GETTING THE RIGHT EVENTS FROM NETWORK ELEMENTS

NMS-A01

Benoit Claise

Housekeeping

- **Please switch off your mobile phones!**
- **Don’t forget to complete your evaluations - you can access them on-line via Schedule Builder!**
- **Visit the World of Solutions on Level -01!**
- **Your session printouts have been prepared by**

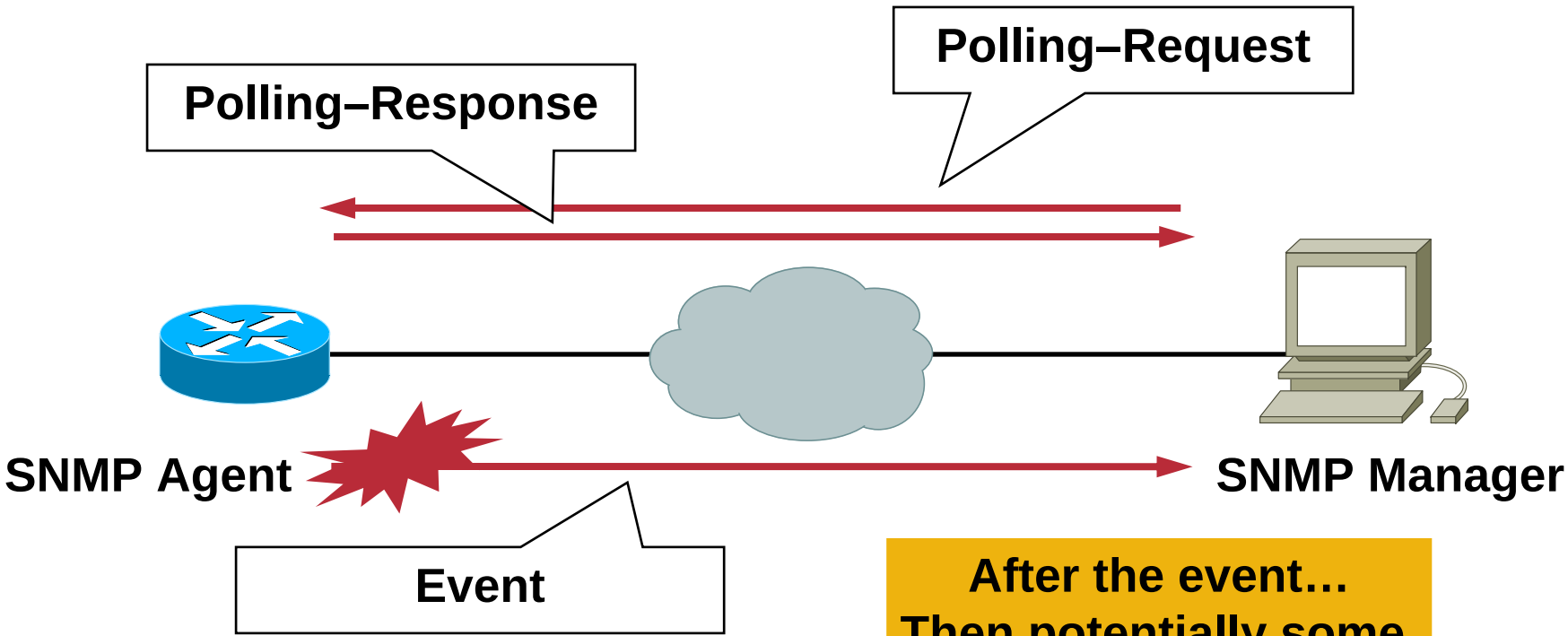
Print Center on Level -01

- **Please remember this is a ‘No Smoking’ venue!**
- **Please remember to wear your badge at all times including the Party!**

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**
  - **Features, tricks, information, examples, etc. on “How to generate the right events from your network elements!”**

