Understanding Fault Management

Session NMS-1011
Suddenly...

The Network Is DOWN

Do You Know What Went Wrong?

• Did a router fail?
• Did several routers fail?
• Was there a fiber cut?
• Did the path to the network management station fail?
A Few Things to Remember

- Faults happen
- Redundancy only works if you notice the first failure
- It’s easier to resolve problems before they affect your customers
- You won’t know what went wrong unless you have appropriate instrumentation AND documentation

What Is a Fault?

- A fault is an unplanned failure of software, hardware, or wetware
- Not every outage is due to a fault
- Not every fault results in an outage
Sources

- Routers, switches, wires, fiber, PDUs, DNS servers, HVACs, power companies, squirrels, floods, soft drinks, clumsy people, nuclear accelerators

Agenda

- Fault Management Tuning Cycle
  - Baseline Network
  - Setup Alarms and Thresholds
  - Excessive/Missed Faults
  - Nominal
- Fault Management Process Cycle
  - Fault Occurs
  - Detection
  - Correlation
  - Diagnosis
  - Correction
  - Nominal
- Tools
Fault Management Tuning Cycle

Fault Management Tuning Cycle

Baselining—What’s Nominal?

• Take a baseline of your network when times are good

• Include:
  - Network and wiring diagrams
  - Device configurations
  - Performance metrics
  - Service level agreements (SLAs)
IP Connectivity and Fault Management

IP Connectivity Identifies Issues Fault Management May Not See and Directs Operators at Service Impacting Faults

IP Connectivity Not Impacted Latency Might Be Operations See a Fault but Does It Impact on Customer Service?

Operations See a Fault but Does It Impact on Customer Service?

Avoid Flying Blind
Use High-Availability Principles for Network Management!

- Have redundant connectivity all the way to the NMS
- Have multiple DNS servers near by
- Ditto for NTP servers
- Have sufficient bandwidth to poll (when needed)
- Have reliable AAA and a backup—if you can’t get in, you can’t fix the problem
Fault Management Tuning Cycle

Set up Alarms and Thresholds

- Alarms may be SNMP notifications, Syslog events, or events triggered from polling
- Many applications include default thresholds
  Defaults may not be the best for your network—Each network is unique
- Check which alarms are covered by built-in notifications or events
- Some polling may be necessary to check other thresholds
SNMP Trap Notification

- SNMP Trap Notification
  Unacknowledged UDP packet
- Contains
  OID:linkDown Notification
  Varbinds:
  \- ifIndex
  \- ifDescr
  \- ifType

1. Load IF-MIB
2. Remote Device Goes Down
3. Agent Generates Notification
   linkDown
   \- ifIndex.4
   \- ifDescr.4 Serial 1/2
   \- ifType.4 propPointToPointSerial(22)
4. SNMP Notification
5. linkDown Notification Delivered to CIC

OID for linkDown

Trap PDU 1.3.6.1.2.1.11.0.2
SNMP Inform Notification

- SNMP Inform Notification
  Acknowledged “Trap”
- Contains
  OID: linkDown Notification
  Varbinds:
  - ifIndex
  - ifDescr
  - ifType

Load IF-MIB

Instance 4

Remote Device Goes Down

SNMP Notification

OID for linkDown

Inform PDU 1.3.6.1.2.1.11.0.2

Response PDU Acknowledging Inform

SNMP Version Differences

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version 1</th>
<th>Version 2c</th>
<th>Version 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informs</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RMON/Event</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication</td>
<td>Community</td>
<td>Community</td>
<td>Users</td>
</tr>
<tr>
<td>Privacy</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IOS/CATOS</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>NMS Support</td>
<td>Ubiquitous</td>
<td>Pretty Good</td>
<td>Limited</td>
</tr>
</tbody>
</table>
Which Objects Does Cisco Support?

Mandatory: MIB-II and IF-MIB
- [link](http://www.cisco.com/go/mibs)
  For all OSes and MIBs
  Describes which products support which MIBs
  Also has the MIBs themselves

Downloading MIBs and Related Files in Bulk
  Consider downloading the whole OID directory for quick searches

How Useful Is Notification-Based Polling?

