Understanding Fault Management
Session NCM-207

All of a Sudden…

• You’ve lost a third of your network
  —www.mybiz.com ping statistics—
  7 packets transmitted, 0 packets received,
  100% packet loss
What Happened?

- Did a router fail?
- Did several routers fail?
- Was there a fiber cut?
- Did path just to the network management station fail?

A Few Things to Remember

- Faults happen
- It’s easier to resolve problems before they affect your customers!
- Have appropriate instrumentation!
We’re Trying to Avoid this...

Fault Tolerance
Agenda

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

The Nice Picture

Workflow Management

Fault Correlation → Telco/ISP System
Agenda

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

The 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
Performance vs. Fault Management

Service Level Management

Users

Performance Management

Fault Management

Devices and Software

Sources

- Routers, switches, wires, fiber, PDUs, DNS servers, HVACs, power companies, squirrels, flooding, soft drinks, clumsy people, nuclear accelerators
Who Fixes Those Problems?

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

Agenda
Knowing There’s a Problem

- Fault reporting mechanisms
  - SNMP
  - SYSLOG
- How to configure them in the device

Architectural View of a Router

- CLI
- SNMP
- SYSLOG
- Higher Level Services
- Serial
- Fast Ethernet
- ATM
- OC48
- DS3
Basic SNMP Objects

- Defined in Management Information Base (MIB)
- Extensible tree-like structure
- Data content is self describing
  ASN.1 subset
- Semantics of each object is predefined

What’s in a MIB?

Mnemonic

sysUpTime OBJECT-TYPE
SYNTAX     TimeTicks
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

::= { system 3 }

How to Encode and Interpret this Variable

Parent

OID
Different Types in MIBs

- Counter32, Counter64
- TimeTicks (time)
- Gauge32
- DisplayString (usually with a size limit)
- Tables with indices

Which Objects Does Cisco Support?

- Mandatory: MIB-II and IF-MIB
  Describes which products support which MIBs
  Also has the MIBs themselves
More Information

- Look at OID directory, as well!
  (especially useful when using free SNMP tools)

SNMP Security

“SNMP is Insecure”

True (with v1 and v2c communities)

And False (with v3 users)

V3 users and passwords NOT stored in normal config
In Cisco IOS

- The simple way:
  snmp-server community PASSWORD [ro|rw] [ACL]
- Allows access to all access on the router for a given ACL
- By itself is a mistake

Security

- SNMP should only be accessible to NMS
- Use ACLs where appropriate
- Use v3 where available
Recent Advisory

- Hidden community string “ILMI”
- Different protections required for different releases
- “show snmp group”
- Check WWW.CISCO.COM for details

Silliness

- The entire MIB tree can be retrieved from a device
- Doing so WILL cause problems
- This can be prevented with views
SNMP Views

- enterprises
- rttmon
- interfaces
- bgp
- ipRouteTable

SNMP Views

- enterprises
- rttmon
- interfaces
- bgp
- ipRouteTable
SNMP Views

- Cisco IOS command:
  
  \texttt{snmp-server view VIEWNAME OID-tree [include|exclude]}

- Followed by
  
  \texttt{snmp-server community PASSWORD view VIEWNAME [ro|rw]}

- This prevents a runaway tree walk, and also limits access to necessary objects

SNMP View Security

- There’s an advisory
  
  \texttt{router(config)#snmp-server view novacm internet included}
  \texttt{router(config)#snmp-server view novacm internet.6.3.16 excluded}
  \texttt{router(config)#snmp-server community public view novacm RO}

- See CCO
Common Example: The IF-MIB

An entry for serial 0/0:

<table>
<thead>
<tr>
<th>Name</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.1</td>
<td>InterfaceIndex</td>
</tr>
<tr>
<td>mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1</td>
<td>INTEGER</td>
</tr>
<tr>
<td>mgmt.mib-2.ifMIB.ifTable.ifEntry.ifInDiscards</td>
<td>Counter32</td>
</tr>
</tbody>
</table>

Contained in LinkUp/LinkDown Traps

Not in a Predefined trap, but Indicates Problems

A Router...