Polling vs. Event Notification



**After the event…
Then potentially some event-based polling**

- **Message:**

  Let the network elements monitor themselves

  Let's tune the right fault management events from the network elements

Polling vs. Event Notification

	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

Agenda

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

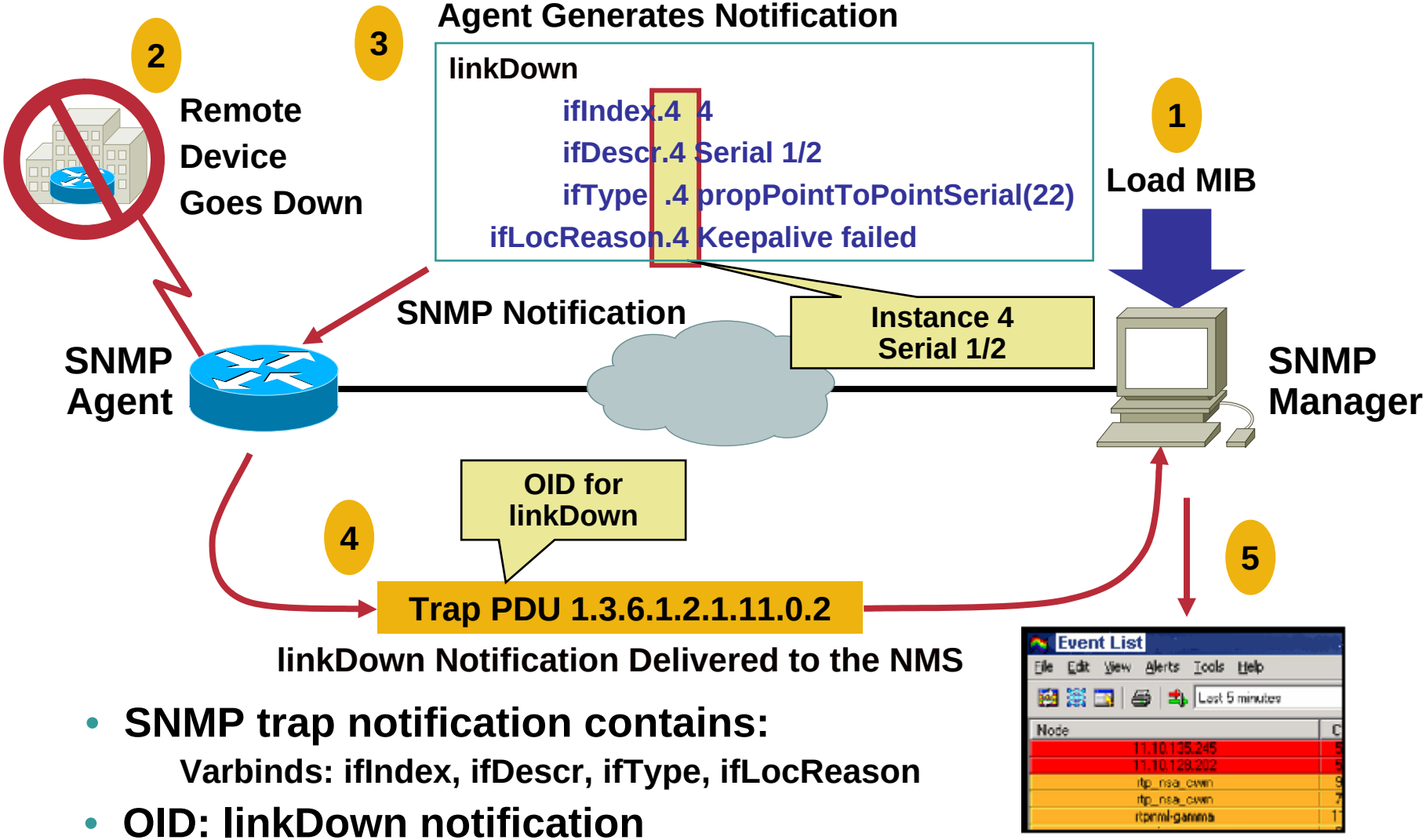
SNMP NOTIFICATION

EVERYBODY KNOWS ABOUT TRAPS!

SNMP Notifications

- **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**

SNMP Trap Notification



- **SNMP trap notification contains:**
  - **Varbinds: ifIndex, ifDescr, ifType, ifLocReason**
- **OID: linkDown notification**

How to Enable SNMP Traps Notification?

- **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:**

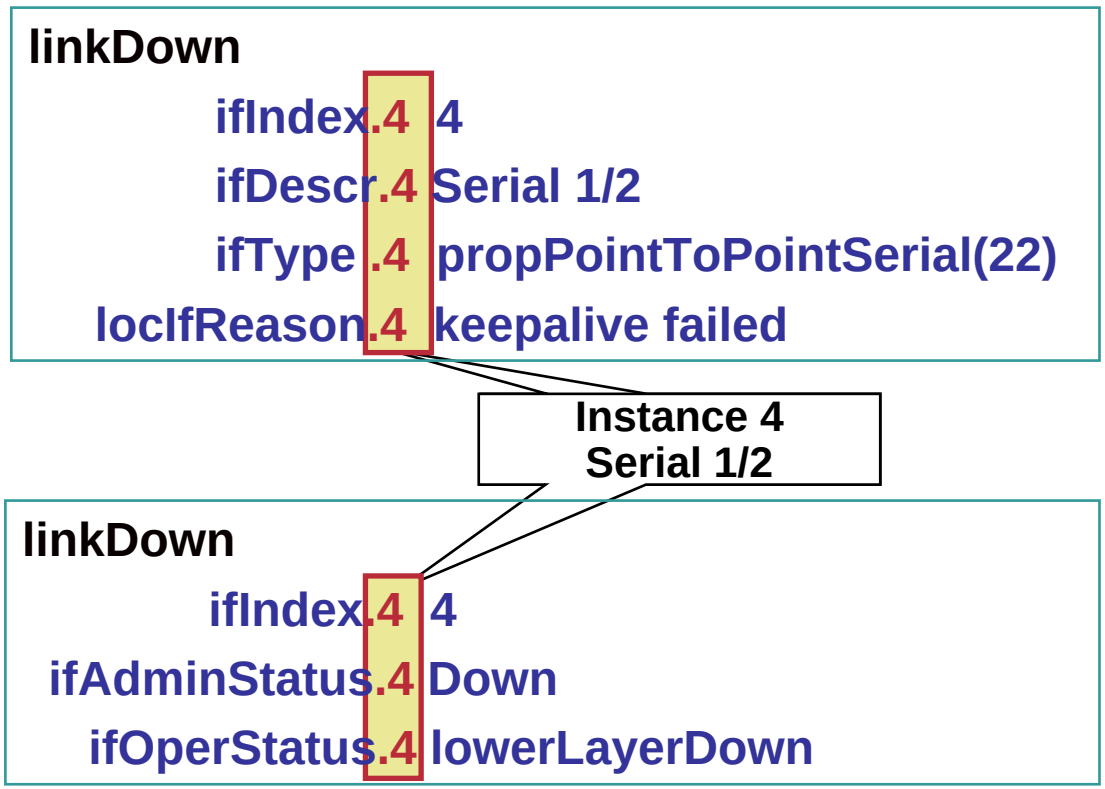
```
Switch>(enable) set snmp trap enable <trap_type>
Switch>(enable) set snmp trap <NMS_host>
```