“There Are So Few SNMP Notifications!”

There Are as Many Notifications as There Are MIB Variables!
Notifications

How to Make your own Notifications

- RMON Events/Alarms
  Available in Cisco IOS® since 11.1
  Available in CatOS always

- Event MIB
  Available in Cisco IOS since 12.1(3)T

Customize objects for use in Notifications

- Expression MIB
  Available in Cisco IOS since 12.0(5)T

Set a Threshold

RMON alarms

- Command line accessible

EVENT-MIB

- Has wildcards, better variety of tests

EXPRESSION-MIB

- Create new objects that can be tested

System Polls Itself!
Example MIB to Create Notification from

- CISCO-PROCESS-MIB
  
  SNMP version of "show process"
  
  Provides total CPU usage as well as per-process usage

- Now, to create a new notification based upon total CPU utilization

Device Checks CPU Utilization Using RMON

- Define the alarm:
  
  RMON alarm 1 cpmCPUTotalTable.1.4.1 60 absolute rising-threshold 90 1 falling-threshold 70
  
  Tests the OID (1 min CPU utilization (cpmCPUTotal1min) found in CISCO-PROCESS-MIB) every 60 seconds

  If the absolute value exceeds 90% fire event 1

  Reset the alarm when the value falls below 70%

- Define the event:
  
  rmon event 1 description "CPU Notification" owner chelliot@cisco.com log trap public
  
  When triggered will both create a log entry and send a SNMP notification

  Equivalent of HPOV Threshold Events—but no Polling!
Event MIB

- More flexible than RMON events/alarms
  RMON is tailored for use with Counter objects
- Can be used to test objects on other devices
- No CLI yet—need to use SNMP directly or through tool

Event MIB

- Based on IETF draft and numbered in Cisco’s namespace from 12.1(3)T through 12.2T
- RFC 2981 implemented in 12.2(4)T
- Allows you to create custom notifications and log them and/or send them as SNMP traps or informs
- Persistence added in 12.2(4)T (same time as RFC)
Event MIB

- Show commands
  show management event
- Debug commands
  debug management event mib

Expression MIB

- Based on IETF draft and numbered in Cisco’s namespace, not RFC 2982—Work is being done to implement RFC
- Allows you to create new SNMP objects based upon formulas
- Available in IOS since 12.0(5)T, added delta and wildcard support in 12.1(3)T
- Persistence added in 12.2(4)T
- No CLI yet—need to use SNMP directly or through tool
Expression MIB

• Delta and wildcard support allows, for example:

  Calculating utilization for all interfaces with one expression

  This will allow you to recreate the locIfInOctets and locIfOutOctets objects in a standards-based manner—with more flexibility

  Calculating errors as a percentage of traffic

Expression MIB

• Show commands

  show management expression

• Debug commands

  debug management expression?

  Evaluator Expression MIB evaluator

  Mib Expression MIB SNMP operations

  Parser Expression MIB parsing
SAA and CISCO-RTTMON-MIB

- Service Assurance Agent (SAA)
- Session level probe
- Generates availability and threshold traps
- Also collects statistics

Service Assurance Agent Today

Increasing Service Value

HTTP
DLSw
Jitter
Path Jitter
APM
ATM*
Cisco IOS-Based Service Assurance* Agent
*With Cisco IOS 12.2(9)T
UDP
ICMP
DNS/DHCP
SNA
Echo
QoS Support (ToS)
TCP
Connect
FTP
Frame Relay
MPLS VPN Aware
Cisco IOS 12.0(5)T and 12.0(8)S—HTTP Operation

- **Operation Mode for HTTP Transaction time:**
  - **Get-Mode**
    - Minimal parameters required; Only the base html page will be retrieved, not the links contained in the page
  - **Raw-Mode**
    - User specifies entire http request (optional payload)
      - It allows for security options, proxy servers, web caching

- **Each Mode Measures**
  - DNS Lookup Time
  - TCP Connect Time
  - HTTP Transaction time

- **Uniform Resource Locator:**
  - `http://<host>:<port>/<url-path>`

---

SAA Traps

- Defined in the CISCO-RTTMON-MIB
  - `rttMonConnectionChangeNotification`
  - `rttMonTimeoutNotification`
  - `rttMonThresholdNotification`
What Happens if a MIB Doesn’t Exist?

