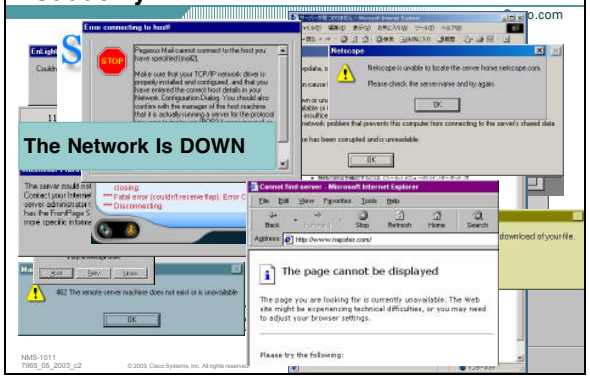
NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Cisco Systems

Suddenly…

Cisco.com



Cisco.com

Understanding Fault Management

Session NMS-1011

Do You Know What Went Wrong?

Cisco.com

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

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

A Few Things to Remember

Cisco.com

- 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

Sources

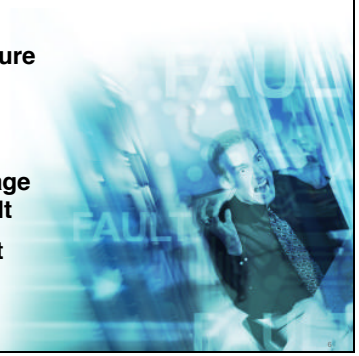
Cisco.com

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

What Is a Fault?

Cisco.com

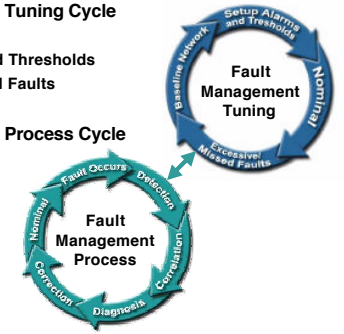
- A fault is an unplanned failure of software, hardware, or wetware
- Not every outage is due to a fault
- Not every fault results in an outage



Agenda

Cisco.com

- 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



Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Fault Management Tuning Cycle

Cisco.com

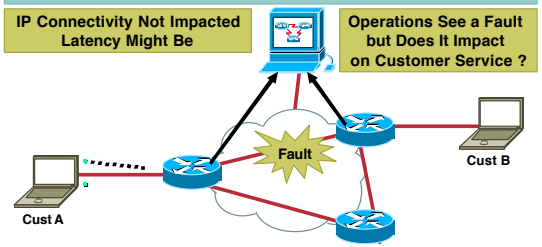
IP Connectivity and Fault Management

Cisco.com

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 ?



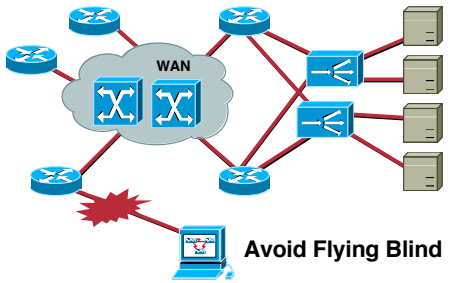
Baselining—What's Nominal?

Cisco.com

- **Take a baseline of your network when times are good**
- **Include:**
  - **Network and wiring diagrams**
  - **Device configurations**
  - **Performance metrics**
  - **Service level agreements (SLAs)**

NMS Placement

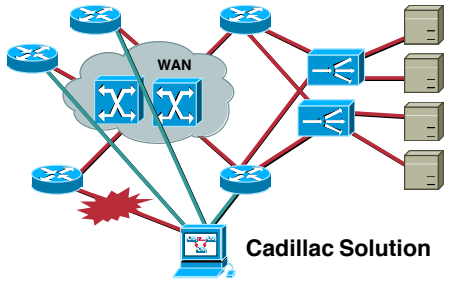
Cisco.com



Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

NMS Placement

Cisco.com



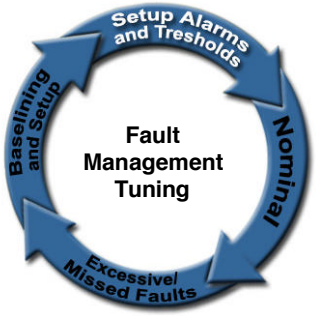
Use High-Availability Principles for Network Management!

