NETWORKERS 2004

GETTING THE RIGHT EVENTS FROM NETWORK ELEMENTS

NMS-3011

© 2004 Cisco Systems, Inc. All rights reserved.

This Tutorial Is …

- **NOT about**
  - **Fault Management Return On Investment**
  - **A level 1 type of presentation**
  - **Marketing slides**
  - **Polling the device to "discover" the fault**
  - **Fault Management Applications details**
- **about**
  - **How to generate the right events from your network elements!**

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

The Network Management TAC Team in EMEA

Cisco.com

Polling vs. Event Notification

Cisco.com

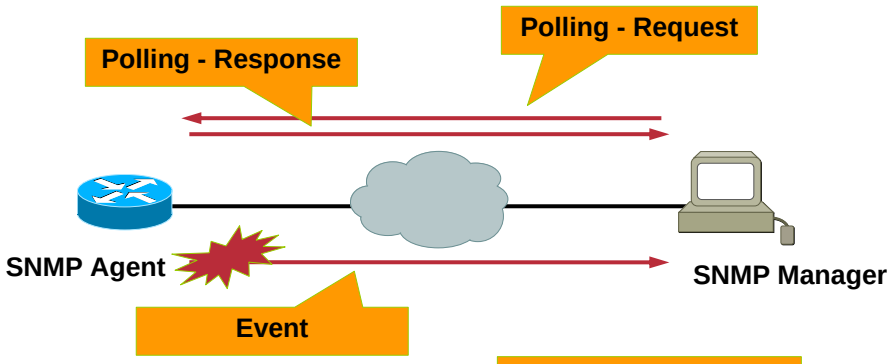
- Network sizes are getting larger and larger
- Polling for Fault Management doesn't always scale
- Event Notification
  - Sent only at the occurrence of a fault
  - Allows to tune fault management to your users and network
- Message:
  - Let the network elements monitoring themselves
  - Let's tune the right fault management events from the network elements

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Polling vs. Event Notification

Cisco.com



After the event …
Then potentially some event based polling

© 2004 Cisco Systems, Inc. All rights reserved.

Polling vs. Event Notification

Cisco.com

	Polling	Event
Load on	Network Manager Station, Links, Network devices	Network engineer, initially, to configure the event
Application	Performance Management (Availability monitoring, Utilization and Forecasting) Fault Management	Proactive Fault Monitoring, Operational Monitoring

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Agenda

Cisco.com

- SNMP Notification: Traps and Informs
- Syslog Message
- RMON Event / Alarm
- EVENT-MIB
- EXPRESSION-MIB
- Specific Scenarios
- Embedded Event Manager
- Embedded Syslog Manager

© 2004 Cisco Systems, Inc. All rights reserved.

SNMP NOTIFICATION

EVERYBODY KNOWS ABOUT TRAPS!

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

SNMP Notifications

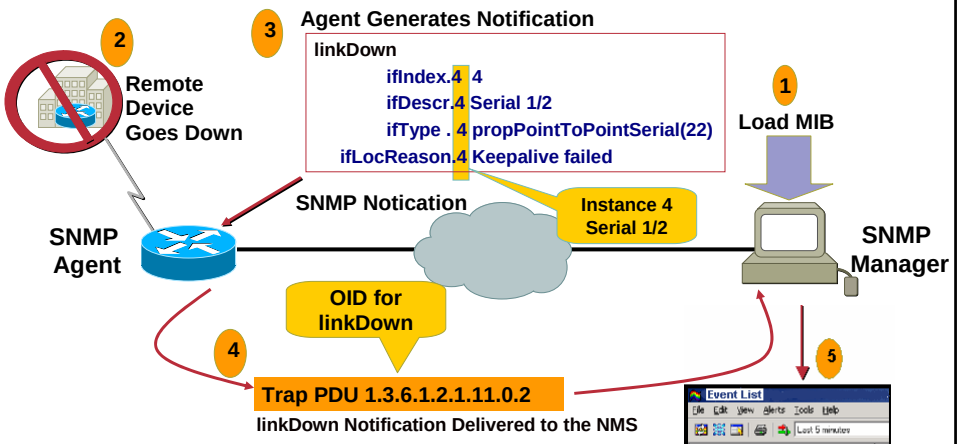
Cisco.com

- Notifications are the messages being generated from the SNMP Agent, regardless of the mechanism to deliver them
- SNMP Notification implemented in SNMPv2:
  - Traps
    - Unacknowledged UDP packet
    - Implemented since SNMPv1
  - Informs
    - Acknowledged UDP packet
    - Implemented since SNMPv2c

© 2004 Cisco Systems, Inc. All rights reserved.

SNMP Trap Notification

Cisco.com



SNMP trap notification contains:

Varbinds: ifIndex, ifDescr, ifType, ifLocReason

OID: linkDown Notification

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Enable SNMP Traps Notification?

Cisco.com

- On a Cisco Router:

```
Router (config)# snmp-server enable traps
<trap_type>
Router (config)# snmp-server host <NMS host>
version <v1/v2c/v3 [auth | noauth | priv]>
<trap_community> <trap_type>
```

- On a Cisco Switch:

```
Switch>(enable) set snmp trap enable <trap_type>
Switch>(enable) set snmp trap <NMS_host>
```


© 2004 Cisco Systems, Inc. All rights reserved.

Traps - Show Commands

Cisco.com

```
Router#show snmp
…
22689 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    229 No such name errors
    0 Bad values errors
    0 General errors
    22450 Response PDUs
    172 Trap PDUs

SNMP logging: enabled
Logging to 10.48.71.130.162, 0/10, 86 sent, 0 dropped.
Logging to 144.254.7.167.162, 0/10, 85 sent, 1 dropped.
```

Router(config)# snmp-server queue-length <length>

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

SNMP V2 Notification

Cisco.com

```
Router(config-if)# shut
Nov 21 07:44:17: %LINK-3-UPDOWN: Interface Serial1/2, changed state
to down
4d23h: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 43061874
snmpTrapOID.0 = snmpTraps.3
ifEntry.1.23 = 23
ifEntry.2.23 = Serial1/2
ifEntry.3.23 = 24
lifEntry.20.23 = administratively down
```

© 2004 Cisco Systems, Inc. All rights reserved.

linkUp/linkDown Notification

Cisco.com

```
linkDown
        ifIndex.4  4
       ifDescr.4 Serial 1/2
        ifType .4 propPointToPointSerial(22)
  locIfReason.4 keepalive failed
```

Instance 4
Serial 1/2

```
linkDown
        ifIndex. 4  4
 ifAdminStatus.4 Down
   ifOperStatus.4 lowerLayerDown
```

Cisco redefinition
CISCO-GENERAL-TRAPS

IETF notification
IF-MIB
(RFC2233/RFC2863)

```
router(config)# snmp-server trap link ietf
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Enable SNMP Inform Notification?

Cisco.com

Enable trap and inform notifications. Ideally "notification" !

```
Router(config)# snmp-server enable traps ...
Router(config)# snmp-server host <host-id> informs
  version [2c | 3 [auth | noauth | priv]]
  <community-string>...
Router(config)# snmp-server informs [retries
  retries] [timeout seconds] [pending pending]
```

By default: 3 retries, 30 sec timeout, 25 informs pending for acknowledgement

- "snmp-server enable informs …" no functionality!
- Switches:
  so far, needed the SNMPv3 architecture
  8.3(1): simplified v2c inform CLI

© 2004 Cisco Systems, Inc. All rights reserved.

SNMP Inform Notification Format

Cisco.com

- InformRequest-PDU (Protocol Data Unit)

PDU type	Request-id	ErrorStatus =0	ErrorIndex =0	Variable-bindings

=0 =0

- Response-PDU =? =?

PDU type	Request-id	ErrorStatus	ErrorIndex	Variable-bindings

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Informs - Show Commands

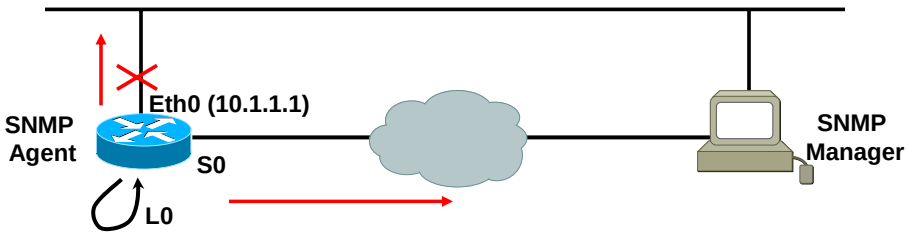
Cisco.com

```
Router#show snmp
…
SNMP Manager-role output packets …
    20 Inform-request PDUs
    0 Timeouts
    0 Drops
    …
SNMP Manager-role input packets …
    20 Response PDUs
    0 Response with errors
    …
SNMP informs: enabled
    …
…
SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 10.48.71.163.162
2 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```


© 2004 Cisco Systems, Inc. All rights reserved.

