

# **Big-Ticket Management and Testing with Low Budget Impact**

**10:15 to 11:15**

**Description:** Many popular commercial network management platforms and testing software are big-ticket items, costing tens or even hundreds of thousands of dollars. Can open-source alternatives provide some or even all of the required functionality at a fraction of the purchase price? Will organizations pay more, or less, for maintenance, support, and enhancements, and who will provide these services? This session will help you weight your open-source options against commercial solutions.

**IT Management and Monitoring, the Open Source Approach...**

# Big-Ticket Management and Testing with Low Budget Impact

Erik M. Cummings  
Production Control Manager, ITSS Operations  
[erik.cummings@stanford.edu](mailto:erik.cummings@stanford.edu)  
<http://www.stanford.edu/dept/itss/>  
05 May 2005



# Table of Contents

- ◆ **Introductions: Session and Instructor**
- ◆ **Discussion of the Open Source Approach**
- ◆ **How to Execute the Approach**
- ◆ **Some of the Possibilities**
- ◆ **Resources and References...**
- ◆ **What now?**
- ◆ **Q & A**

# Introduction to this Session

- ◆ **What the Open Source Approach to Mgmt is...**
- ◆ **How to execute this approach...**
- ◆ **How to sell it...**
- ◆ **What are the implications/long term effects?**
- ◆ **Some of the possibilities.**
- ◆ **What now?**

# What this Session is NOT:

- ◆ A detailed discussion of any of the possibilities...
- ◆ A How-To for your particular environment.
- ◆ A Tutorial on any Open Source Tools.
- ◆ A definitive list of solutions...

# Intro to Your Speaker:

- ◆ **Manager of Production Control: Stanford University.**
- ◆ **Director of IT: MediaLive International**
- ◆ **Lead Engineer – Netops: Ziff-Davis Events (aka MediaLive International)**
- ◆ **Manager of IS: Barr Systems, Inc.**
- ◆ **Sr. Network Engineer: Santa Fe Community College (Gainesville, FL)**
- ◆ **Network Engineer: EDSI**
- ◆ **Sr. Network Administrator: 1<sup>st</sup> MarDiv, USMC**

# The Open Source Approach:

- ◆ **You've heard all the axioms:**
  - ◆ **Open Source doesn't mean free.**
  - ◆ **Open Source doesn't have support.**
  - ◆ **Open Source is less secure.**
  - ◆ **...etc...**
- ◆ **But you've seen some successes:**
  - ◆ **Apache**
  - ◆ **Linux**
  - ◆ **BIND**
  - ◆ **...etc...**

# The Open Source Approach:

- ◆ **Open Source Applications and tools.**
- ◆ **Open and Accessible Data.**
- ◆ **An understanding that there is no “Out-of-the-box” answer.**
- ◆ **An understanding that research and planning are critical!**
- ◆ **An understanding that the “buck stops here.”**
- ◆ **A commitment to hard work.**
- ◆ **A possibility for big pay-off!**

# What this approach does NOT mean:

- ◆ **Closed source/proprietary solutions and/or tools.**
- ◆ **An “out-of-the-box” solution.**
- ◆ **Free/cost-free.**
- ◆ **Effortless.**
- ◆ **Carefree.**
- ◆ **Easy.**
- ◆ **Big-Dollars!**

# Executing the OS Approach:

- ◆ **Two Methods:**

1. **If you build it...they will come...**

2. **The 6 P's.**

**(Prior Planning Prevents Piss Poor Performance)**

# Okay, How do I sell it?

**With research, thought, good planning, and analysis...coupled with a solid understanding of the limitations and implications, the OS Approach can bring huge monetary pay-off.**

- **Clearly define and present your “need”.**
- **Present solid research and someone else’s real-life implementation.**
- **Don’t limit yourself to Open Source!**
- **Don’t say it’s free!**
- **Present known limitations!**
- **Present a commercial alternative.**

# Executing the OS Approach:

- ◆ **Research**
- ◆ **Consideration**
- ◆ **Compromise**
- ◆ **Results**
- ◆ **Long Term Effect...**