Traps-Show Commands


```
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>

linkUp/linkDown Notification



Cisco Redefinition

CISCO-GENERAL-TRAPS

IETF Notification

IF-MIB (RFC2233/RFC2863)

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

How to Enable SNMP Inform Notification?

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

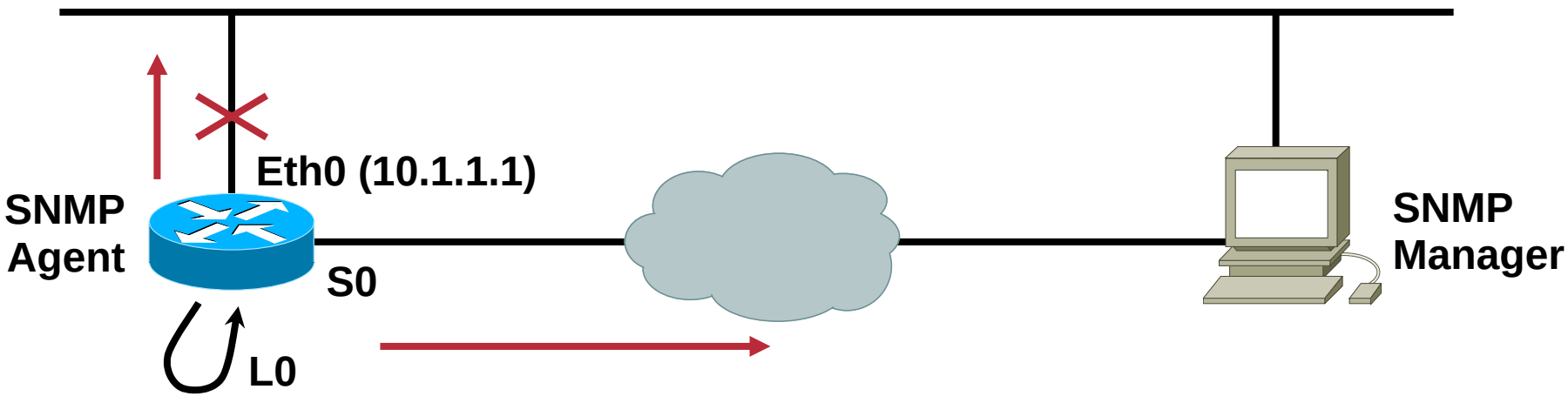
- **"snmp-server enable informs…" no functionality!**
- **Switches:**

  So far, needed the SNMPv3 architecture
  8.3(1): simplified v2c inform CLI

Informs: Show Commands


```
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
```

SNMP Source Trap Notification




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

Or even better

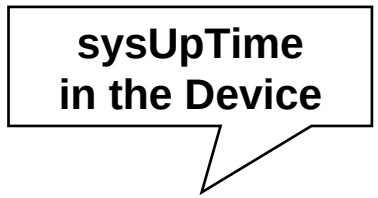
```
Router(config)# snmp-server trap-source loopback 0
```

SNMP Traps vs. Informs

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

Notification Deduplications Notion of Time

SNMPv2-Notification-PDU



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

- The notifications have no notion of UTC time
  - NTP is of NO USE between network elements and notification receiver for SNMP notifications
  - Big drawback of SNMP notifications
- No solution for network-wide alarm deduplications or analysis
  - Only track: the fault management applications look at the time the notifications are received
- Similar problem with SNMPv1: trap also sends the sysUpTime

How to Find Out About Notifications?

Cisco.com

```
Router(config)# snmp-server enable traps ?
   atm              Enable SNMP atm traps
  bgp       Enable BGP state change traps
  config    Enable SNMP config traps
   …
```

- **TAC Web document**

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

- **What device supports which MIB?**

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

NOTIFICATION-LOG-MIB

- 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
```