Interface Serial 1/0
...ifTable.ifEntry.ifOperStatus.1
...ifTable.ifEntry.ifInDiscards

Interface Serial 1/0.1
...ifTable.ifEntry.ifOperStatus.2
...ifTable.ifEntry.ifInDiscards

Interface Serial 1/0.2
...ifTable.ifEntry.ifOperStatus.3
...ifTable.ifEntry.ifInDiscards

Interface Serial 1/1
...ifTable.ifEntry.ifOperStatus.4
...ifTable.ifEntry.ifInDiscards

Interface Serial 1/1.1
...ifTable.ifEntry.ifOperStatus.5
...ifTable.ifEntry.ifInDiscards

Interface Serial 1/1.2
...ifTable.ifEntry.ifOperStatus.6
...ifTable.ifEntry.ifInDiscards
Difference between Ping and SNMP

Ping

Session/Application
Transport
Internet
L2

SNMP
MIB-2, BGP...
Ethernet MIB...

Polling vs. Notifying

- Polling: NMS asks for status
- Notifying: Device actively notifies NMS of problems
- Two types of notifications
  - Trap—unreliable, no state retained
  - INFORMs
Cost of Polling

- Query and response per object
- X each device
- Every N seconds

More Math

- Checking interface status of 20 interfaces = 20 queries
- X 100 devices = 2000 queries
- Basic query for ifInOctets = ~ 87 byte query and 90 byte response
Cost of Queries

Bytes to Bits: 277,600—and those Are Interfaces

Cost of Traps

- No queries
- But you may need to poll for other reasons (performance metrics)
- SMART polling engines can really make the difference!
SNMP Trap Reliability

“SNMP Traps are Unreliable”

True… Use v2c Informs!

Traps and Informs

- Trap

- Inform

Acknowledgement
Configuring Traps

- Basic command
  ```snmp-server enable traps [notification type] [options]
  (bgp, config, entity, frame-relay, isdn, rtr, snmp)
  snmp-server host 10.1.1.1 version v2c community
  ```
- Turns on different types of traps

Configuring Informs

- Requires “ENTERPRISE-PLUS”
  ```snmp-server enable traps (...) snmp-server host 10.1.1.1 informs (...)
  ```
Checking Your Configuration

- Check your trap server log
- “Show snmp pending”
- “Show snmp sessions”

SNMP Version Differences

<table>
<thead>
<tr>
<th></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>No</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>
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 trap-based polling

What Happens if a MIB Doesn’t Exist?

- Information may be found using SYSLOG

- SYSLOG produces (mostly) structured logs of information

- Tools such as sniff, Cisco Info Center consume SYSLOG
Looking for Notifications in MIBs

- Two ways:
  - Check the documentation
  - Spot it in your NMS

Checking the Documentation

```
rttMonTimeoutNotification NOTIFICATION-TYPE

OBJECTS {  rttMonCtrlAdminTag,
            rttMonHistoryCollectionAddress,
            rttMonCtrlOperTimeoutOccurred

}  

STATUS current

DESCRIPTION

"A rttMonTimeoutNotification indicates the occurrence of a timeout for a RTT operation, which indicates the clearing of such a condition by a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperTimeoutOccurred changing value.

When the RttMonRttType is 'pathEcho', this notification will only be sent when the timeout occurs during an operation to the target and not to a hop along the path to the target. This also applies to the clearing of the timeout.

If History is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not 'echo' or 'pathEcho', the rttMonHistoryCollectionAddress object will be null.

::= { rttMonNotifications 2 }"
```
What’s Nominal?

- Some problems are detected by noticing a configuration change or a performance problem
- Take a baseline of performance metrics when times are good

SAA and CISCO-RTTMON-MIB

- Service assurance agent
- Session level probe
- Generates availability and threshold traps
- Also collects statistics
Configuring SAA

```
(config)# rtr 1
(config-rtr)# type http operation get url http://www.cisco.com
(config-rtr)# exit
(config)# rtr schedule 1 start-time now
(config)#
```

RTT-MON Traps

- rttMonConnectionChangeNotification
- rttMonTimeoutNotification
- rttMonThresholdNotification
SAA Example

Going Up the Stack
Know Thy Router!