- Information may be found using Syslog
- Syslog produces (mostly) structured logs of information
- Syslog receivers/processors include:
  
  Unix syslogd
  
  Cisco Info Center
  
  CW2K RME Syslog Analyzer
Syslog

• Very basic reporting mechanism
• Very basic “standard”
• Text messages on UDP port 514

Syslog Benefits

• Easy to implement clients
• All ASCII (easy to manipulate)
• The UNIX standard
Syslog Problems

- It’s not reliable
- It’s not secure
  Not much worse than SNMP traps
- One way: No query capability
- Priority isn’t consistently used

Syslog Format

`<priority> NETASCII “0”`

`<facility>.<level>`

local7.info nms-host /usr 90% full

<priority> is not retained in the syslog message file
Timestamp is added by logging host
Logged message looks like:

Apr 18 12:02:34 nms-host /usr 90% full
There Is a Cisco IOS Message Standard for Syslog

- `%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text`
- Documentation for each release explains the meaning of many of these events
- Facility is not the same as the syslog facility
  - syslog facility is set by configuring:
    - `logging facility<facility>`
  - syslog facility defaults to local7
- Severity maps to syslog level

What If There Is No Syslog Event?

- Screen Scraping
  - Telnet/expect scripts sometimes can be the only way to get information
Fault Management Tuning Cycle

Does Your Fault Console Look Like this?
Monitor Excessive or Missed Faults

• Adjust thresholds as necessary to catch all faults (no false-negatives) but still have a tolerable false-positive rate
• Iterative process—the network administrator’s job is never done

Agenda

✓ Fault Management Tuning Cycle
  Baseline Network
  Setup Alarms and Thresholds
  Excessive/Missed Faults
  Nominal

• Fault Management Process Cycle
  Fault Occurs
  Detection
  Correlation
  Diagnosis
  Correction
  Nominal

• Tools
Fault Management Process Cycle

Fault Occurs → Detection → Correlation → Diagnosis → Correction → Nominal → Fault Occurs

Fault Management Process

The Fault
Fault Management Process Cycle

Knowing there’s a Problem

- Event reporting mechanisms
  - SNMP Traps/Informs
  - SYSLOG
  - Polling
  - Help Desk
- Collect to central repository
SAA Example

What to Do when You Get a Trap or Inform?

• Now’s the time to poll!
  Both the device itself and perhaps neighboring devices!

• This is known as event-based polling
When Did an Event Happen?

- Having the right time is very important
  Watch multiple time zones
- Use NTP

Fault Management Process Cycle
Definition

- Fault correlation: Tying of two or more events to a single fault or group of faults
- Fault correlation! = Diagnosis

Element-Based Correlation
Network-Based Correlation

Correlating Faults and Our SAA Example
Bunches of Events

Device Duplicates

WAN

Overload!

Remove Duplicates and Correlate

Fault Correlation
Fault Correlation Tools

• Rule-based systems that determine that two or more faults are related

• Good ones classify and prioritize as well
  
  Ciscoworks Device Fault Manager
    Device level only
  
  SMARTS inCharge
    Device and network
  
  Cisco Information Center
Fault Management Process Cycle

Fault Occurs → Detection → Correlation → Diagnosis → Correction → Nominal

Fault Management Process

Two Ways to Diagnose Problems

• Smart computers
• Smart humans
• Sometimes both
  
  See troubleshooting course
Root Cause Analysis

- Network-based mechanisms require some knowledge of topology
- Deals mostly with “hard” failures
- Usually limited to some subset of the network
- May determine a layer 1 failure, but not “Backhoe Syndrome”

Fault Management Process Cycle
Who Fixes those Problems?