NOTIFICATION-LOG-MIB

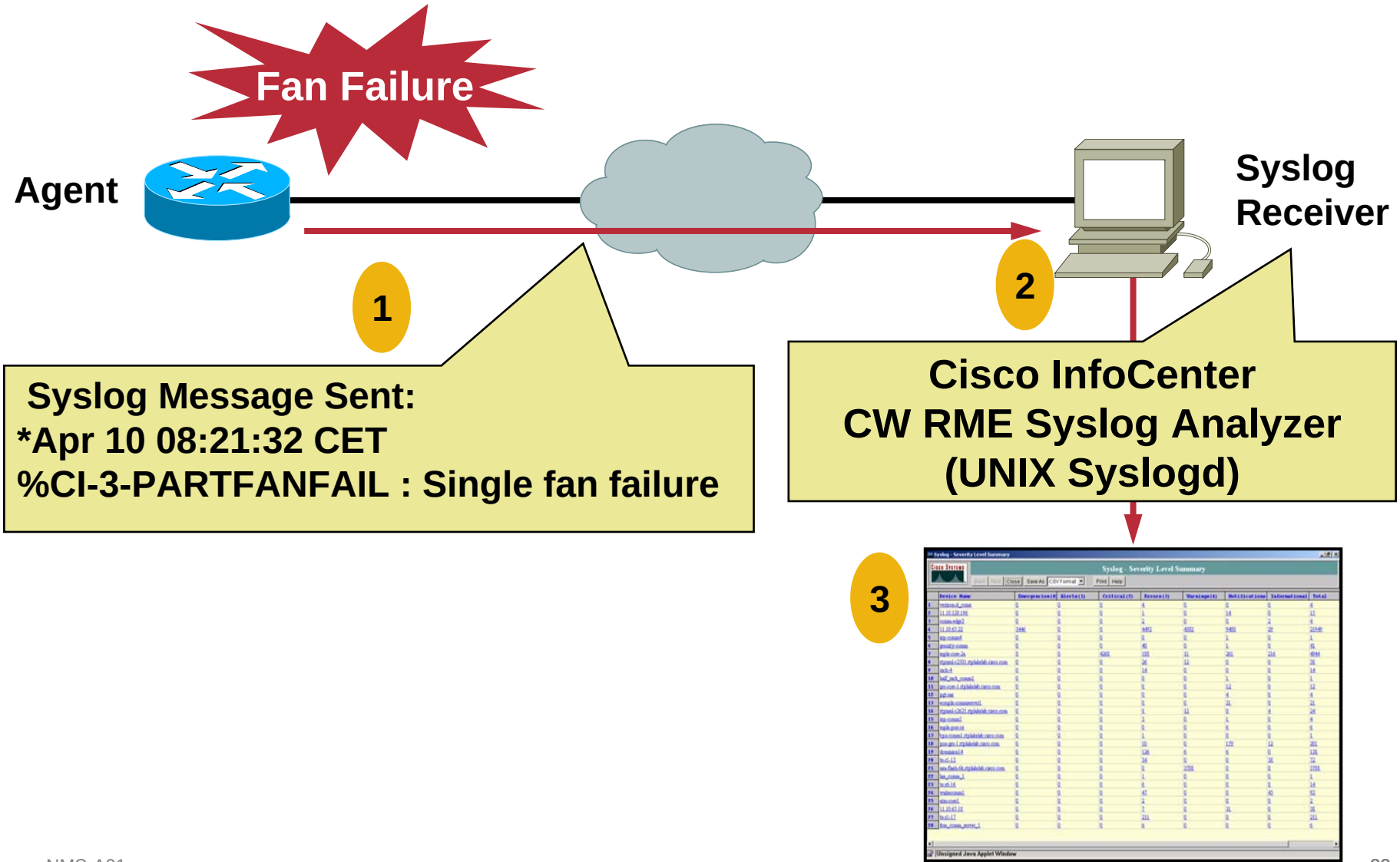

```
Router#show snmp mib notification-log all

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

SYSLOG MESSAGES

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

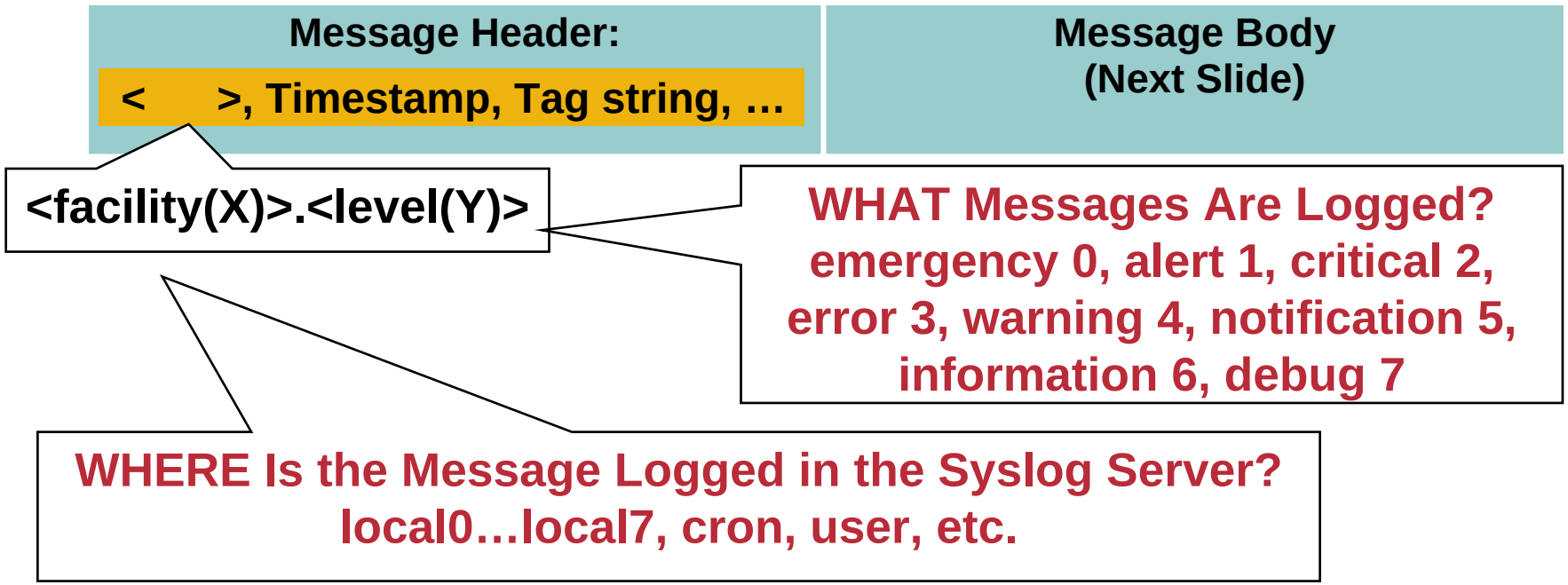
Syslog Message



Syslog Message

- 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
- Text messages sent to a Syslog daemon, on UDP port 514
- Very basic “standard”, informational RFC 3164
- RFC 3195: reliable delivery for Syslog
- Complementary to other events (SNMP notifications)

Syslog Message Format



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

  Message Header: local7.emergency

How to Enable Syslog Message on Cisco IOS?

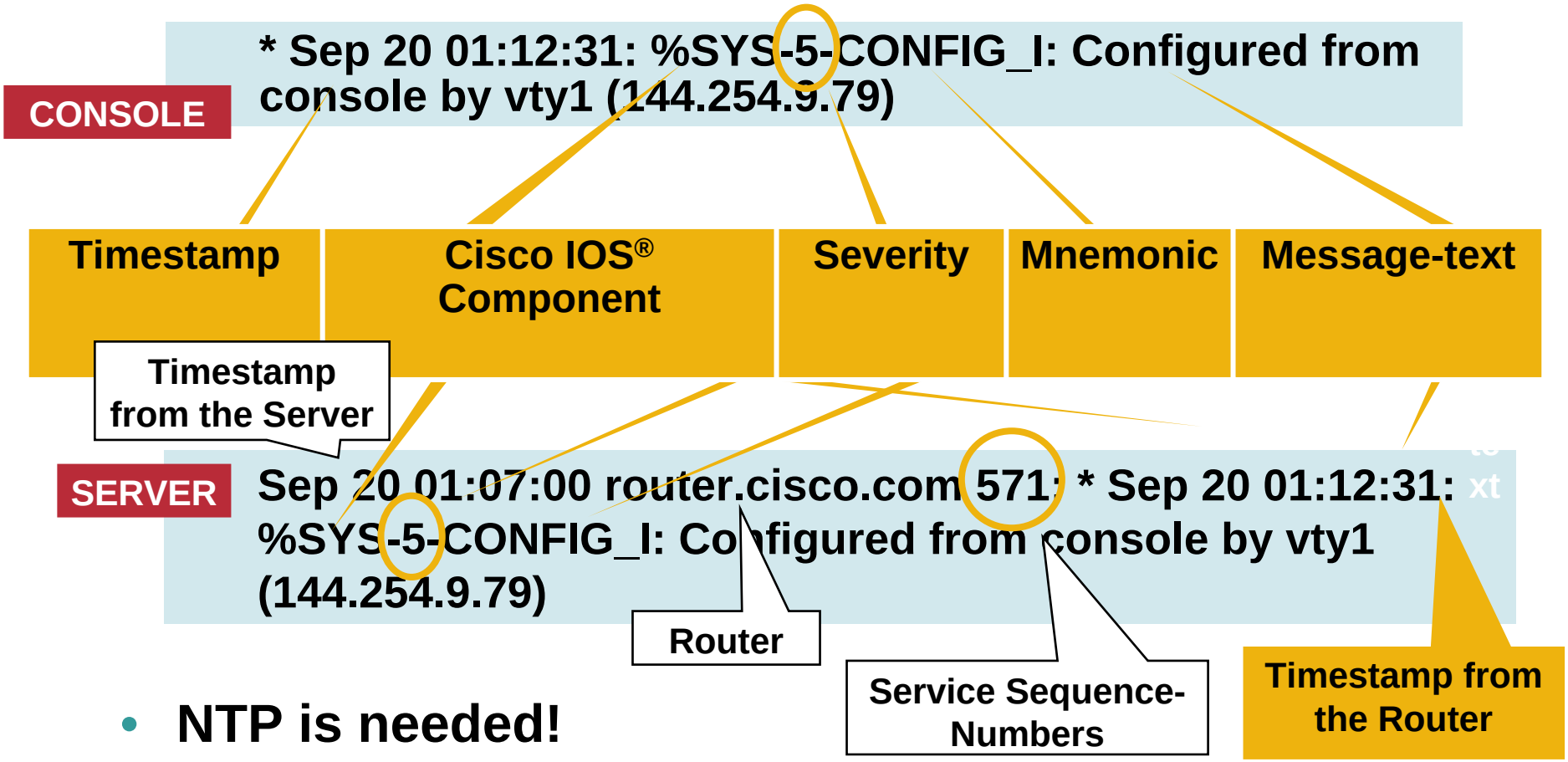
- **On a Cisco router:**

