32 bit/33 MHz Compact PCI Interface

6U Compact PCI card



10 Mbps Ethernet
Physical Layer= 4B/5B, LVDS, Data Strobe Encoded
2 pairs xmit / 2 pairs rec.
12.5 MHz xmit rate

Rad-Hard Switch



Router Configurations

- **Plain-text Mode**
  - Simple packet forwarding via static routes.
  - No QoS rules.
  - Rate-limit rules apply to aggregate traffic flowing through the interface to simulate throughput over a space link.

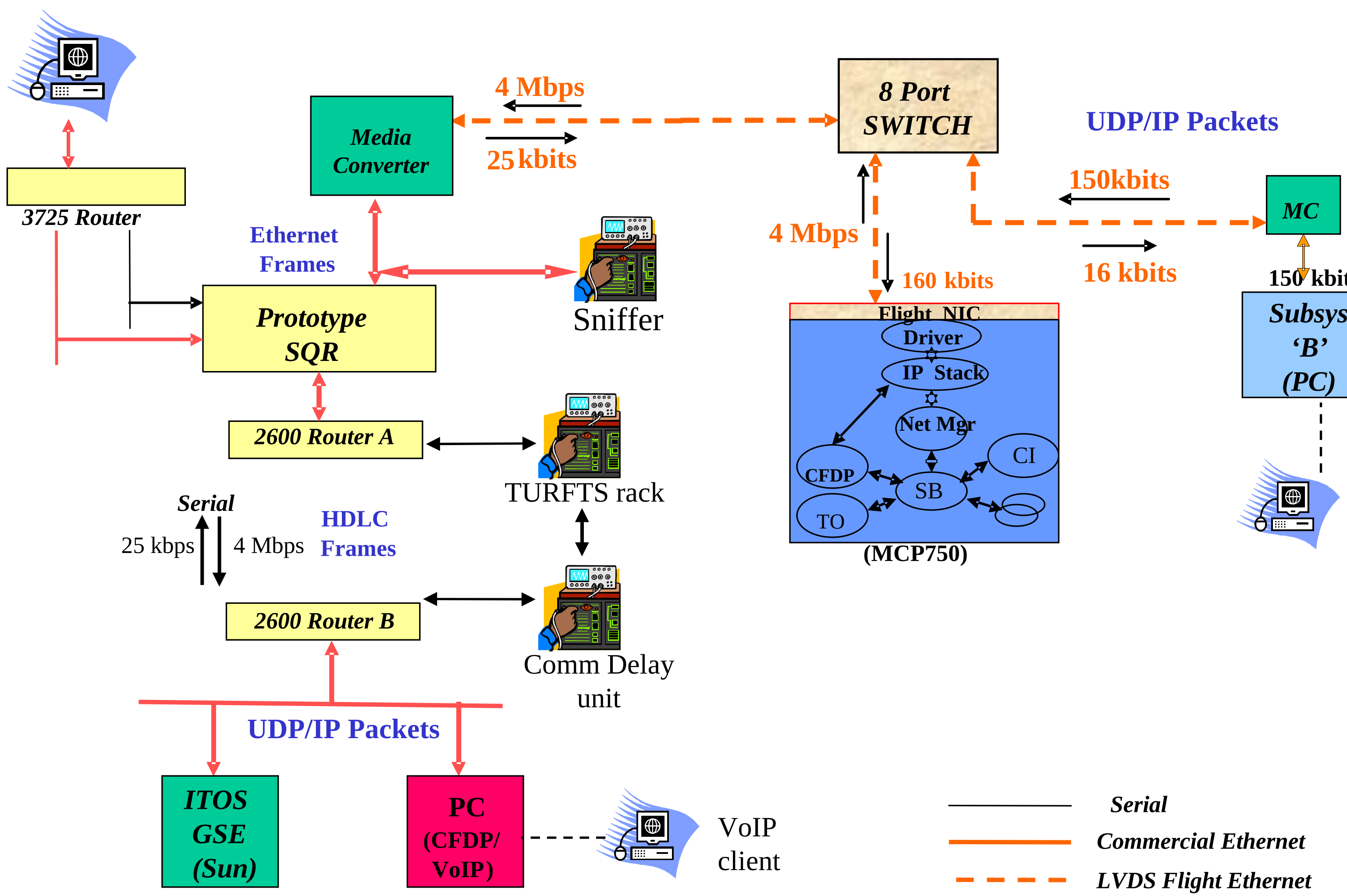
- **IP-Sec Mode**
  - Forward Link traffic is authenticated & encrypted using IKE & IP-Sec via an IP-Sec tunnel between the Ground Station router and SQR.
  - Return Link traffic is plain-text, traversing an IP tunnel between the SQR and Ground Station router. (Note: encrypting high rate Return Link traffic yields a prohibitive CPU footprint on the spacecraft).
  - The space link is composed of two IP tunnels, each used unidirectionally; the Cisco smartguys figured that one out.
  - No crypto session timeouts so session keys are retained while out of contact, and when uni-directional links are operating.
  - 3DES & AES algorithms were used in conformance to GSFC mandates.