# What are you trying to do?

- ◆ **Monitoring:**

- ◆ **Network**
- ◆ **Systems**
- ◆ **Security**

- ◆ **Troubleshoot?**

- ◆ **Manage:**

- ◆ **Network**
- ◆ **Systems**
- ◆ **Security**

# Know what is out there!

- ◆ **Hundreds, even thousands of solutions.**
- ◆ **Every scale you could imagine...**
- ◆ **Where are all these solutions?**
  - ◆ **Google is your friend!**
  - ◆ **CAIDA (Cooperative Association for Internet Data Analysis)**
  - ◆ **SourceForge**

# Match Your Needs

- ◆ **Start with your perfect world scenario.**
- ◆ **Really understand the capabilities and limitations of potential solutions.**
- ◆ **Be prepared to compromise!**
- ◆ **Know what you CANNOT compromise on!**

# OS Approach Costs

- ◆ **Licensing.**
  - ◆ Just because it's Open Source, doesn't mean it's free!
- ◆ **Implementation:**
  - ◆ Money to hire consultants.
  - ◆ Time and Energy to do it yourself.
- ◆ **Support:**
  - ◆ Break/fix...
  - ◆ Self-support (again with the time and energy!)
  - ◆ Commercial ( <http://www.findopensource.com> )

# OS Approach Costs (cont)

- ◆ **Customization?**
- ◆ **Ongoing updates/patches/fixes?**
- ◆ **Depends on your changing world**
  - ◆ **Infrastructure and system changes, updates and implementation means customization on your Mgmt/Monitoring.**
  - ◆ **Desire for new/improved features, as well as fixes for security drives patching.**

# A Few Possibilities: (Network and Systems Monitoring)

- ◆ NagIOS
- ◆ Big Brother
- ◆ Angel
- ◆ Modules/Plug-ins
- ◆ Scripts
- ◆ MRTG
- ◆ Scotty
- ◆ openNMS
- ◆ Cheops-ng

# A Few Possibilities: (Troubleshooting)

- ◆ **MTR**
- ◆ **Snort (AirSnort?)**
- ◆ **TCPDump**
- ◆ **Ethereal**
- ◆ **Etherape**
- ◆ **IPTraff**
- ◆ **Ntop**
- ◆ **Argus**
- ◆ **Kismet**
- ◆ **sysmon**

# A Few Possibilities: (Security Mgmt and Assessment)

- ◆ **OSSIM**
- ◆ **IPChains tools**
- ◆ **IDS/Snort and add-ons...**
- ◆ **dsniff**
- ◆ **Saint**
- ◆ **Satan**
- ◆ **Nessus**
- ◆ **Nmap**