```
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

Syslog Message "Body" Format in the Cisco IOS



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

Syslog: Show Commands on Cisco IOS (Cont.)


```
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
```

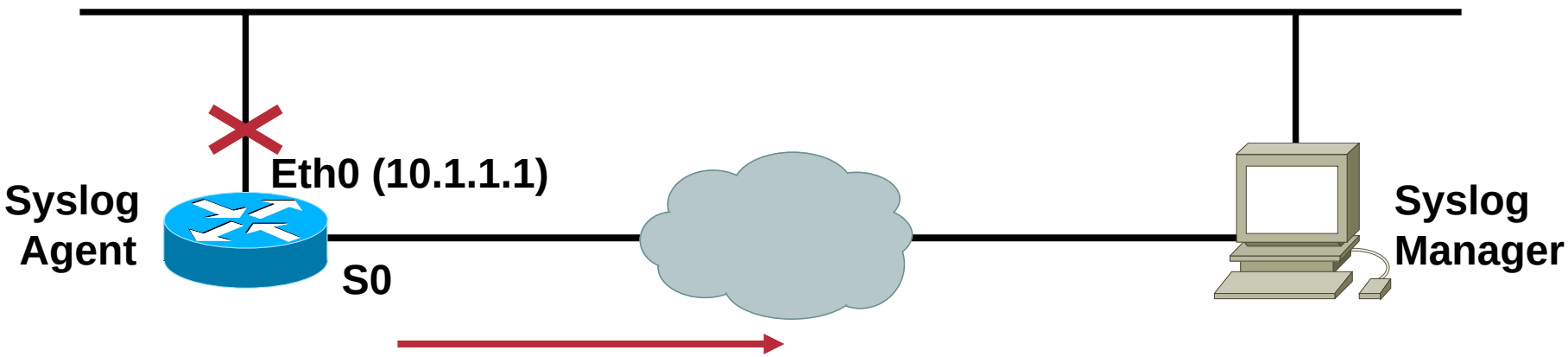
How to Enable Syslog Message on Catalyst OS?