SNMP Source Trap Notification

Cisco.com




```
Router(config)# snmp-server trap-source ethernet 0
 (notification sent even if ethernet 0 is down)
```

Or even better

```
Router(config)# snmp-server trap-source loopback 0
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

SNMP Traps vs. Informs

Cisco.com

	Traps	Informs
Reliability	None	Some
Retries	Not Applicable	3 (default)
Resources	x	X
Source	Source Interface configuration	Not Implemented

© 2004 Cisco Systems, Inc. All rights reserved.

Notification and Time

Cisco.com

SNMPv2-Notification-PDU

sysUpTime in the device

PDU type	Request-id	ErrorStatus =0	ErrorIndex =0	Variable-bindings: sysUpTime …

- For alarms correlation, the right time is important
  - Use NTP between network elements
  - Use NTP between network elements and the notification receiver (attention to different timezone)
  - Note: SNMPv1 Trap also sends the sysUpTime
- Alarms correlation and informs:

  The management system must do alarms deduplication based on the time!

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Find Out about Traps and Informs?

Cisco.com

```
cognac(config)#snmp-server enable traps ?
  atm      Enable SNMP atm traps
  bgp      Enable BGP state change traps
  config   Enable SNMP config traps
  dial     Enable SNMP dial control traps
  dlsw     Enable SNMP dlsw traps
  …
```

- TAC Web document

  http://www.cisco.com/warp/customer/477/SNMP/SNMPTrapsInImages.html

- Working on “Traps & Syslog in Images”

© 2004 Cisco Systems, Inc. All rights reserved.

How to Find Out about Traps and Informs?

Cisco.com

- Provided in corresponding MIBs supported on Cisco devices.
- What device supports which MIB?

  http://www.cisco.com/go/mibs

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

NOTIFICATION-LOG-MIB

Cisco.com

- RFC-3014 “NOTIFICATION-LOG MIB”
- Notification buffer: allow a management station to retrieve notifications that have been missed.
- Notifications visualization without a receiver. Useful for troubleshooting!
- No persistence across reload

```
Router(config)#snmp mib notification-log ?
  default       create/configure default log
  globalageout  modify the global ageout
  globalsize    modify the global size
```


© 2004 Cisco Systems, Inc. All rights reserved.

NOTIFICATION-LOG-MIB

Cisco.com

```
Router#show snmp mib notification-log all
Notification ID cisco.0.1
sysUpTime when logged 4057361, Accessed by
1 log(s), contains 8 varbinds
Notification ID snmpTraps.4
sysUpTime when logged 4098180, Accessed by
1 log(s), contains 6 varbinds
```

- The MIB returns the MIB values, not the CLI

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

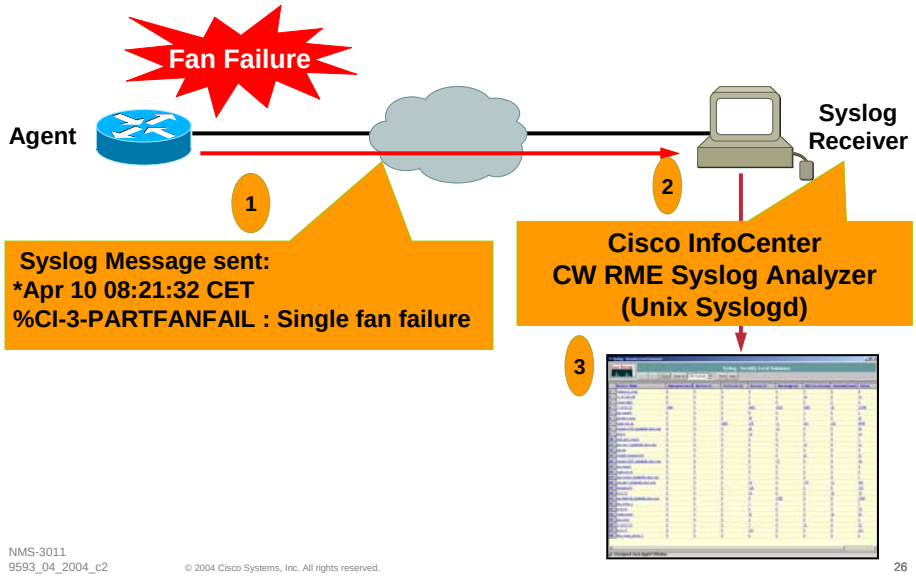
SYSLOG MESSAGE

WHAT HAPPENS IF THE NOTIFICATION DOESN'T EXIST?
OR IF THERE IS NO SNMP NOTIFICATION RECEIVER?

© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Message

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Syslog Message

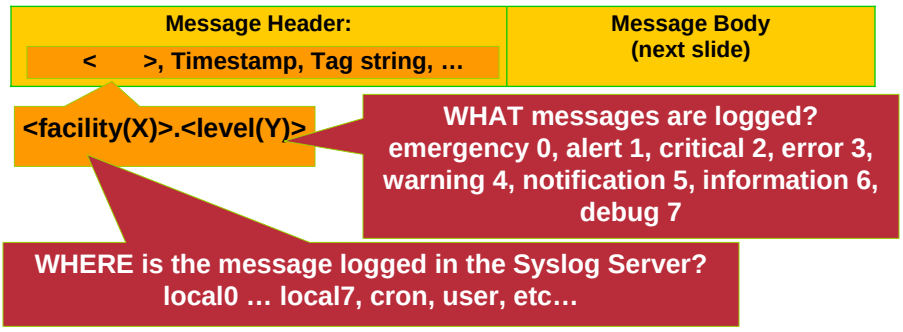
Cisco.com

- Syslog produces (mostly) structured logs of information. Allowing software subsystems to report and save important error messages either locally or to a remote logging server
- Very basic reporting mechanism: no variable bindings, plain english text
- Very basic “standard”, now an Informational RFC 3164
- Text messages sent to a Syslog daemon, on UDP port 514
- Syslog message is complementary to other events (SNMP notifications)

© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Message Format

Cisco.com



- <facility.level> is not retained in the Syslog message file
- Additional timestamp is added by logging host
- Header example

  Message Header: local7.emergency

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Enable Syslog Message on Cisco IOS?

Cisco.com

- On a Cisco Router:

```
Router(config)# logging on
Router(config)# logging <server_ip_address>
Router(config)# logging facility local6
Router(config)# service sequence-numbers
Router(config)# service timestamps log
[datetime | uptime]
Router(config)# service timestamps log datetime
[msec] [localtime] [show-timezone] [year]
```

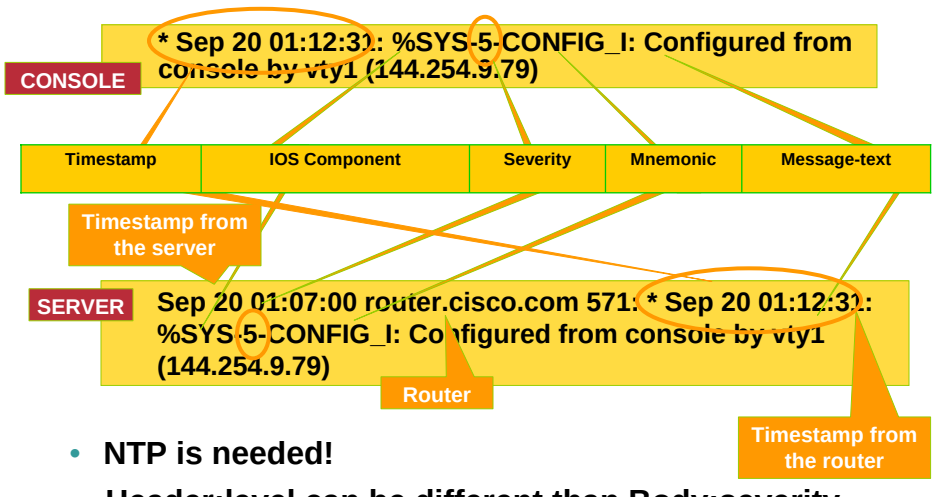
Optional: default is in UTC with no milliseconds and no time zone

Note: UTC, Universal Time, since 1970

© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Message "Body" Format in the Cisco IOS

Cisco.com



- NTP is needed!
- Header:level can be different than Body:severity

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Syslog - Show Commands on Cisco IOS (Cont.)

Cisco.com

```
Router# show logging
Syslog logging: enabled (0 messages dropped, 13 messages rate-limited, 0
flushes, 0 overruns)
   Console logging: level debugging, 34 messages logged
   Monitor logging: level debugging, 0 messages logged
   Buffer logging: level debugging, 47 messages logged
   Logging Exception size (8192 bytes)
   Trap logging: level debugging, 51 message lines logged
      Logging to 10.48.71.225, 51 message lines logged

      Log Buffer (8192 bytes):
      *Apr 10 08:21:32 CET: %SYS-5-RESTART: System restarted --
      *Apr 10 08:21:32 CET: %SNMP-5-COLDSTART: SNMP agent on host popo is
                                 undergoing a cold start
      *Apr 10 08:21:32 CET: %LINK-5-CHANGED: Interface FastEthernet5/1,
                                 changed state to administratively down
```


© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable Syslog Message on Catalyst OS?

Cisco.com

- On a Cisco Catalyst Switch:

```
Switch(enable)> set logging session enable
Switch(enable)> set logging server
<Server_ip_address>
Switch(enable)> set logging server facility
local7
Switch(enable)> set logging server severity 3
Switch(enable)> set logging console enable
Switch(enable)> set logging timestamp enable
```

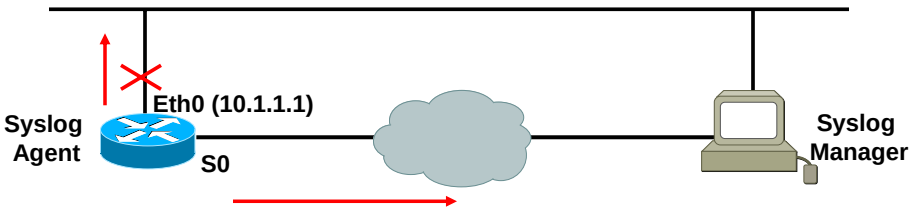
Local time configured on the switch (Optional)

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Syslog Source Interface

Cisco.com




```
Router(config)# logging source-interface loopback 0
```


© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Message Filtering: Example 1

Cisco.com

- How to get the error messages which have severity level equal or lower than error?