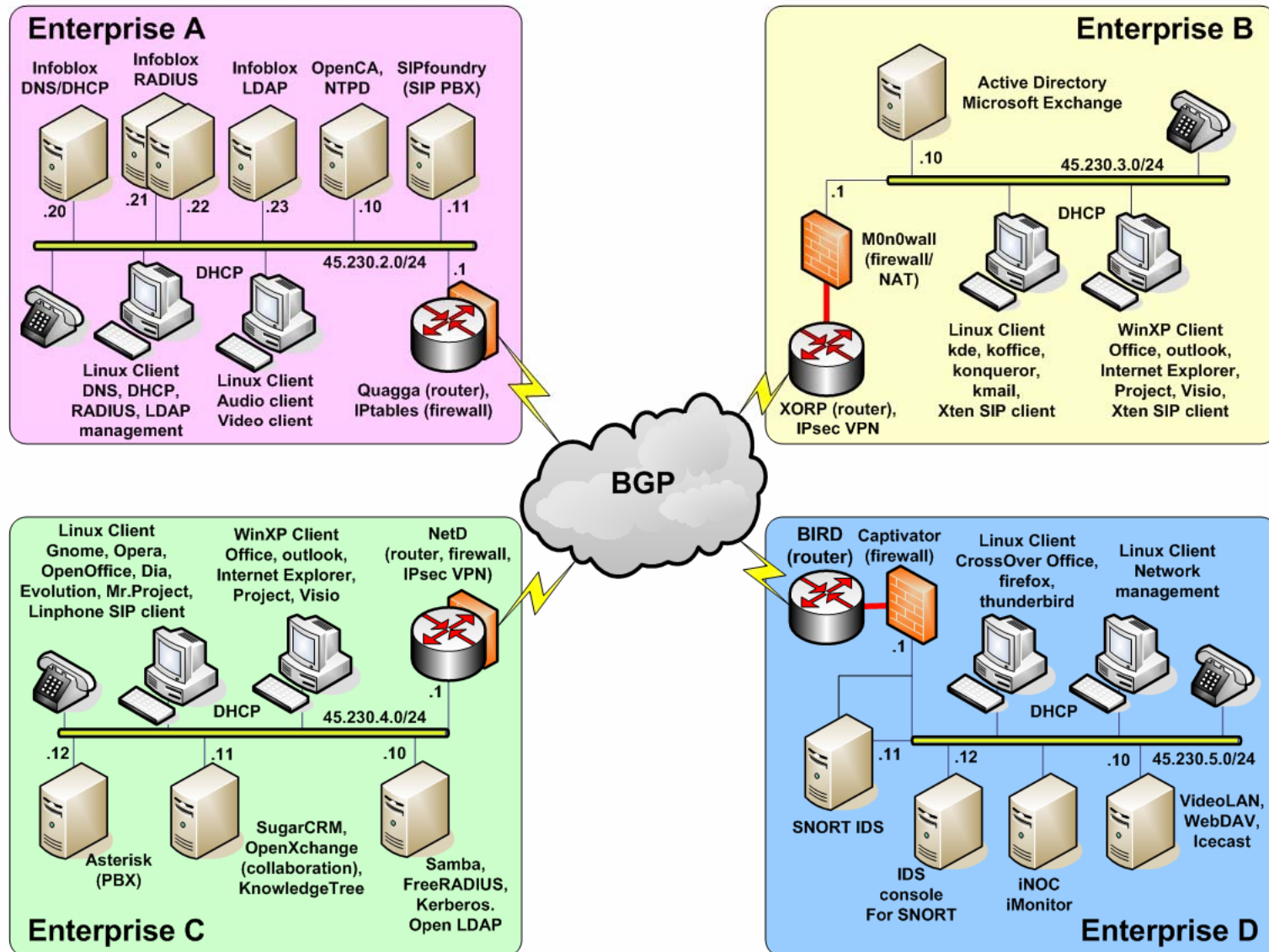
# **A Few Possibilities: (Management and Configuration)**

- ◆ **Webmin**
- ◆ **phpMyadmin**
- ◆ **phpmyldapadmin**
- ◆ **phpmyoracleadmin**
- ◆ **NagIOS**
- ◆ **And many more...search by service?**