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)

Syslog Source Interface




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

Syslog Message Filtering: Example 1

- 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
```

Syslog Message Filtering: Example 2

- 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
```

Convert a Syslog Message to a SNMP Notification?

- **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
```

- **How to convert to an inform?**

Attention to the <all> Keyword !!!

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

Syslog Writing to Flash

- 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
      disk1/:syslog size 134217728 filesize 16384


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

Syslog Issue
Consistent Message Format

- **Syslog isn’t consistently used across different Cisco platforms and Cisco IOS versions**

  Example: environmental monitor initiated shutdown event

  Cisco IOS 11.2 → ENVM-1-SHUTDOWN

  Cisco IOS 12.0 → ENVM-0-SHUT

How to Find Out About Syslog Messages?

Cisco.com

- **‘Cisco IOS Software System Error Messages’ per Cisco IOS release**

  For Cisco 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

XML Interface to Syslog Messages

- 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
```

XML Interface to Syslog Messages
Events Comparison


```
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>
```

Syslog Messages vs. SNMP Notifications

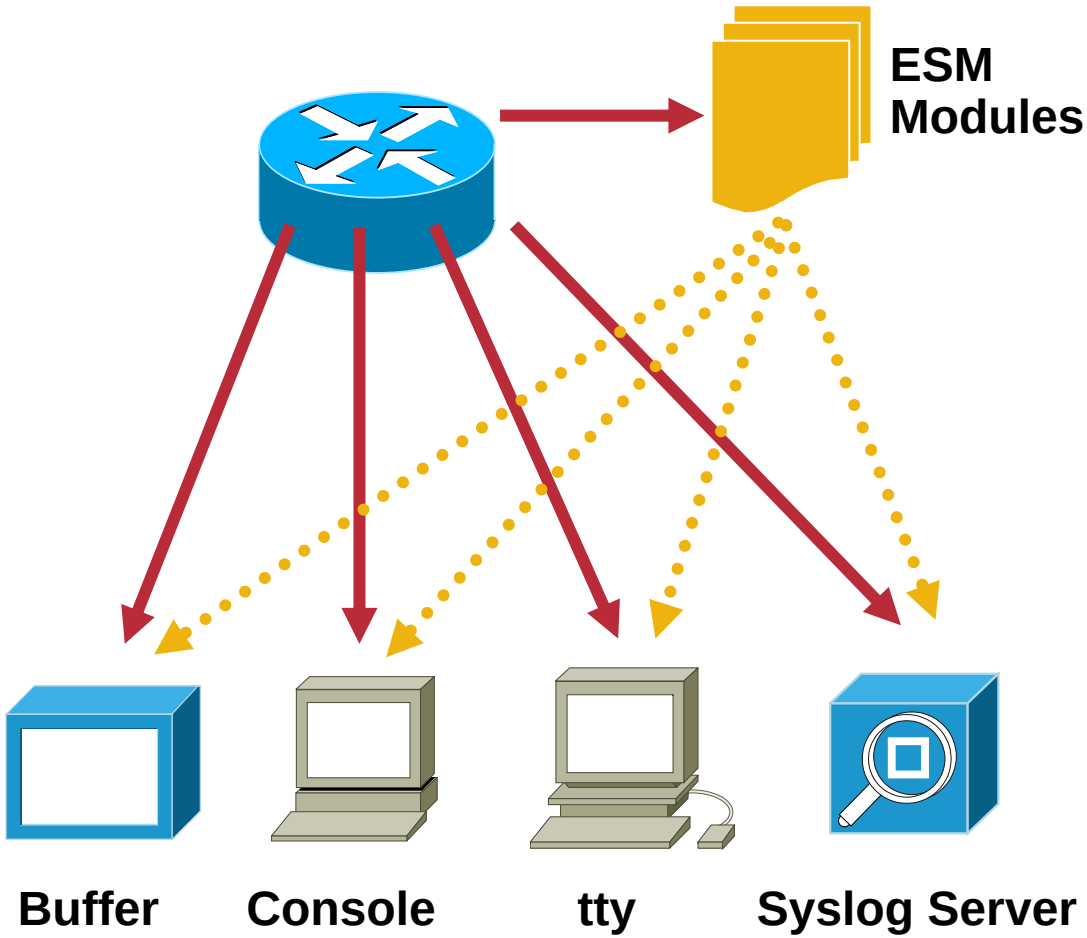
	Syslog	Notification
NMS	Syslog Daemon	Trap Receiver
Protocol/ Port	UDP 514	UDP 162
Filtering	Yes	Limited
Format	Easy-to-Read Format, No MIB Needed	More Rigid Format, Parse Able
Reliability	None (RFC 3195 Reliable Syslog) (Syslog Writing to Flash)	None with Traps Some with Informs (NOTIFICATION-LOG MIB)

Note: the Syslog message could be sent faster!