Cisco.com

- 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

Cisco.com



Setup Alarms and Thresholds

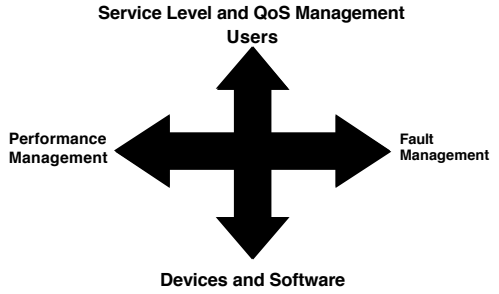
Cisco.com

- 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

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Management Domain

Cisco.com



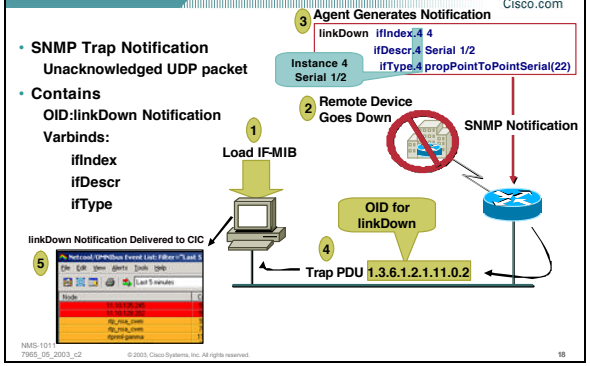
NMS-1011
7965_05_2003_c2

17

SNMP Trap Notification

Cisco.com

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



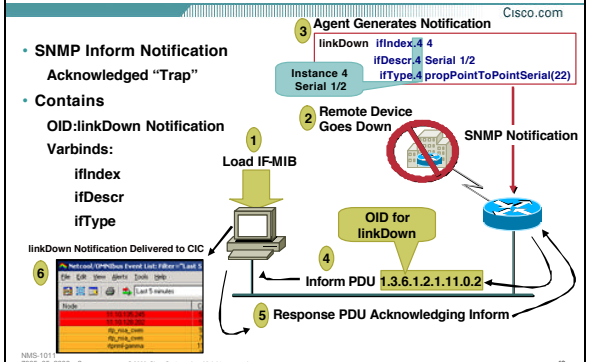
NMS-1011
7965_05_2003_c2

18

SNMP Inform Notification

Cisco.com

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



NMS-1011
7965_05_2003_c2

19

SNMP Version Differences

Cisco.com

	Version 1	Version 2c	Version 3
Informs	No	Yes	Yes
RMON/Event	Yes	Yes	Yes
Authentication	Community	Community	Users
Privacy	No	No	Yes
IOS/CATOS	Supported	Supported	Supported
NMS Support	Ubiquitous	Pretty Good	Limited

NMS-1011
7965_05_2003_c2

20

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Which Objects Does Cisco Support?

Cisco.com

Mandatory: MIB-II and IF-MIB

- **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

- **ftp://ftp.cisco.com/pub/mibs**
  - **Consider downloading the whole OID directory for quick searches**

How Useful Is Notification-Based Polling?

Cisco.com

"There Are So Few SNMP Notifications!"

There Are as Many Notifications as There Are MIB Variables!

Notifications

Cisco.com

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

Cisco.com

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!

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Example MIB to Create Notification from

Cisco.com

- **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

Cisco.com

- 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

Cisco.com

- **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

Cisco.com

- **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)**

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Event MIB

Cisco.com

- Show commands

  show management event

- Debug commands

  debug management event mib

Expression MIB

Cisco.com

- 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

Cisco.com

- 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

Cisco.com

- Show commands

  show management expression

- Debug commands

  debug management expression?