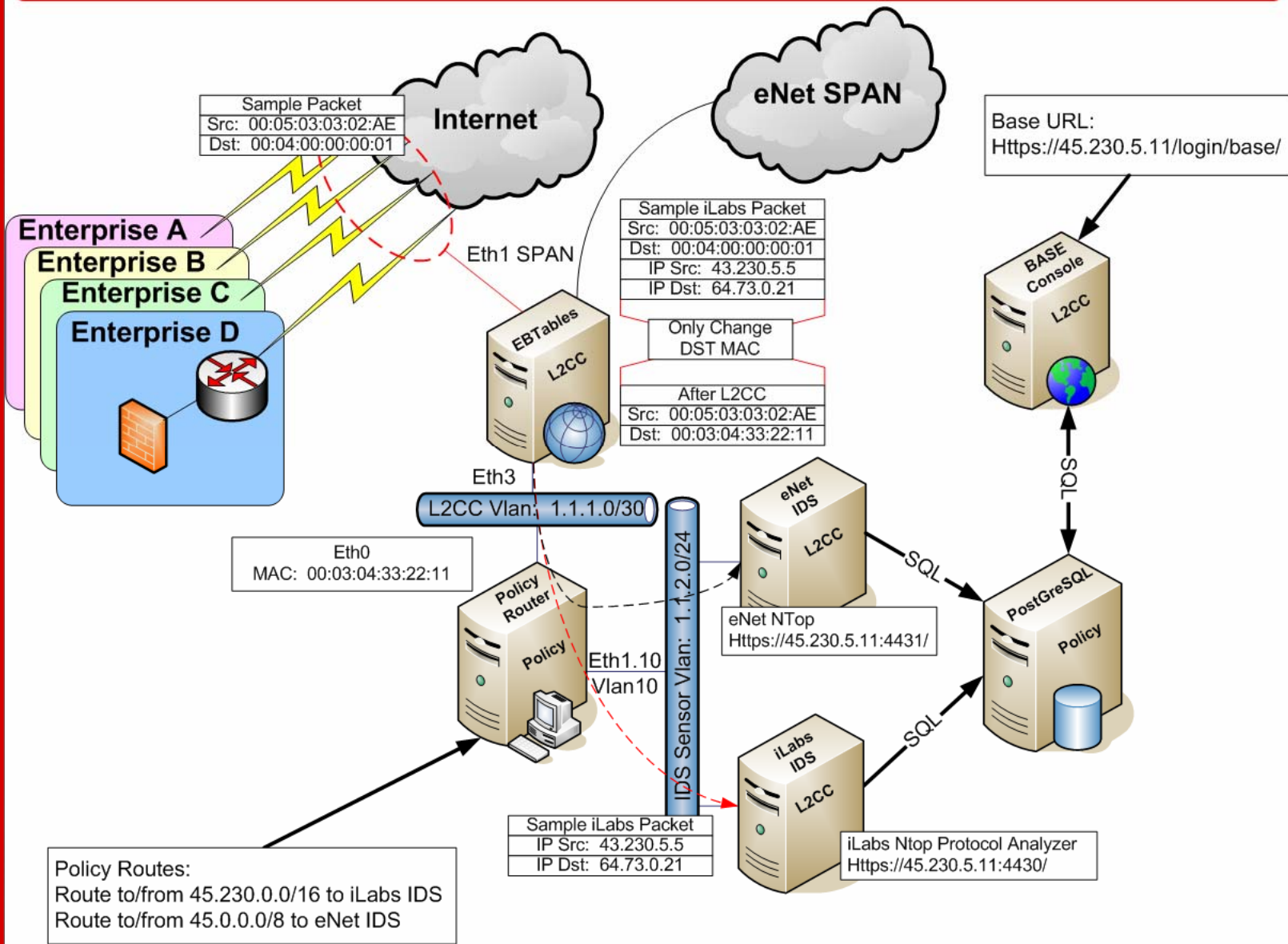
# InteropNet Labs

- ◆ **Open Source Solutions Initiative**
- ◆ **Show Floor, Booth 2607**
- ◆ **Real Life work, continuing development and testing...**

# InteropNet Labs - Las Vegas 2005 – Open Source Software Initiative



# InteropNet Labs - Las Vegas 2005 – Open Source Software Initiative – IDS Load Balancer



# Comparing OS and Commercial Approaches

- ◆ **Support (the Finger-Pointing Scenario!)**
- ◆ **Implementation**
- ◆ **Long Term Liability**
- ◆ **Cost!**
- ◆ **Effort and Energy**
- ◆ **Feature Path**
- ◆ **Development Speed**
- ◆ **Development Stability**
- ◆ **Security**

# Some of the Commercial Apps

- ◆ **Unicenter**
- ◆ **What's Up Gold**
- ◆ **Cisco Works**
- ◆ **SMARTS InCharge (EMC)**
- ◆ **BMC Patrol**
- ◆ **OpenView**
- ◆ **Spectrum**

# Some Key Considerations:

- ◆ **Integrating Open Source and Proprietary Applications...**
- ◆ **Relying on your environment**
- ◆ **Watching the Watcher!**
- ◆ **Network, network, network...**
- ◆ **Being Realistic...**

# Resources and References:

- ◆ <http://www.caida.org>
- ◆ <http://www.google.org>
- ◆ <http://www.findopensource.com>

# What Now?

- ◆ **Look at your environment.**
- ◆ **Figure out what you need.**
  
- ◆ **Reach out for research!!!**



# Q&A

# ?



# Thank You!

Erik M. Cummings  
Production Control Manager, ITSS Operations  
[erik.cummings@stanford.edu](mailto:erik.cummings@stanford.edu)  
<http://www.stanford.edu/dept/itss/>  
05 May 2005