EMBEDDED SYSLOG MANAGER

SOME MORE FLEXIBILITY FOR THE SYSLOG MESSAGES

Embedded Syslog Manager (ESM)



- 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, 12.2(25)S

Embedded Syslog Manager (ESM)
Configuration Example


```
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 script

```
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

Embedded Syslog Manager (ESM)
Example 1

- **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 args CONFIG_I 4
```

Embedded Syslog Manager (ESM)
Example 1


```
#  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
```

Embedded Syslog Manager (ESM)
Example 2

- **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)
```

Embedded Syslog Manager (ESM)
Other Examples

- **Message routing:** categorize messages using criteria other than facility or severity

  Example: send all spanning tree messages to a separate syslog server (setting a specific stream ID in the TCL script)

- **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

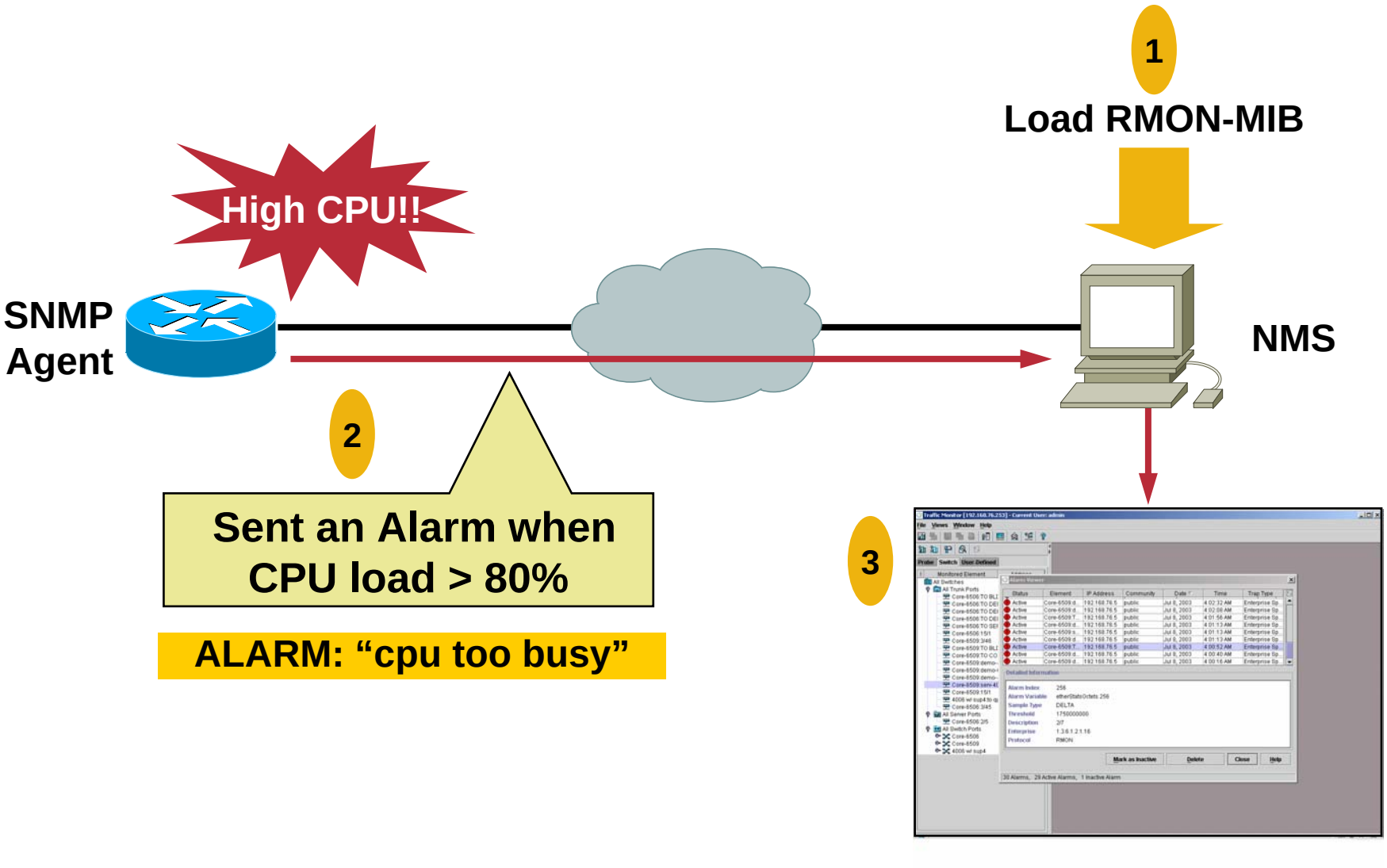
  Example: “configuration changes” sent to administrators via an email message