  Evaluator Expression MIB evaluator

  Mib Expression MIB SNMP operations

  Parser Expression MIB parsing

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

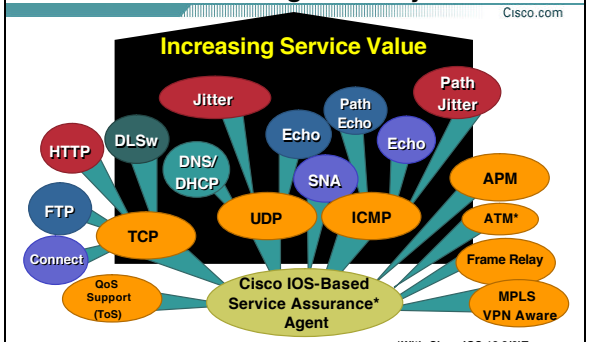
SAA and CISCO-RTTMON-MIB

Cisco.com

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

Service Assurance Agent Today

Cisco.com



*With Cisco IOS 12.2(9)T

Cisco IOS 12.0(5)T and 12.0(8)S—HTTP Operation

Cisco.com

- 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

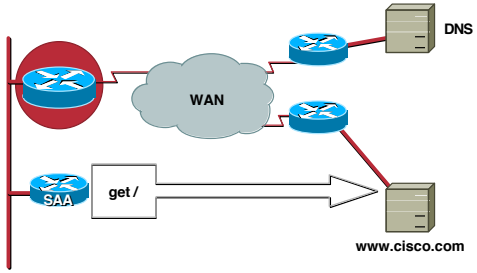
Cisco.com

- Defined in the CISCO-RTTMON-MIB
  - rttMonConnectionChangeNotification
  - rttMonTimeoutNotification
  - rttMonThresholdNotification

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Know Thy Router!

Cisco.com



What Happens if a MIB Doesn't Exist?

Cisco.com

- 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

Cisco.com

- Very basic reporting mechanism
- Very basic "standard"
- Text messages on UDP port 514

Syslog Benefits

Cisco.com

- Easy to implement clients
- All ASCII (easy to manipulate)
- The UNIX standard

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

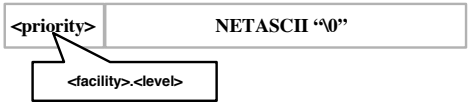
Syslog Problems

Cisco.com

- 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

Cisco.com



<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

Cisco.com

- %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?

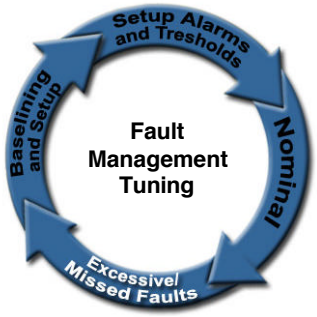
Cisco.com

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

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

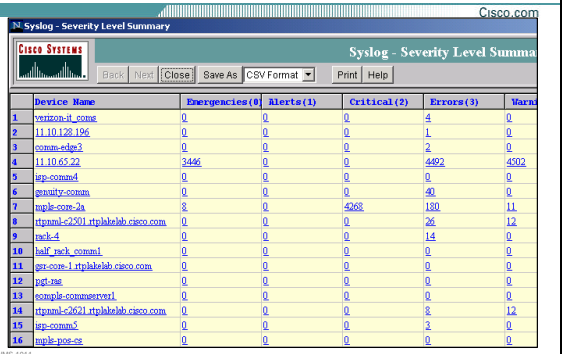
Fault Management Tuning Cycle

Cisco.com



Does Your Fault Console Look Like this?