```
Router(config)# logging 10.10.10.10
Router(config)# logging facility local6
Router(config)# logging trap errors
Router(config)# logging console debugging
```

Confusing! Should be level!!

(the one in the syslog header)

- On the Syslog server(UNIX), the corresponding line in Syslog.conf file is:

```
local6.errors                    /var/log/mylog
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Syslog Message Filtering: Example 2

Cisco.com

- How to only log the error messages related to spanning tree?

```
Switch> (enable) set logging session enable
Switch> (enable) set logging server 10.10.10.10
Switch> (enable) set logging server severity 0
Switch> (enable) set logging level spantree 0
Switch> (enable) set logging server facility local5
Switch> (enable) set logging console enable
```

- On the Syslog server(UNIX), the corresponding line in Syslog.conf file is:

```
local5.emerg                    /var/log/spantree
```


© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Messages vs. SNMP Notifications

Cisco.com

	Syslog	Notification
NMS	Syslog Daemon	Trap receiver
Protocol/Port	UDP 514	UDP 162
Filtering	Yes	Limited
Format	easy-to-read format, No MIB needed	More rigid format, parse able
Reliability	None (RFC 3195 reliable syslog)	None with traps Some with informs (NOTIFICATION-LOG MIB)

Note: the syslog message could be sent faster!

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Convert a Syslog Message to a SNMP Notification?

Cisco.com

- Why?
  - Not all error messages are supported via notifications
  - Syslog daemon not running in the NMS
  - Events correlation need
- Send a trap/inform from the CISCO-SYSLOG-MIB when a new syslog message is generated
- How to convert to a trap?

```
Router (config)# snmp-server enable traps syslog
```

Attention to the <all> keyword !!!

- How to convert to an inform?

```
Router (config)# snmp-server host <x.x.x.x>
        informs version 2c public syslog
```


© 2004 Cisco Systems, Inc. All rights reserved.

Syslog Writing to Flash

Cisco.com

- System error and debug messages saved on the router's CompactFlash Disks (also known as ATA Flash disks)
- Persistent across reboot
- Introduced in 12.0(26)S

```
Router(config)# logging buffered
Router(config)# logging persistent url
      disk0/syslog size 134217728 filesize 16384

Router# copy slot0:/syslog
      ftp://myuser/mypass@192.21.1.129/syslog
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Syslog Issue
Consistent Message Format

Cisco.com

- **Syslog isn't consistently used across different Cisco Platforms and IOS versions**

  Example: environmental monitor initiated shutdown event

  IOS 11.2 -> ENVM-1-SHUTDOWN

  IOS 12.0 -> ENVM-0-SHUT

© 2004 Cisco Systems, Inc. All rights reserved.

How to Find Out about Syslog Messages?

Cisco.com

- **'Cisco IOS Software System Error Messages' per IOS release**

  For IOS version 12.2:
  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_system_message_guide_book09186a008009e73d.html

- **'System message' per Cisco Switch, Cisco 6000 switch:**

  http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_system_message_guide_chapter09186a00800f2709.html

- **Error Message Decoder**

  http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl

- **Output Interpreter**

  https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

XML Interface to Syslog Messages

Cisco.com

- Enable syslog messages to be sent in an Extensible Markup Language (XML) format
- Logs in a standardized XML format can be more readily used in external customized monitoring tools
- Tags are hard-coded
- Available in 12.2(15)T
- Configuration:

```
Router(config)#logging console xml
Router(config)#logging monitor xml 6
Router(config)#logging host 128.107.165.215 xml
Router(config)#logging host 171.69.1.129
Router(config)#logging buffered xml 10000
```


© 2004 Cisco Systems, Inc. All rights reserved.

XML Interface to Syslog Messages Events Comparison

Cisco.com

```
000013: *Oct 11 14:52:10.039: %SYS-5-CONFIG_I:
   Configured from console by vty0 (172.19.208.14)
```

```
<ios-log-msg>
  <facility>SYS</facility>
  <severity>5</severity>
  <msg-id>CONFIG_I</msg-id>
  <seq>000013</seq>
  <time>*Oct 11 14:52:10.039</time>
  <args>
    <arg id="0">console</arg>
    <arg id="1">vty0 (172.19.208.14)</arg>
  </args>
</ios-log-msg>
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

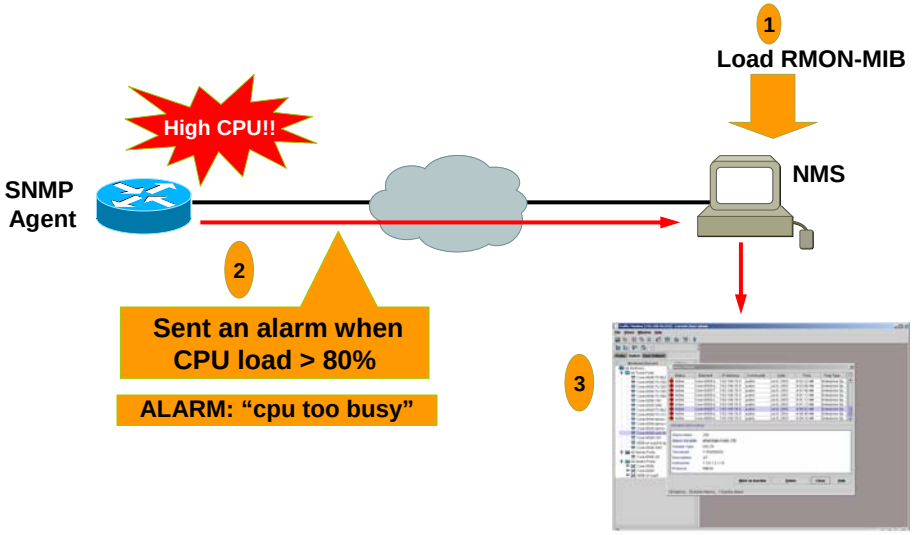
RMON EVENT AND ALARM

**SOMETIMES THE EXACT NOTIFICATION DOESN'T EXIST!
BUT THE SNMP OBJECTS TO TRIGGER THE NOTIFICATION
DO EXIST!**

© 2003, Cisco Systems, Inc. All rights reserved.

RMON Event and Alarm

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

RMON Event and Alarm

Cisco.com

- Allows Proactive monitoring:
  - The device polls itself
- RMON-MIB used to configure SNMP traps:
  - Traps, no informs (will be an enhancement)
  - Integer32, Counter32, Counter64, Gauge or Timeticks may be sampled
- Included in all Cisco IOS software images
  - since IOS 11.1
  - CLI or SNMP configuration
- Included in all the Switches images
  - Only SNMP configuration

© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable RMON Event and Alarm via CLI?

Cisco.com

- Configure RMON to generate a trap if CPU utilization reaches 80%, and rearm the trap if utilization drops below 40%, sampling interval is 20 seconds

T (sec)

```
Router(config)#rmon alarm 1
   cpmCPUTotalEntry.3.0 20 absolute
   rising-threshold 80 1 falling-threshold
   40 2 owner me
Router(config)#rmon event 1 log Trap
   public description "cpu busy" owner me
Router(config)#rmon event 2 log
   description "cpu not too busy"
```

Rising condition

Triggering event#1

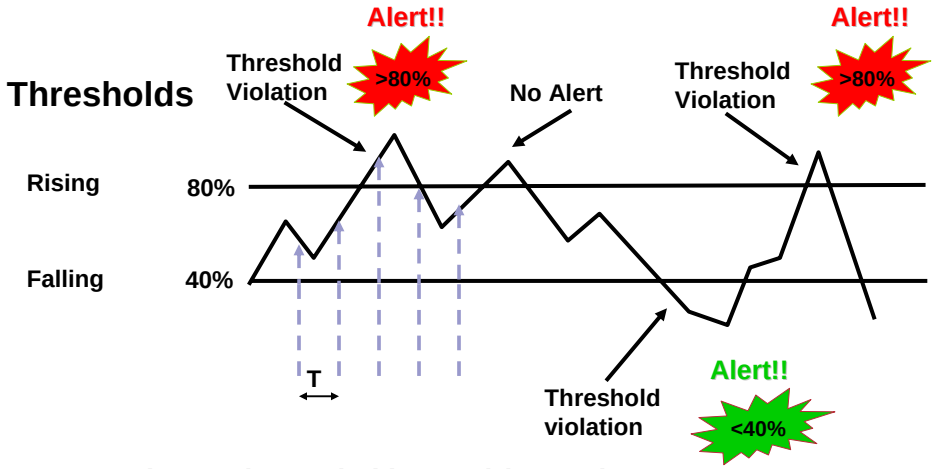
Triggering event#2

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

RMON Reaction Condition

Cisco.com



T: internal sampled interval (20 sec)

© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable RMON Event and Alarm via SNMP?