Operational Scenario Info

- **IPSec used for all IP operations**
  - All forward link traffic is encrypted.
  - All traffic not decrypted by IPSec is dropped at the SQR via access list rules; only packets delivered by the IPSec tunnel are forwarded.
  - Encrypted blind commanding supported.
  - Initial IKE handshake requires bidirectional comms. Once the sessions are established, the traffic composition is unchanged but contents are encrypted.

- **Due to lack of an IOS driver for a CPCI HDLC card in the SQR cage, an additional Cisco 2600 was used to convert the serial HDLC space-link to Ethernet**
  - no rate limiting, tunneling or QoS semantics were configured- only packet forwarding.
  - CPU impact on router from HDLC framing/deframing and link management was not testable.
  - IPSec is passed through; All tunnels extend from the SQR to the ground router.

Embedded Space Router Testbed



Questions to be answered:

- ***CPU & memory utilization figures***
  - How busy is the cpu?
  - How much buffer memory is required to handle the traffic load?

- ***Consequences of protocols such as IP-Sec, CFDP & TCP***
  - How do failures manifest?
  - How do protocols recover from partial or complete link failure?
  - How do protocols handle uni-directional link states & changes from uni-directional to bi-directional?

- ***Management of the space-link.***
  - How does packet loss affect operations?

Results

- Had sufficient memory: no packet drops were recorded in the SQR.
- Bulk data transmission from Spacecraft to Mission Control w/ file transfer protocol responses traversing the IPSec tunnel: CPU footprint ~10%
- Same bulk transmission with bi-directional VoIP between Spacecraft and Mission Control: CPU footprint ~15% - VoIP forward traffic over the IPSec link was somewhat expensive.
- CFDP worked well
  - Unidirectional links work as expected; protocol handled the link transitions gracefully using the configured timeouts; no link state knowledge was incorporated in the protocol operation.
  - Protocol resumes and finishes without error as bidirectional comms are restored.
- IPSec is more complex
  - Once IKE sessions are established, crypto worked well unidirectionally & was a nice way to secure the command link without addtl flight software.
  - Crypto time-out requires bi-directional link to initialize.
  - Cross-vendor compatibility issues; Sun vs Cisco.
  - Flight deployment will require significant management by Flight Software.
  - Need for pre-shared keys for contingency commanding.
- For general support of onboard TCP applications, a SCPS gateway is likely required for lunar scale delay products.
- Skype was annoying; configurable data-rates, uni-directional and “connection-less” calls are important features.
- IP as end-to-end transport was a big win; when the testbed was disassembled, moved, reassembled and integrated with the TURFTS system, only a couple hours of negotiating IP addresses and router config was necessary to bring up the entire system.

Conclusions (1 of 2)