CISCO-PROCESS-MIB

- SNMP version of “show process”
- Provides CPU usage
How Useful Is Trap-based Polling?

“There are so few traps!”

There are as many traps as there are MIB variables!

Set a Threshold

• RMON alarms
  Command line accessible

• DISMAN-EVENT-MIB
  Has wildcards, better variety of tests

System Polls Itself!
Checking CPU Using RMON

- RMON alarm enterprises.9.109.1.1.1.4.1
  60 absolute rising-threshold 90 1
  falling-threshold 50
  Tests the OID (CPU utilization found in CISCO-PROCESS-MIB)
  If the absolute value exceeds 60 (%)
  fire event 1
  Reset the alarm when the value falls below 50%

Tools Available

- Tons
- Check out CCO and partners
- See also: http://dmoz.org/Computers/Software/Networking/Network_Performance/RMON_and_SNMP/
SYSLOG

- Very basic reporting mechanism
- Very basic “standard”
- Text messages on UDP port 540

SYSLOG Format

```
<Priority> NETASCII "0"
```

```
<Priority> Apr 18 12:02:34 upstairs /usr 90% full
```
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 v1 or v2c traps
- One way: no query capability
- Priority isn’t consistently used
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 messages

Configuring SYSLOG

- Logging command
  sets host, facility, rate limit, and more
When Did an Event Happen?

- Having the right time is very important
  Watch multiple timezones
- Use NTP
  (You’ll see this again ;-)
Definition

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

Element Based Correlation

Router A

ATM CLOUD

LinkDown(1, up, down)
BGPdown(B)

Router B
Router C
Router D
Router E
Router F
Network-Based Correlation

Correlating Faults and Our SAA Example
The Nice Picture

Workflow Management

Fault Correlation

Telco/ISP System

Bunches of Events

Device Duplicates

Overload!
Remove Duplicates and Correlate

Hierarchical Mechanisms
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
- Cisco Information Center

NMS Placement

Avoid Flying Blind
The Cadillac Solution

- Monitoring doesn’t impact your live network bandwidth
- Same CPU cost
- Costs more money
- Screws up auto-discovery

Keep Management Net Routing Simple!
Use HA Principles for Network Management!

- Have redundant connectivity all the way to the NMS
- Have multiple DNS servers near by
- Have sufficient bandwidth to poll (when needed)
- Have reliable AAA; if you can’t get in, you can’t fix the problem

Agenda

- Fault Occurs
- Nominal
- Fault Management Process
- Detection
- Correlation
- Diagnosis
- Correction
Two Ways to Diagnose Problems

- Smart computers
- Smart humans
- Sometimes both

See troubleshooting course

Root Cause Analysis
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”
Agenda

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?

- Importance
  - High
  - Moderate
  - None

- Time to Repair

Work Flow Management

- Importance
  - High
  - Moderate
  - Low

- Function
  - Management
  - IP
  - Web
  - Voice
  - DBA
Helping the NOC

- **NOW!**
  - High Importance
  - Management
    - IP
    - Web
    - Voice
    - DBA
  - Fault Correlation
- Maintenance Window

Multiple Sources and Prioritizing

- **warmStart**
  - Fault Correlation
  - authFailure trap
  - Disk space 90%
- Function
  - High
  - Moderate
  - Low
Without the Pretty Pictures

```plaintext
traphandle rmon.rmonEventsV2.risingAlarm dispatchIP

grep $host ignore-these-hosts.txt > /dev/null
if (status == 0) exit
switch (alarmVariable)
openCase(CPU, ThresholdValue == 99 ? Urgent : Medium)
```

Summary

- Move away from the fishbowl approach
- Aim to tackle faults before they are visible to your users
- Know how to monitor each service
- Trap based polling scales!
Thanks!

Understanding Fault Management

Session NCM-207
Please Complete Your Evaluation Form

Session NCM-207