Cisco.com

- Send a trap when the number of bytes going into interface with ifIndex 12, during the last 2 minutes is above 140000000

```
snmpset -c private <router> eventStatus.123 integer 2
snmpset -c private <router> eventDescription.123 string “above 140000000“
snmpset -c private <router> eventType.123 integer 4
snmpset -c private <router> eventCommunity.123 string "public“
snmpset -c private <router> eventOwner.123 string "event_owner“
snmpset -c private <router> eventStatus.123 integer 1
snmpset -c private <router> alarmStatus.321 integer 4
snmpset -c private <router> alarmStatus.321 integer 2
snmpset -c private <router> alarmInterval.321 integer 120
snmpset -c private <router> alarmVariable.321 integer ifInOctets.12
snmpset -c private <router> alarmRisingThreshold.321 integer 140000000
snmpset -c private <router> alarmFallingThreshold.321 integer 10
snmpset -c private <router> alarmRisingEventIndex.321 integer 123
snmpset -c private <router> alarmOwner.321 string "alarm_owner"
snmpset -c private <router> alarmStatus.321 integer 1
```

eventIndex

AlarmIndex

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Which MIB Variables to Monitor?

Cisco.com

dot3StatsCarrierSenseErrors

bufferFail

ciscoEnvMonTemperatureState

cpmCPUTotal5min

ifOutDiscards

ciscoEnvMonFanState

bufferNoMem

locIfResets

locIfCollisions

locIfCollisions

ifOperStatus

ciscoMemoryPoolFree

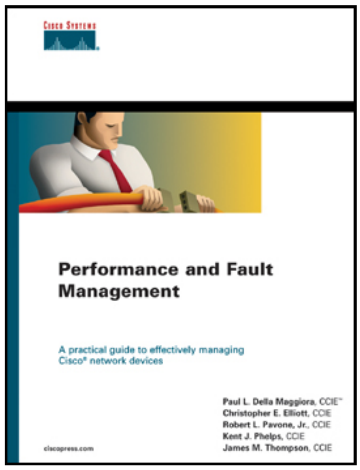
locIfInputQueueDrops

locIfCarTrans

locIfInCRC

bufferFail

locIfOutputQueueDrops



See the APPENDIX

© 2004 Cisco Systems, Inc. All rights reserved.

Fault Management
Which MIB Variables to Monitor?

Cisco.com

Interface

	Object Descr	OID	Poll Int	Threshold
locIfResets	number of times the interface internally reset	.1.3.6.1.4.1.9.2.2.1.1.17	15 min	
ifOperStatus	The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed	.1.3.6.1.2.1.2.2.1.8	5 min	!= 1
locIfCarTrans	Number of times interface saw the carrier signal transition	.1.3.6.1.4.1.9.2.2.1.1.21	15 min	
locIfCollisions	number of output collisions detected on this interface	1.3.6.1.4.1.9.2.2.1.1.25	15 min	
locIfInCRC	number of input packets which had cyclic redundancy checksum errors	.1.3.6.1.4.1.9.2.2.1.1.12	15 min	

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

ifIndex and RMON Persistence

Cisco.com

- **ifIndex persistence**

  Router

```
router(conf) snmp-server ifindex persist
router(conf-if) snmp-server ifindex persist
```

  Switch: ifIndex persistence by default

- **RMON persistence**
  - **Router: event/alarm saved in the startup configuration**
  - **Switch: no event/alarm persistence**

© 2004 Cisco Systems, Inc. All rights reserved.

RMON Event/Alarm Issue Mapping the 2 Events to the Alarm

Cisco.com

```
Router(config)#rmon alarm 1 cpmCPUTotalEntry.3.0 20
     absolute rising-threshold 80 1
     falling-threshold 40 2 owner me
Router(config)#rmon event 1 log trap public
     description "cpu busy" owner me
Router(config)#rmon event 2 log trap public
     description "cpu not too busy"
```

- **From the NMS point of view, no link between the event “cpu busy” and the alarm setting: MIB variable, threshold, sampling period**

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB

**SOMETIMES THE EXACT NOTIFICATION DOESN'T EXIST!
BUT THE SNMP OBJECTS TO TRIGGER THE
NOTIFICATION DO EXIST!**

© 2004 Cisco Systems, Inc. All rights reserved.

Event-MIB Advantages Versus RMON Event and Alarm

Cisco.com

- **The EVENT MIB provides a superset of the capabilities of the RMON alarm and event**
- **The EVENT MIB calls "triggers" The RMON MIB calls "alarms," but the concepts are the same**
- **More flexible test types with the EVENT-MIB**
  - **Existence test: absent, present, changed**
  - **Boolean test: <>, =, <, <=, >, >=**
  - **Wildcard**
- **Event MIB proposed by Cisco to IETF DISMON Working Group, accepted standard track RFC-2981**

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Event-MIB Advantages Versus RMON Event and Alarm

Cisco.com

- EVENT MIB can monitor
  - any MIB object (existence)
  - any integer/counter (boolean, threshold)
- RMON MIB can only monitor
  - integer/counter (threshold)
- EVENT-MIB allows alarms to be generated for MIB objects that are on another network element
- EVENT-MIB sends an SNMP notification in response to a trigger (like RMON) but add the concept of setting a MIB object (integers)
- EVENT-MIB can specify which variables to add to the notification

© 2004 Cisco Systems, Inc. All rights reserved.

EVENT-MIB: Example 1 Wildcarding

Cisco.com

- Wildcarding is a powerful functionality which allows you to monitor multiple instances of an object
- Can specify a single OID for monitoring, or use wildcarding to specify a group of OIDs
- Example:

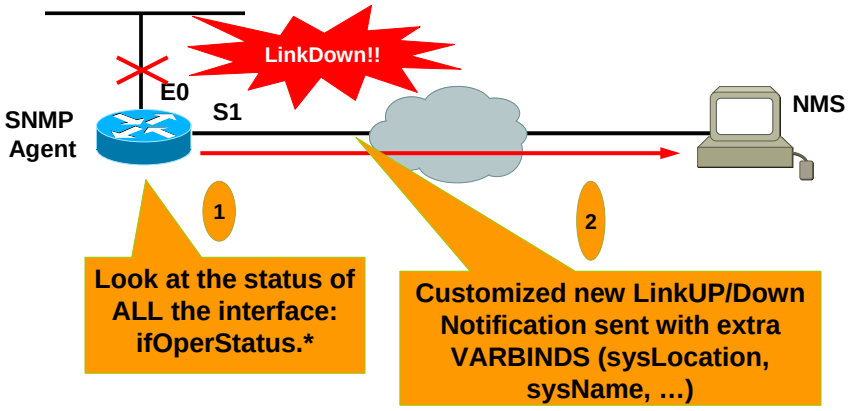
  monitor ifInOctets for all interfaces. The EVENT-MIB is configured to monitor the delta values of ifInOctets for all interfaces once per minute. If any of the samples exceed the delta rising or falling triggers, a trap notification will be sent

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB: Example 2
Add Variable to Notification

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

How to Find Out about EVENT-MIB Support in Cisco IOS?

Cisco.com

- Event MIB Support in Cisco IOS Release 12.1(3)T and 12.0(12)S
- RFC 2981-compliant support is in IOS release 12.2(4)T

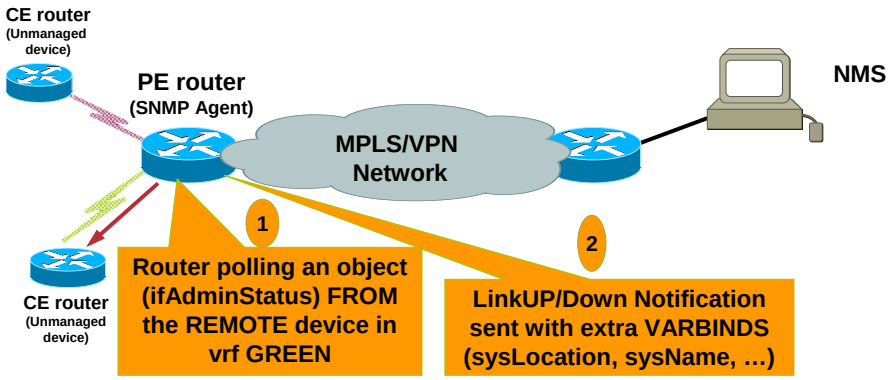
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800c391a.html
- Only SNMP support so far
- No CLI. Scriptable Interface for adding command line support in 13.(7)T

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB: Example 3
Remote Device Monitoring (foreseen by RFC)

Cisco.com



- "Remote monitoring uses the tag service of the Management Target MIB [RFC2573] to select and access remote systems as an ordinary SNMP- based management application.", RFC2981

© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable the EVENT-MIB?
Step 1. Any MIB Object Type

Cisco.com

- Each trigger is configured to watch a single object or a group of objects specified by a wildcard
- The object-type can be any one of the types:

INTEGER_TYPE	OCTET_PRIM_TYPE
NULL_TYPE	OBJECT_ID_TYPE
SEQUENCE_TYPE	INTEGER_32_TYPE
IP_ADDR_PRIM_TYPE	COUNTER_TYPE
GAUGE_TYPE	TIME_TICKS_TYPE
OPAQUE_PRIM_TYPE	COUNTER_32_TYPE
GAUGE_32_TYPE	UNSIGNED32_TYPE
COUNTER_64_TYPE	

However, the type of sampling dictates the types of objects that can be monitored

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Enable the EVENT-MIB? Step 2. Possibility: Sampling Type

Cisco.com

- The Event MIB process checks the state of this watched object at predefined intervals.
- The type of sampling that can be done on an object is of two types:
  - Absolute
  - Delta
- Configurable observation interval

© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable the EVENT-MIB? Step 3. Test Type and Parameters

Cisco.com

- The test that can be done on the watched object is one or a combination of the following:
  - Existence
    - Absent, Present, Changed
  - Boolean
    - Unequal, Equal, Less, LessOrEqual, Greater, GreaterOrEqual
  - Threshold
    - Rising, Falling, Rising or Falling

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

How to Enable the EVENT-MIB? Step 4. Actions

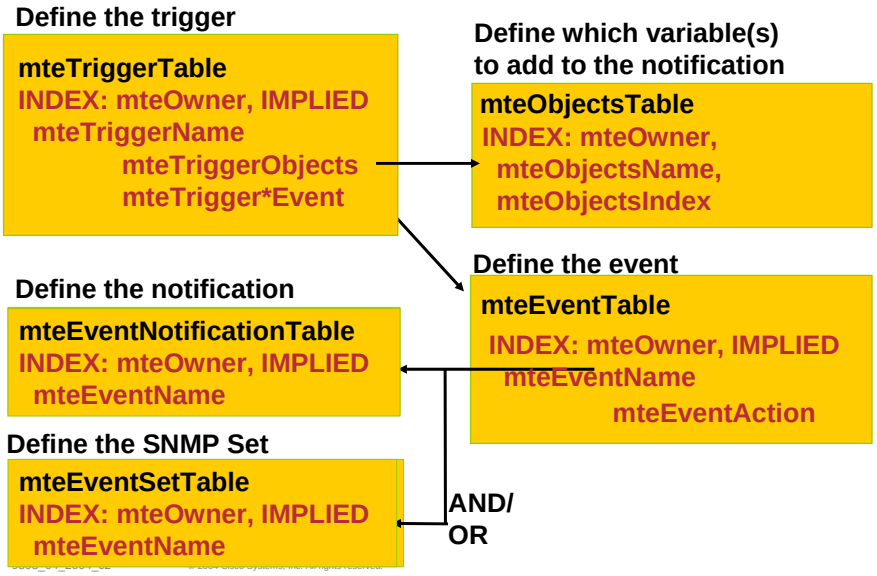
Cisco.com

- **This could one or both of the following:**
  - **Notifications (Traps/Informs), with the possibility to add extra Object ID's to the notification.**
  - **SNMP Set**

© 2004 Cisco Systems, Inc. All rights reserved.

How to Enable EVENT-MIB?

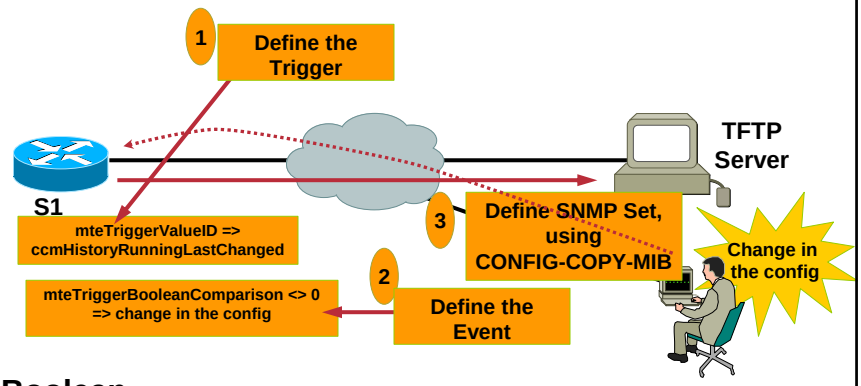
Cisco.com



Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB – Example 4
SNMP Set

Cisco.com



- **Boolean**

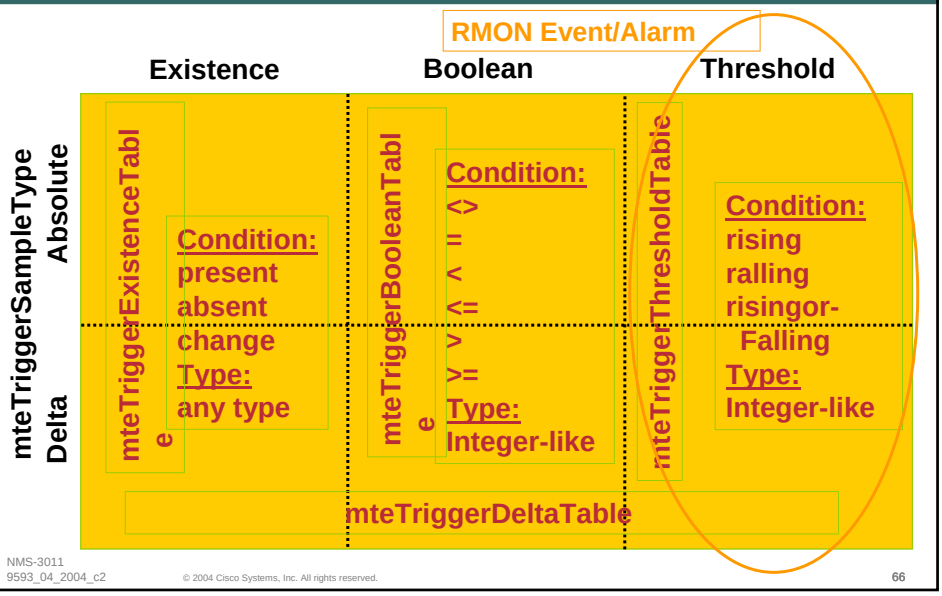
  test that can be done on the watched object: *Unequal*

- **SNMP Set**

© 2004 Cisco Systems, Inc. All rights reserved.

Event MIB vs. RMON Event&Alarm

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Event MIB vs. RMON Event&Alarm

Cisco.com

- If we want a trigger:
  - Threshold based,
  - On the local device (not remote),
  - Without wildcard,
  - With no extra objects in notification,
  - With no SNMP Set
- Then it is easier to use the RMON Event/Alarm

© 2004 Cisco Systems, Inc. All rights reserved.

EVENT-MIB Feature MIB Persistence

Cisco.com

- Allows the MIB to be persistent across reloads, i.e. MIB information retains the same set object values each time a networking device reboots

```
Router(config)# snmp mib persist [event]
```

- Write to NVRAM by using the “write mib-data“
- Any modified MIB data must be written to NVRAM memory using the “write mib-data”

```
Router# write mib-data
```

- Added in 12.2(4)T3

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB Show Command and Debug

Cisco.com

- Displays the SNMP Event values that have been configured on your routing device through the use of the Event MIB

```
Router# show management event
```

- Prints messages to the console whenever a the Event MIB evaluates a specified trigger

```
Router# debug management event mib
```


© 2004 Cisco Systems, Inc. All rights reserved.

Show Command Example

Cisco.com

```
 Router#show management event
Mgmt Triggers:
(1): Owner: john
(1): 01 , Comment: test, Sample: Del, Freq: 60
Test: Threshold
ObjectOwner: , Object:
OID: ifEntry.10, Enabled 1, Row Status 2
Threshold Entry:
Rising: 0, Falling: 0, DeltaRising: 0, DeltaFalling: 0
ObjOwn: , Obj:
RisEveOwn: , RisEve: , FallEveOwn: , FallEve:
DelRisEveOwn: , DelRisEve: , DelFallEveOwn: , DelFallEve:

Delta Value Table:

Mgmt Events:

Object Table:

Failures: Event = 0, Trigger = 0
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Show Command Example, Commented

Cisco.com

```
Router#show management event
Mgmt Triggers:
(1): Owner: john (mteOwner)
(1): 01 (mteTriggerName), Comment (mteTriggerComment):
"test", Sample (mteTriggerSampleType): Del (this means
delta), Freq (mteTriggerFrequency): 60
Test (mteTriggerTest): Threshold
ObjectOwner: , Object:
OID (mteTriggerValueID): ifEntry.10, Enabled
(mteTriggerEnabled) 1, Row Status (mteTriggerEntryStatus) 2
Threshold Entry:
Rising: 0, Falling: 0, DeltaRising: 0, DeltaFalling: 0
ObjOwn: , Obj:
RisEveOwn: , RisEve: , FallEveOwn: , FallEve:
DelRisEveOwn: , DelRisEve: , DelFallEveOwn: , DelFallEve:

Delta Value Table:

Mgmt Events:

Object Table:

Failures: Event = 0, Trigger = 0 0
```


© 2004 Cisco Systems, Inc. All rights reserved.

EXPRESSION-MIB

SOMETIMES THE DESIRED SNMP OBJECT DOESN'T EXIST BUT CAN BE DERIVED FROM MULTIPLE OTHER OBJECTS

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EXPRESSION-MIB

Cisco.com

- Allows you to create new SNMP objects based upon existing MIB variables and formulas
- Based on IETF draft, again in the DISMON Working Group, and numbered in Cisco's namespace
- Interesting when combined with the EVENT-MIB
- Note that RFC 2982 exists now
- Available in IOS since 12.0(5)T, added delta and wildcard support in 12.1(3)T

© 2004 Cisco Systems, Inc. All rights reserved.

EVENT-MIB & EXPRESSION-MIB Example 1: Notification

Cisco.com

- An access router would like to send a trap only for the high speed interface
- RouterA sends a Trap when Serial0 has:

  BW>100Kbits & OperStatus=DOWN

- Steps:

Expression-MIB

Create an expression that will return "1" when the condition is TRUE and "0" when FALSE

Exp1 = (ifSpeed > 100000) && (ifOperStatus == 2)

Event-MIB

If Exp1 == "1" generates an Event. This will be checked every minute

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB & EXPRESSION-MIB Example 1: Notification

e1exp in ASCII