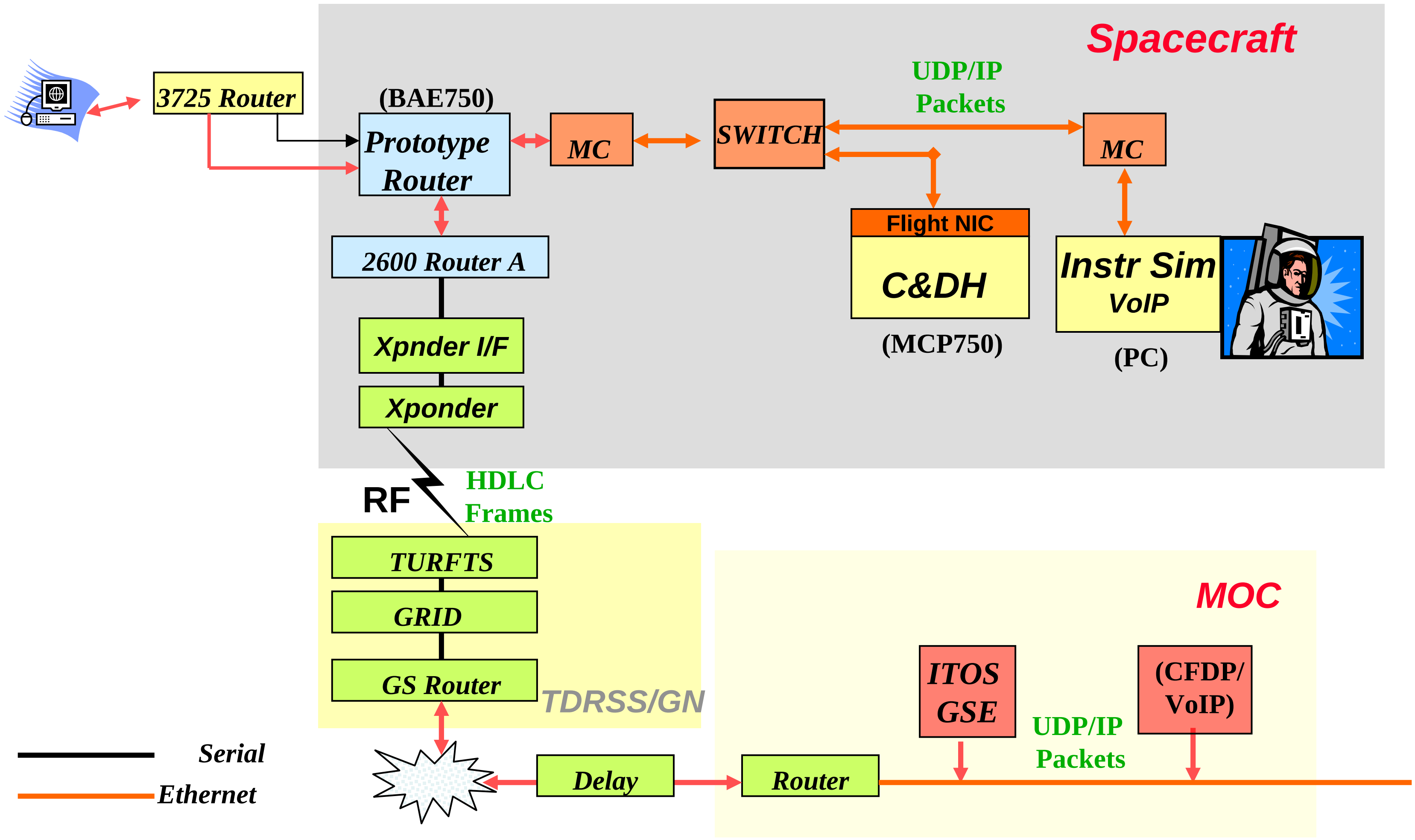
- ***Hardware footprint & performance***
  - Pro: Cisco SQR worked nicely as a standard IOS; entirely conformant with expected characteristics.
  - Con: Requires hardware resources roughly equivalent to a C&DH computer- but could scale down a bit before performance is considerably affected.

- ***Router command and control***
  - Command, control and monitoring features of IOS are sufficient for normal operation; SNMP and other tools are likely more than adequate.
  - Contingency modes will likely require a console serial port always operable & connected to the C&DH systems for command/control.
  - Deployed system would probably include digital I/O to reset, power on/off and configure SQR, and possibly firmware augmentation to parse magic command packets.
  - Onboard flash boot & maintenance features will be necessary.

Conclusions (2 of 2)

- ***IP Quality of Service policies***
  - Forwarding policies at router must be carefully designed. Typical packet forwarding rules will not adequately control queuing & utilization over the space link.
  - Access-lists are needed at each end of the space link to ensure only valid space-link traffic traverses either link.
  - Application layer software must throttle itself to keep from overusing bandwidth and to conform to system engineering policy, particularly when transmitting over the space-link.
    - This is problematic when using IP because such measures are not usually implemented in the app layer at all. A feedback mechanism from the router feeding the space link is clearly required if the space link is to meet utilization requirements.
    - DiffServe/IntServe are helpful but insufficient as the sole means of implementing system engineering.
- ***IP-Sec***
  - Disabling session timeouts is a cheap & easy way to obtain persistent state for long-term crypto.
  - Pre-shared, static keys for contingency operation should be considered.
  - IP-Sec CPU overhead makes encryption expensive for high rate Return Links. For the typical low bandwidth Forward Link, IP-Sec adds little cost and considerable security.

Integrated Ethernet/IP Testbed



Path to Flight

- **Embedded Space Router (ESR)**
  - BAE750 has compatible flight board
  - Add IOS driver for HDLC card.
  - Flash/EEPROM for IOS image (currently booting from outside source)
  - Implementation of command/control features for contingency ops.

- **NIC and Switch**
  - Flyable with rad-hard part upgrades & ETU board development.
  - Qualify/test to 100Mb- not precluded by existing design.
  - 100 megabit Switch may have reduced or mixed rate ports because of bandwidth limitations in the FPGA & memory.
  - Upgrade to 1 Gig would require a major revisit to the design.

For more information:

- Flight & Ground Comm
  - Dave.Israel@nasa.gov
- Rad-Hard Ethernet Hardware
  - Michael.R.Lin@nasa.gov
- Flight software/onboard network
  - Jane.Marquart@nasa.gov
  - gregory.menke@gsfc.nasa.gov
- Cisco embedded space router
  - harif@cisco.com