

Network & System Management

A Practical Framework



Practical Network and System Management

ENGINEERED NETWORKS

www.engineered-net.com

ssurdock@engineered-net.com

Date: 03/18/05

© 2005 Engineered Networks

Rev: 1.0

Page: 1

Published Frameworks

- Telecommunications Management Network (TNM)
- IT Service Management (ITSM)
 - IT Infrastructure Library (ITIL)
- Microsoft Operations Framework (MOF)
- Open Systems Interconnection (OSI) Management Architecture
 - FCAPS

Operations Framework

- IT Infrastructure Library (ITIL)
 - Service Delivery
 - Service Support
 - Planning to Implement Service Management
 - ICT Infrastructure Management
 - Application Management
 - Security Management
 - Business Perspective

Network & System Management

- OSI Management Architecture
 - Fault
 - Configuration
 - Accounting
 - Performance
 - Security

Fault Management

- Problem identification
- Problem isolation
- Analysis procedures & tools
- Problem resolution
 - Resolution procedures in place?

Configuration Management

- Asset tracking
- License management
- Release management
 - ITIL procedures excel
 - http://visibleops.tripwire.com/visible_ops.cfm
- Monitor, log and detect changes!

Accounting Management

- System usage
- License metering

Performance Management

- Traffic analysis
- Baseline performance
- Trending performance
- Capacity planning & system sizing
- Application Performance

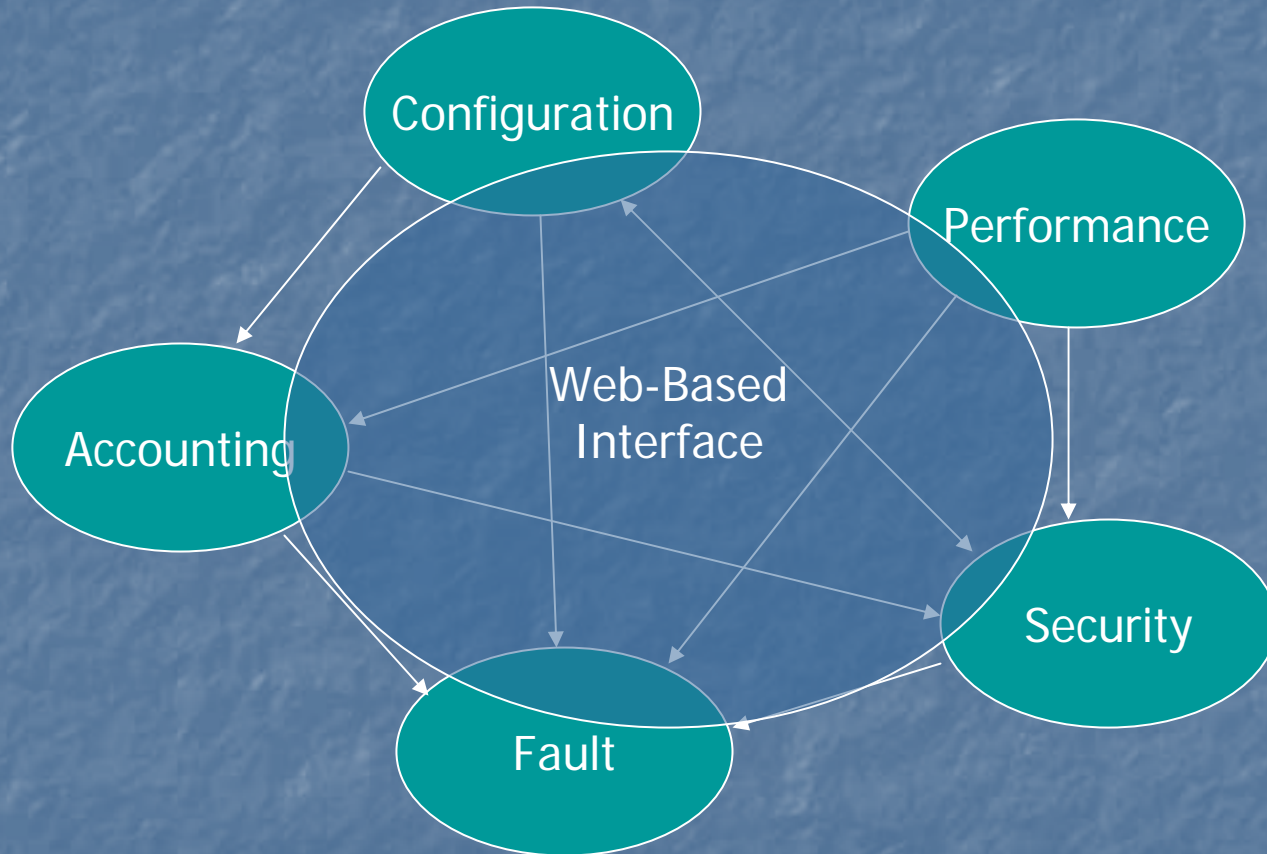
Security Management

- Policy definition
- Policy enforcement
 - Authentication & authorization
 - Access control
- Detection of policy violation
- Response

Approaches

- Procedures, techniques & tools
- Tools
 - Isolated point systems
 - Integrated point systems
 - Management frameworks

Management System



The Truths

- Management is more process than tools
- No one product does everything well
- Every environment is different
 - So the tools and procedures will be different

Fill In The Gaps

- Assess what is missing
 - Do you have enough data to make an informed decision?
 - Do you have to look too many places for the information?
- Consolidated logging
- Consolidated statistical data
- Consolidated configuration information

Centralized Logging

- Hits three of the five areas
 - Security Management
 - Fault Management
 - Configuration Management

Polling For Statistical Data

- Store and archive the data
- Baseline the data
- Alert on error or other anomaly
- Polling server request data from devices
 - ICMP (ping), SNMP, WBEM WMI, Application

Problem Identification

- Know before your users
- Event console
 - Fed by other systems
- Identify severity & automate
- Create trouble ticket
- Changes feed configuration management system

Configuration

- 80% of outages are self inflicted
- Rebuild is often easier than repair
- Create a repeatable build library for ALL infrastructure devices.
- Detect deviations from the baseline
- Automate, automate, automate

Security Management

- Assess
 - Risk = asset value X threats X vulnerabilities
- Protect
 - Defense in depth
- Detect
 - Logging and alerting
- Respond
 - Make sure it doesn't happen again

Cover Your Bases

- **Fault Management**
- **Configuration Management**
- **Accounting Management**
- **Performance Management**
- **Security Management**
- **Crawl, Walk, Run**

The End

- Thank you for coming!
- The Presentation can be found at:
<http://www.engineered-net.com/Library>
- The winner is...