- Network managers don’t know everything
- Workflow management is the process of delegating to the right person to fix the right problem in a timely fashion

Workflow Management

- Tools to track the state of network
- Used for escalation, division of labor, provisioning, and planning
- Examples include ‘remedy’ and ‘clarify’
How Important Is that Fault?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Time to Repair</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Remember this Slide?

IP Connectivity Identifies Issues Fault Management May Not See and Directs Operators at Service Impacting Faults

- IP Connectivity Not Impacted
- Latency Might Be
- Operations See a Fault but Does It Impact on Customer Service?
Work Flow Management

Importance

High
Moderate
Low

Management

IP
Web
Voice
DBA

Function

Helping the NOC

Importance

High
Moderate
Low

Management

Maintenance Window

Function

NOW!

Fault Correlation
Multiple Sources and Prioritizing

Function

- Low
- Moderate
- High

Management

IP
Web
Voice
DBA

Fault Correlation

warmStart

authFailure Trap

Disk Space 90%

Multiple Sources and Prioritizing

And All is Quiet…for now!

Suddenly…

The Network is DOWN

Fault Detection

Nominal Management Process

Fault Occurs

Nominal at Last!

Correction

Diagnosis

Correlation
Agenda

✓ Fault Management Tuning Cycle
  Baseline Network
  Setup Alarms and Thresholds
  Excessive/Missed Faults
  Nominal

✓ Fault Management Process Cycle
  Fault Occurs
  Detection
  Correlation
  Diagnosis
  Correction
  Nominal

• Tools

CiscoWorks Device Fault Manager
CiscoWorks Device Fault Manager
CiscoWorks Device Fault Manager

CiscoWorks RME Syslog Analysis
Tools Issues

Internetwork Performance Monitor

- Measure latency end-to-end and hop-by-hop
- Measure latency using synthetic traffic (TCP connect, DNS, DHCP, voice, etc.)

Tools Issues

- Internetwork Performance Monitor (IPM)
  - CiscoWorks network management application
  - Access IPM server using web-based clients
- Service Assurance Agent (SAA)
  - Embedded in Cisco IOS®
Tools Issues

Internetwork Performance Monitor

• Analysis of end-to-end network delay
• Identify network bottlenecks
• Identify and measure performance for all available layer 3 network paths
• Provide real-time and historical reports and graphs on network-wide VoIP characteristics including: Jitter, latency, and dropped packets
• Generate alarms based on response time thresholds (SNMP notifications)
• Troubleshoot key components by measuring performance via hop-by-hop response time; identifies which network devices are introducing latency and jitter

CiscoWorks IPM
Summary

• Aim to tackle faults before they are visible to your users
• Know how to monitor each service
• Notification-based polling scales!
• Fault Management should significantly improve network availability
Recommended Reading

Performance and Fault Management

Available on-site at the Cisco Company Store

Other Network Management Sessions

Network Management
- NMS-1001 Introduction to Network Management
- NMS-2001 Network Troubleshooting Tools and Techniques
- NMS-1011 Principles of Fault Management
- NMS-2021 Configuration of Large-Scale Networks with CiscoWorks
- NMS-4021 Advanced Configuration Methods
- NMS-1031 Introduction to Collecting Traffic Accounting Information
- NMS-4031 Advanced NetFlow Accounting
- NMS-1041 Introduction to Performance Management
- NMS-2041 Performance Measurement with Cisco IOS Software
- NMS-4041 Advanced Performance Management with Cisco Service Assurance Agent
- NMS-1051 Securely Managing Your Network

Services
- NMS-1101 Understanding DNS and DHCP
- NMS-2102 Deploying and Troubleshooting NAT

High Availability
- NMS-1201 Improving Network Availability
- NMS-2201 Deploying Highly Available Enterprise Networks
Questions?

Please Complete Your Evaluation Form

Session NMS-1011