```
snmpset -v 2c -c private RouterA expNameStatus.101.49.101.120.112
   integer 6
snmpset -v 2c -c private RouterA expNameStatus.101.49.101.120.112
   integer 5
snmpset -v 2c -c private RouterA expExpressionIndex .101.49.101.120.112
   gauge 1
snmpset -v 2c -c private RouterA expExpressionComment.1 octetstring "e1
   expression“
snmpset -v 2c -c private RouterA expExpression.1 octetstring '$1 <
   100000 && $2 == 2‘
snmpset -v 2c -c private RouterA expObjectID.1.1 objectidentifier
   ifSpeed.16
snmpset -v 2c -c private RouterA expObjectID.1.2 objectidentifier
   ifOperStatus.16
snmpset -v 2c -c private RouterA expObjectSampleType.1.1 integer 1
snmpset -v 2c -c private RouterA expObjectSampleType.1.2 integer 1
snmpset -v 2c -c private RouterA expObjectStatus.1.1 integer 1
snmpset -v 2c -c private RouterA expObjectStatus.1.2 integer 1
snmpset -v 2c -c private RouterA expNameStatus.101.49.101.120.112
   integer 1
```

.16=ifIndex Serial0

Absolute(1)

EVENT-MIB & EXPRESSION-MIB Example 1: Notification

#N caracters for the mteOwner

mteOwner = tom

#mteTriggername = trigger1

```
mteTriggerEntry Index=3.116.111.109.116.114.105.103.103.101.114.49 = Y
mteEventEntry Index= 3.116.111.109.101.116.101.110.116.49 = Z
snmpset -v 2c -c private RouterA mteTriggerEntryStatus.Y integer
snmpset -v 2c -c private RouterA mteTriggerEntryStatus.Y integer
snmpset -v 2c -c private RouterA mteTriggerValueID.Y objectidentifier
   1.3.6.1.4.1.9.10.22.1.4.1.1.2.1.0.0.0
snmpset -v 2c -c private RouterA mteTriggerValueIDWildcard.Y integer 2
snmpset -v 2c -c private RouterA mteTriggerTest.Y o "40“
snmpset -v 2c -c private RouterA mteTriggerFrequency.Y gauge 60
snmpset -v 2c -c private RouterA mteTriggerSampleType.Y integer 1
snmpset -v 2c -c private RouterA mteTriggerEnabled.Y integer 1
snmpset -v 2c -c private RouterA mteEventEntryStatus.Z integer 6
snmpset -v 2c -c private RouterA mteEventEntryStatus.Z integer 5
snmpset -v 2c -c private RouterA mteEventActions.Z o “80”
```

#mteEventname = event1

Existance(0)
Boolean(1)
Threshold(2)

Absolute (1)

When condition is met>send notification

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB & EXPRESSION-MIB Example 1: Notification

Cisco.com

```
snmpset -v 2c -c private RouterA mteTriggerBooleanValue.Y i 1
snmpset -v 2c -c private RouterA mteTriggerBooleanComparison.Y i 2
snmpset -v 2c -c private RouterA mteTriggerBooleanObjectsOwner.Y o “tom”
snmpset -v 2c -c private RouterA mteTriggerBooleanObjects.Y o “objects1”
snmpset -v 2c -c private RouterA mteTriggerBooleanEventOwner.Y o “tom”
snmpset -v 2c -c private RouterA mteTriggerBooleanEvent.Y o “event1”
Creating the ObjectTable
snmpset -v 2c -c private RouterA mteObjectEntryStatus.Z.1 i 6
snmpset -v 2c -c private RouterA mteObjectEntryStatus.Z.1 i 5
snmpset -v 2c -c private RouterA mteObjectsID.Z o ifAdmin.13
snmpset -v 2c -c private RouterA mteObjectEntryStatus.Z.1 i 1
Attaching the object to the event:
snmpset -v 2c -c private RouterA mteEventNotificationObjectsOwner.Z o “tom”
snmpset -v 2c -c private RouterA mteEventNotificationObjects.Z o “objects1”
Activating the Trigger and the Event
```

Unequal(1)
Equal(2)
less(3)…

© 2004 Cisco Systems, Inc. All rights reserved.

EVENT-MIB & EXPRESSION-MIB Example 2: Simple Capacity Planning

Cisco.com

- If my link utilization is above 50% for an hour, it’s time to upgrade the link
- Steps:

  Create an expression

  utilization = (ifInOctets + ifOutOctets) * 800 / hour / ifSpeed

Expression-MIB

If utilization above 50% of the bandwidth generates an Event. This will be checked every minute

Event-MIB

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

EVENT-MIB & EXPRESSION-MIB Example 3: Table Entry Count

Cisco.com

- Sometimes there is no counter for the number of table entries in the MIB definition
- Create an expression1 that will match all entries
- Create an expression2 that will sum expression1
- Other examples:
  - Number of ethernet interfaces up
  - Number of entries in the CAM table
  - Number of static route in the routing table

© 2004 Cisco Systems, Inc. All rights reserved.

EXPRESSION-MIB Show Command and Debug

Cisco.com

- Show commands

```
Router# show management expression
```

- Debug commands

```
Router# debug management expression ?
   evaluator   Expression MIB evaluator
   mib         Expression MIB SNMP operations
   parser      Expression MIB parsing
```

- CLI show commands
- CLI debug commands
- SNMP configuration (no CLI yet)

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Expression MIB Feature MIB Persistence

Cisco.com

- Allows the MIB to be persistent across reloads, i.e. MIB information retains the same set object values each time a networking device reboots

```
Router(config)# snmp mib persist [expresion]
```

- Any modified MIB data must be written to NVRAM memory using the “write mib-data”

```
Router# write mib-data
```

- Added in 12.2(4)T3

© 2004 Cisco Systems, Inc. All rights reserved.

EVENT-MIB & EXPRESSION-MIB

Cisco.com

- Feedback?

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

SPECIFIC SCENARIOS

MPLS/VPN SYSLOG & SNMP NOTIFICATION,
SAA & SNMP,
NBAR,
ETC…

© 2004 Cisco Systems, Inc. All rights reserved.

Disabling the Logging of Some Interfaces

Cisco.com

- **Limit the amount of output that is logged from the group-async interface and ISDN D channels.**
- **Occurs regularly on access interfaces. Dialer interfaces going up and down is normal behavior and does not indicate a problem.**

```
Router(config)# interface Group-Async 1
Router(config-if)# no logging event link-status
Router(config-if)# no snmp trap link-status

Router(config)# snmp ifmib trap throttle
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Monitoring Service
Service Assurance Agent

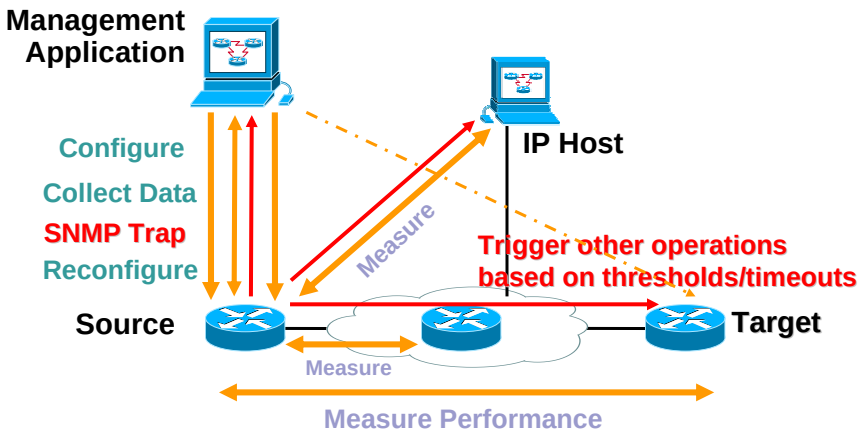
Cisco.com

- Active probing from the router
- THE feature to monitor services
- Wide measurement capabilities (UDP, TCP, ICMP, delay, jitter,…)
- Accessible using CLI and SNMP
- Proactive notification via SNMP traps

© 2004 Cisco Systems, Inc. All rights reserved.

Monitoring Service
Service Assurance Agent

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Monitoring Service VOIP Example

Cisco.com

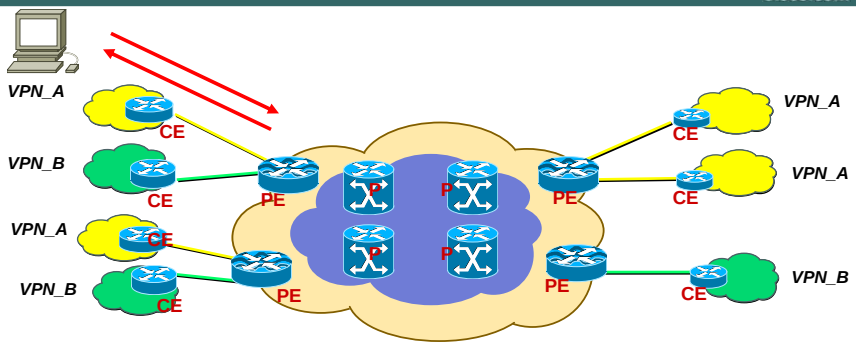
```
rtr 11 type jitter dest-ipaddr 198.198.198.1
  dest-port 3000 codec G711alaw
  tag jitter-with-voice-scores

rtr reaction-configuration 11 react connectionLoss
  threshold-type immediate action-type trapOnly
rtr reaction-configuration 11 react jitterAvg
  threshold-value 1 1 action-type trapOnly
  threshold-type immediate
rtr reaction-configuration 11 react MOS threshold-
  value 390 220 action-type trapOnly
  threshold-type immediate

rtr logging traps

rtr schedule 11 start-time now

snmp-server host 10.48.71.94 version 2c public
snmp-server enable traps syslog
```

Available in 12.3(7)T

© 2004 Cisco Systems, Inc. All rights reserved.