Cisco.com



	Device Name	Emergencies(0)	Alerts(1)	Critical(2)	Errors(3)	Warn
1	verizon-it_comm	0	0	0	4	0
2	11.10.128.196	0	0	0	1	0
3	comm-edge3	0	0	0	2	0
4	11.10.65.22	3446	0	0	4492	4502
5	sip-comm4	0	0	0	0	0
6	gwunity-comm	0	0	0	40	0
7	mple-core-2a	8	0	4268	180	11
8	rtpnuml-c2501.rtplabelab.cisco.com	0	0	0	26	12
9	rack-4	0	0	0	14	0
10	leaf_rack_comm1	0	0	0	0	0
11	ger-core-1.rtplabelab.cisco.com	0	0	0	0	0
12	pgt-rac	0	0	0	0	0
13	ecmple-commserver1	0	0	0	0	0
14	rtpnuml-c2621.rtplabelab.cisco.com	0	0	0	8	12
15	sip-comm5	0	0	0	3	0
16	mple-pos-ce	0	0	0	0	0

Monitor Excessive or Missed Faults

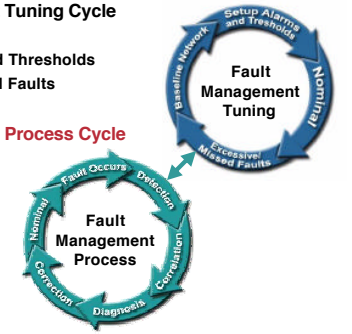
Cisco.com

- 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

Cisco.com

- ✓ 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

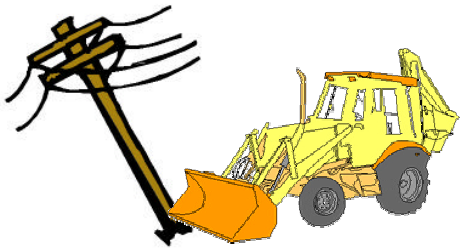


Fault Management Process Cycle

Cisco.com

The Fault

Cisco.com



Fault Management Process Cycle

Cisco.com

Knowing there's a Problem

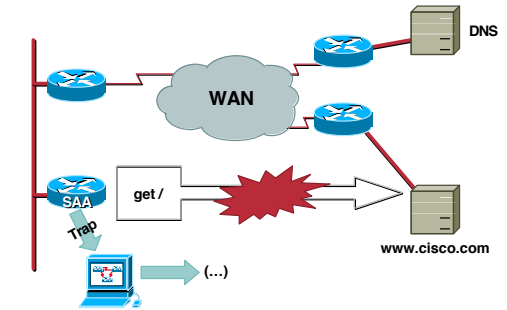
Cisco.com

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

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

SAA Example

Cisco.com



What to Do when You Get a Trap or Inform?

Cisco.com

- 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?

