PS2 Network Analyzer
Overview

- Network Analysis/Monitoring Overview
- PS2 Architectural Overview
- Project Goals
Network Analysis – Why

- Discover faulty equipment
- Detect malicious users/hackers
- Determine usage patterns and bottlenecks
Network Analysis – Implementation

- Listen to all network traffic
- Process all `interesting' packets
- Record relevant information
- Produce a useable report
Network Analysis – Issues

• Bottlenecks – Network traffic is too much for equipment to handle

• Buffer overflow

• Lost packets due to processing delays

• Erroneous reporting

• Memory intensive tables
Network Analysis – Solutions

• Layered Architecture
  – Filter out data as soon as we know we can ignore it
• Fast (hash based) network flow table lookups
• Expiry timers
• External Report Generation
PS2 Architecture

- Geared toward multimedia applications (i.e. games)
- Very little data cache
- Fine grained parallelism
- Wide data bus
PS2 Architecture (cont.)
Obstacles

• Memory Requirements
  – How does one fit an over 10MB of libraries plus a 2.5MB kernel into 8MB

• Library/Kernel Compatibility

• Library bugs
  – Flawed network driver implementation
Solutions

- Use equivalent libraries
  - uClibc
  - Dietlibc
- Compression
- Open Source Kernel Upgrades
- Available Betas
Implementation

• Remove extraneous libraries.
• Create boot image and compress it.
• Write scripts so that the boot sequence immediately executes the Argus port.
Results
Q & A

• Why?
  
  – I wanted to do something `practical' and this seemed more practical than spending $300 for a Rabbit card which I wouldn't use in the future
  
  – Why not