SNMP VRF Aware (VRF Aware Polling)

Cisco.com




```
Router(config)# snmp-server host <host-address>
   <community-string> [vrf vrf-name]
```

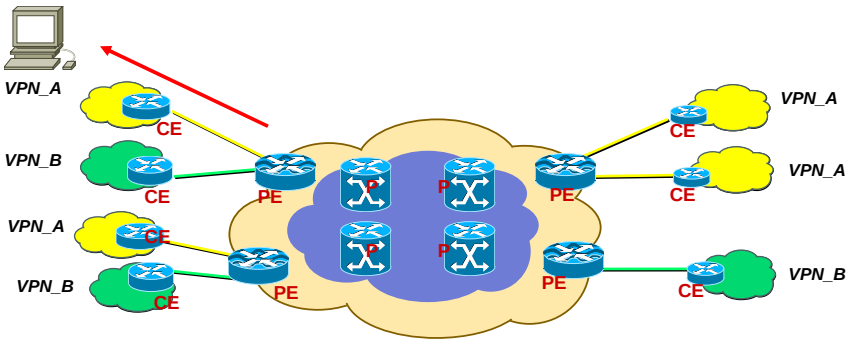
- **Allow a certain community name to come from a specific VRF only**
- **Note: not all MIBs are VRF aware**

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

VRF Aware Notifications

Cisco.com



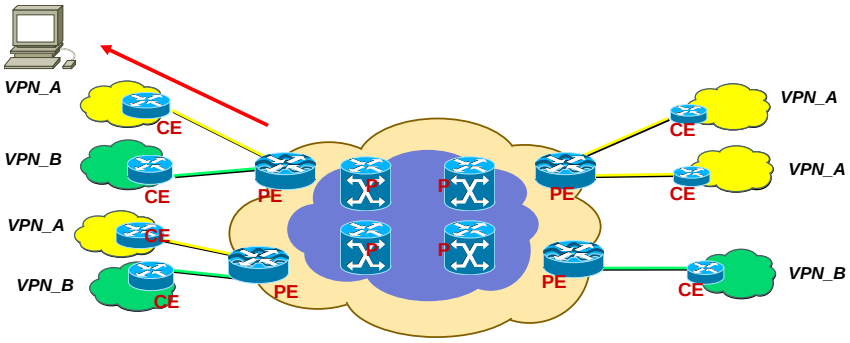
- Notifications sent to a receiver in a VRF

```
Router(config)#snmp-server host
      <receiver-ip-addr> vrf yellow public
```


© 2004 Cisco Systems, Inc. All rights reserved.

VRF Aware Syslog (Under Development)

Cisco.com



- Syslog messages sent to a server in a VRF

```
Router(config)#logging host vrf <yellow>
      <syslog-ip-address>
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

NBAR-MIB

Cisco.com

- Network Based Application Recognition
- Accounting (bytes, packets, rate) per protocol discovered by protocol-discovery
  - "show ip nbar protocol-discovery“
- Real Time thresholding with traps:
  - redefined the event/alarm trap from RMON
  - Awareness of what NBAR does to the CPU

© 2004 Cisco Systems, Inc. All rights reserved.

EMBEDDED EVENT MANAGER

THE NEWEST IN CISCO IOS

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Event Manager (EEM) 1.0 Overview

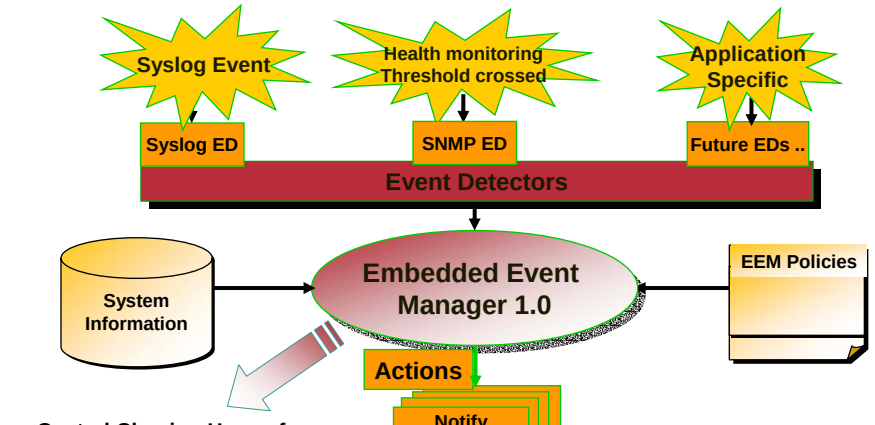
Cisco.com

- In-box monitoring of different components of the system via a set of software agents (event detectors)
- Event detectors (ED) notify EEM when an event of interest occurs
- Advantages:
  - Local programmable actions, triggered by specific events
- Introduced in 12.0(26)S, 12.3(4)T

© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Event Manager (EEM) The Framework

Cisco.com



- Central Clearing House for events detected in a Cisco IOS Device
- Distributes Event Information to Interested Applications

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Event Manager (EEM) Overview

Cisco.com

- Event Detectors
  - EEM 1.0 SNMP & Syslog Event Detectors
  - EEM 2.0 will deliver: other Event Detectors, ability to invoke TCL scripts
- Current Actions
  - Log a prioritized message to Syslog
  - Send an event to CNS Bus for upstream processing by a Cisco CNS device
  - Reload the entire system (*)
  - Switch-over to Standby Route Processor in a 'dual RP' configuration (*)

(*) EEM 1.0 originally developed to support IOS High Availability, even if applicable to more general situation

© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Event Manager (EEM) 1.0 Example 1

Cisco.com

- Applets are groupings of an 'event specification' and a policy action that is taken when the specified event occurs

```
event manager applet fe0trans
  event syslog pattern .*UPDOWN.*FastEthernet0/0.*
  action 1.0 syslog priority emergency msg "New
   syslog $_syslog_msg"
  action 2.0 cns-event CNS event data
```

- Example: causes an emergency level syslog message and a CNS event to be sent when a log message indicates that the FastEthernet0/0 port changed state to either up or down

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Event Manager (EEM) 1.0 Example 2

Cisco.com

ciscoMemoryPoolFree

```
event manager applet memory-demo
 event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-
  type exact entry-op lt entry-val 5120000 poll-
  interval 10
 action 1.0 syslog priority critical msg "Memory exh
  austed; current available memory is $_snmp_oid_val
   bytes"
 action 2.0 force-switchover
```

- Example: The applet will run when the available memory on the primary RP falls below the specified threshold of 5120000 bytes

© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Event Manager (EEM) 1.0 Environment Variables

Cisco.com

- These environment variables can be used in ‘msg’ text
- Will be replaced with the relevant text

- Environment Variable Available for All Events
  - $_event_type The event type that triggered the event
  - $_event_pub_time The time at which the event type was published
- Environment Variable Available for SNMP Events
  - $_snmp_oid The SNMP object OID that caused the event to be published
  - $_snmp_oid_val The SNMP object ID value when the event was published
- Environment Variable Available for Syslog Events
  - $_syslog_msg The syslog message that caused the event to be published

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Event Manager (EEM) 1.0 Advantages

Cisco.com

- SNMP monitoring AND syslog as event detectors
- More flexible threshold than RMON Event/Alarm
  - Greater than, greater or equal, ...
  - Like the EVENT-MIB
- Can customize the notification
  - Some environment variales
  - Redefined syslog priority level
- Control is in the customer's hands: full customization
- Better hysteresis mechanism control thanks to the exit options

© 2004 Cisco Systems, Inc. All rights reserved.

EMBEDDED SYSLOG MANAGER

THE NEWEST IN CISCO IOS

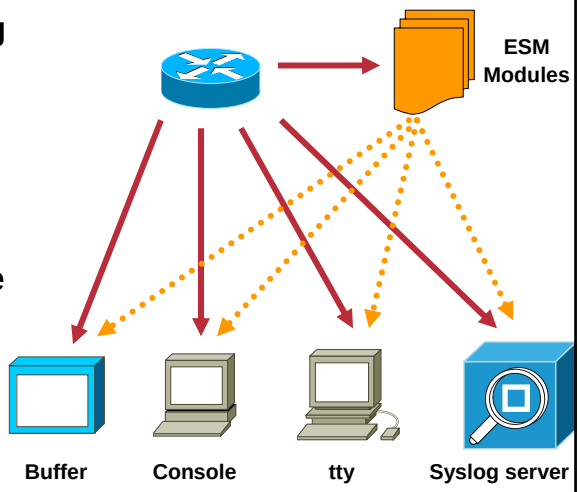
© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Syslog Manager (ESM)

Cisco.com

- Post-process Syslog messages with selected ESM filters (Proactive Rules-based analysis)
- User definable scripting (TCL)
- New message queue in ***Parallel*** with classic Syslog
- Available in images with TCL 8.3.4, in 12.3(2)T



© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Syslog Manager (ESM) Configuration Example

Cisco.com