Cisco.com

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

Fault Management Process Cycle

Cisco.com

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

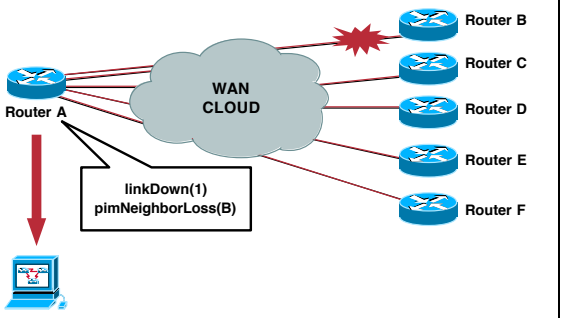
Definition

Cisco.com

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

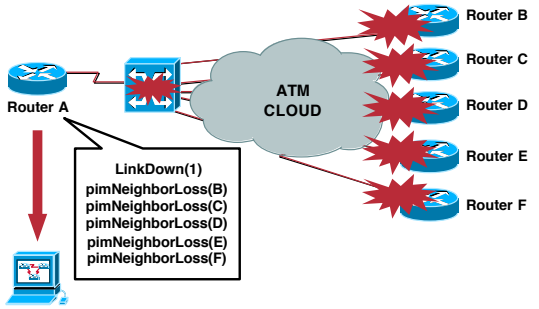
Element-Based Correlation

Cisco.com



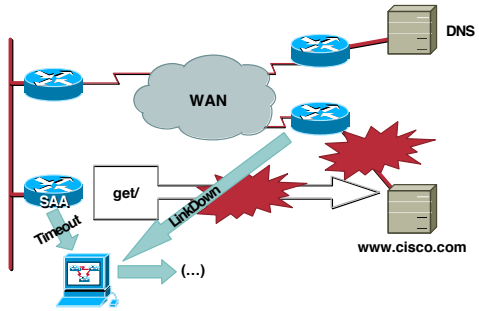
Network-Based Correlation

Cisco.com



Correlating Faults and Our SAA Example

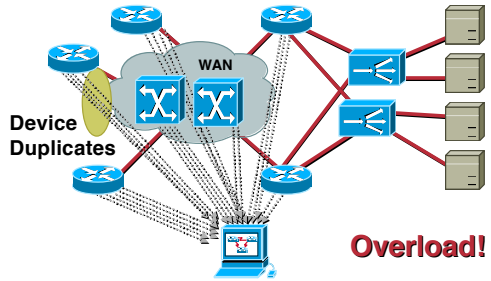
Cisco.com



Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

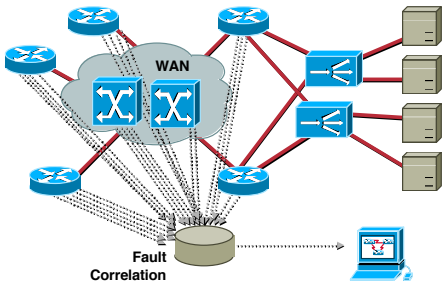
Bunches of Events

Cisco.com



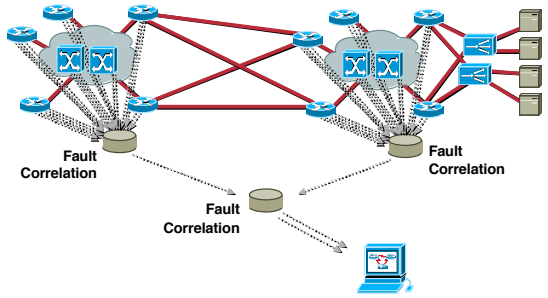
Remove Duplicates and Correlate

Cisco.com



Hierarchical Mechanisms

Cisco.com



Fault Correlation Tools

Cisco.com

- 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

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Fault Management Process Cycle

Cisco.com

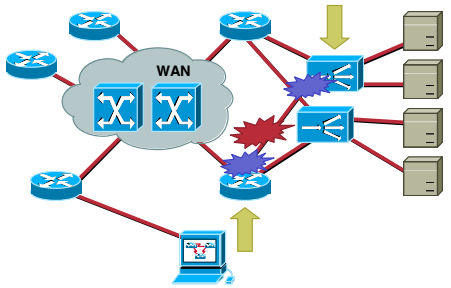
Two Ways to Diagnose Problems

Cisco.com

- Smart computers
- Smart humans
- Sometimes both
  - See troubleshooting course

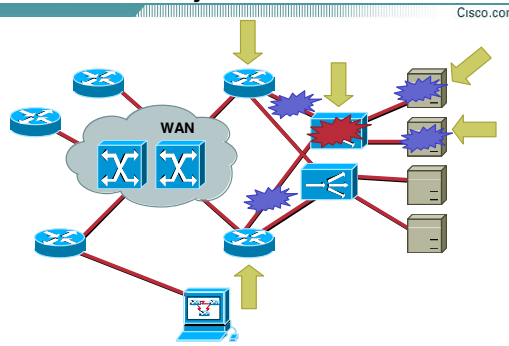
Root Cause Analysis

Cisco.com



Root Cause Analysis

Cisco.com



Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011

Root Cause Analysis

Cisco.com

- 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

Cisco.com

Who Fixes those Problems?

Cisco.com

- 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

Cisco.com

- Tools to track the state of network
- Used for escalation, division of labor, provisioning, and planning
- Examples include ‘remedy’ and ‘clarify’

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
NMS-1011