```
Router(config)# logging filter <URL> [<position>]
                [args <argstring>]
```

"URL", the location of the TCL script (Cisco IOS, flash, web, tftp server)

"Position", ordering of filters when multiple exist

"Args", arguments to the Tcl scrip

```
Router(config)# logging console filtered
Router(config)# logging host <x.x.x.x> filtered [stream_id]
```

The stream_ID is added by the script, for event routing

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Syslog Manager (ESM) Example 1

Cisco.com

- **Severity Escalation: Messages that Cisco deemed low priority may be very important to some customers**
- **Example: escalate syslog messages that contain the word 'CONFIG_I' to severity level of 4 (they are by default level 5)**

```
Router(config)# logging filter slot0:/escalate.tcl CONFIG_I 4
```


© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Syslog Manager (ESM) Example 1

Cisco.com

```
#  Embedded Syslog Manager, Severity Escalation Module
#  ===================================================================
# Usage: Set CLI Args to "mnemonic new_severity"
# Namespace: global
# Check for null message

if { [string length $::orig_msg] == 0} {
   return ""
}

if { [info exists ::cli_args] } {
    set args [split $::cli_args]
    if { [ string compare -nocase [lindex $args 0] $::mnemonic ] == 0 } {
        set ::severity [lindex $args 1]
        set sev_index [ string first [lindex $args 0] $::orig_msg ]
        if {  $sev_index >= 2 } {
           incr sev_index -2
           return [string replace $::orig_msg $sev_index $sev_index \
              [lindex $args 1]]
        }
    }
}
return $::orig_msg
```


© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Embedded Syslog Manager (ESM) Example 2

Cisco.com

- **Message Correlation – To help reduce the volume of messages when certain well-known network events occur, ESM can correlate local events, and summarize them.**
- **Example: link-flapping messages can be counted over a period of time, and a single syslog message sent**

```
00:22:11: %LINK-3-UPDOWN: serial1 flapping
(4 changes to up/4 changes to down between 00:21:09 and 00:22:11)
```


© 2004 Cisco Systems, Inc. All rights reserved.

Embedded Syslog Manager (ESM) Other Examples

Cisco.com

- **Message Routing: customers may wish to categorize messages using criteria other than facility or severity**

  Example: Send all Spanning tree messages to a separate syslog server

- **SMTP-based email alerts: capability for notifications using TCP to external servers, such as TCP-based syslog collectors or Simple Mail Transfer Protocol (SMTP) servers**

  Example: "configuration changes" sent to administrators via an email message

- **Your example ... The possibilities are never-ending!**

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

SUMMARY

© 2004 Cisco Systems, Inc. All rights reserved.

Principles of Fault Management in Cisco Devices

Cisco.com

- Quick fault detections is strategic to Network Management
- Systematic network element polling doesn't always scale
- Let's tune the right fault management events from the network elements themselves
- We investigated a few ways
- Then potentially event-based polling …

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Other Network Management Sessions

Cisco.com

- NMS-1N01 - Introduction to Network Management – Networkers On-Line
- NMS-1N02 - Introduction to SNMP and MIBs – Networkers On-Line
- NMS-1N03 - Accurate Time Synchronization – Networkers On-Line
- NMS-1N04 - Introduction to Service Assurance Agent – Networkers On-Line
- NMS-1N41 - Introduction to Performance Management – Networkers On-Line
- NMS-1011 - Principles of Fault Management
- NMS-1101 - Understanding DNS and DHCP
- NMS-2001 - Network Troubleshooting Tools and Techniques
- NMS-2021 - Large Scale Deployments of CiscoWorks
- NMS-2031 - Traffic Accounting Scenarios
- NMS-2032 - NetFlow for Accounting, Analysis and Attack
- NMS-2042 - Performance Measurement with Cisco Devices
- NMS-2051 - Securely Managing Your Network
- NMS-2102 - Deploying and Troubleshooting NAT
- NMS-2101 - DNS Deployment and Operation
- NMS-4012 - MPLS Embedded Management Tools
- NMS-4043 - Advanced Service Assurance Agent
- NMS-2T00 - Network Management Best Practices - Techtorial

© 2004 Cisco Systems, Inc. All rights reserved.

Complete Your Online Session Evaluation!

Cisco.com

WHAT: Complete an online session evaluation and your name will be entered into a daily drawing

WHY: Win fabulous prizes! Give us your feedback!

WHERE: Go to the Internet stations located throughout the Convention Center

HOW: Winners will be posted on the onsite Networkers Website; four winners per day

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Q and A

© 2004 Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS

© 2003, Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Appendix

© 2003, Cisco Systems, Inc. All rights reserved.

Fault Management
Which MIB variables to monitor?

Interface

	Object Descr	OID	Poll Int	Threshold
locIfResets	number of times the interface internally reset	.1.3.6.1.4.1.9.2.2.1.1.17	15 min	
ifOperStatus	The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed	.1.3.6.1.2.1.2.2.1.8	5 min	!= 1
locIfCarTrans	Number of times interface saw the carrier signal transition	.1.3.6.1.4.1.9.2.2.1.1.21	15 min	
locIfCollisions	number of output collisions detected on this interface	1.3.6.1.4.1.9.2.2.1.1.25	15 min	
locIfInCRC	number of input packets which had cyclic redun-dancy checksum errors	.1.3.6.1.4.1.9.2.2.1.1.12	15 min	

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Fault Management
Which MIB variables to monitor?

Cisco.com

Interface	Object Descr	OID	Poll Int	Threshold
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters	.1.3.6.1.2.1.2.2.1.16	30 min	
locIfInputQueueDrops	The number of packets dropped because the input queue was full	.1.3.6.1.4.1.9.2.2.1.1.26	30 min	> 1% of incoming traffic
locIfOutputQueueDrops	The number of packets dropped because the output queue was full	.1.3.6.1.4.1.9.2.2.1.1.27	30 min	> 10% of outgoing traffic
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space	.1.3.6.1.2.1.2.2.1.13	30 min	

© 2004 Cisco Systems, Inc. All rights reserved.

Fault Management
Which MIB variables to monitor?

Cisco.com

Ethernet	Object Descr	OID	Poll Int	Threshold
dot3StatsCarrier SenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame	.1.3.6.1.2.1.10.7.2.1.11	15 min	>= 2
dot3StatsDeferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.	.1.3.6.1.2.1.10.7.2.1.7	15 min	
dot3StatsExcessive Collisions	Count of frames for which transmission failed because of excessive collisions	.1.3.6.1.2.1.10.7.2.1.9	15 min	0.2% of traffic
dot3StatsInternalMac ReceiveErrors	Count of frames for which reception fails because of an internal MAC sublayer receive error.	.1.3.6.1.2.1.10.7.2.1.16	15 min	1% of incoming traffic
dot3StatsInternalMac TransmitErrors	Count of frames for which transmission fails because of an internal MAC sublayer transmit error.	.1.3.6.1.2.1.10.7.2.1.10	15 min	1% of outgoing traffic

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Fault Management
Which MIB variables to monitor?

Cisco.com

Memory	Object Descr	OID	Poll Int	Threshold
bufferFail	number of buffer allocation failures	.1.3.6.1.4.1.9.2.1.46	15 min	
bufferNoMem	number of buffer create failures due to no free memory	.1.3.6.1.4.1.9.2.1.47	15 min	>= 1
ciscoMemoryPool Free	number of bytes from the memory pool that are currently unused on the managed device	1.3.6.1.4.1.9.9.48.1.1.1.6	30 min	
ciscoMemoryPool LargestFree	largest number of contiguous bytes from the memory pool currently unused	.1.3.6.1.4.1.9.9.48.1.1.1.7	30 min	
ciscoMemoryPool Used	number of bytes from the memory pool that are currently in use	.1.3.6.1.4.1.9.9.48.1.1.1.5	30 min	
ciscoMemoryPool Free	number of bytes from the memory pool that are currently unused on the managed device	.1.3.6.1.4.1.9.9.48.1.1.1.6	15 min	

© 2004 Cisco Systems, Inc. All rights reserved.

Fault Management
Which MIB variables to monitor?

Cisco.com

Environment	Object Descr	OID	Poll Int	Threshold
ciscoEnvMonFan State	The current state of the fan being instrumented.	.1.3.6.1.4.1.9.9.13.1.4.1.3	15 min	>= 1
ciscoEnvMonSupply State	The current state of the power supply being instrumented.	.1.3.6.1.4.1.9.9.13.1.5.1.3	15 min	>= 1
ciscoEnvMon TemperatureState	The current state of the testpoint being instrumented.	.1.3.6.1.4.1.9.9.13.1.3.1.6	15 min	!= 1
ciscoEnvMon VoltageState	The current state of the testpoint being instrumented.	.1.3.6.1.4.1.9.9.13.1.2.1.7	15 min	!= 1

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr

Fault Management
Which MIB variables to monitor?

Cisco.com

Miscellaneous

	Object Descr	OID	Poll Int	Threshold
cpmCPUTotal5min	Overall CPU busy percentage in the last 5 min period This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	.1.3.6.1.4.1.9.9.109.1.1.1.1.5	5 min	
sysUpTime	system uptime in 1/100ths of seconds	.1.3.6.1.2.1.1.3	5 min	< 30000

© 2004 Cisco Systems, Inc. All rights reserved.

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
9593_04_2004_c2.scr