- **Your example…the possibilities are endless!**

RMON EVENT AND ALARM

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

RMON Event and Alarm

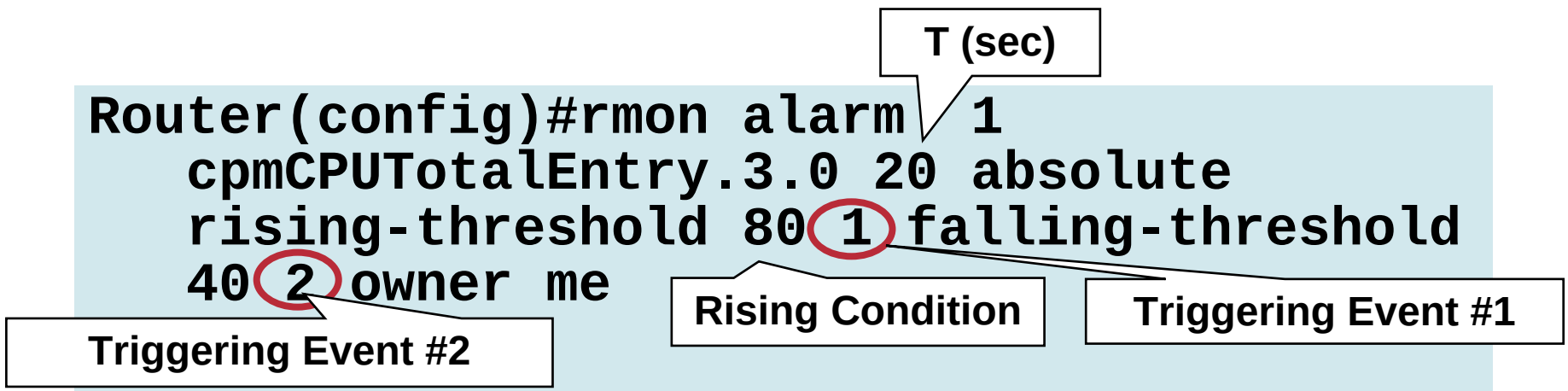


RMON Event and Alarm

- **Allows proactive monitoring:**
  - **The device polls itself**
- **RMON-MIB used to configure SNMP notification:**
  - **Traps and informs** NEW
  - **Integer32, Counter32, Counter64, Gauge, or Timeticks may be sampled**
- **Included in all Cisco IOS software images**
  - **Since Cisco IOS 11.1**
  - **CLI or SNMP configuration**
- **Included in all the switches images**
  - **Only SNMP configuration**

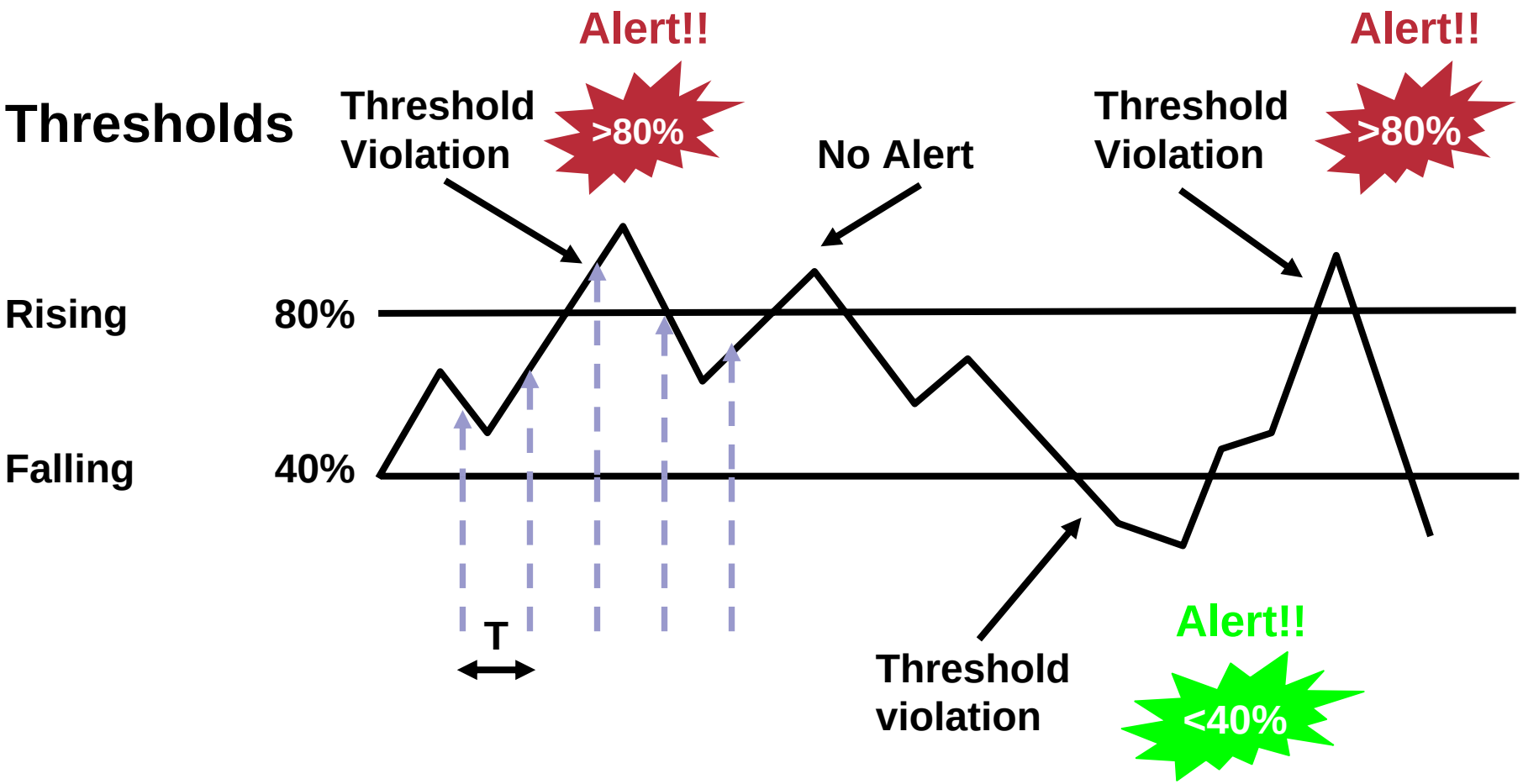
How to Enable RMON Event and Alarm via CLI?

- 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




```
Router(config)#rmon event 1 log Trap
   public description "cpu busy" owner me

Router(config)#rmon event 2 log
   description "cpu not too busy"
```

RMON Reaction Condition



T: Internal Sampled Interval (20 sec)

How to Enable RMON Event and Alarm via SNMP?

Send a trap when the number of bytes going into interface with ifIndex 12, during the last two 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> alarmSampleType.321 integer 1
snmpset -c private <router> alarmRisingThreshold.321 integer 140000000
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
```

Which MIB Variables to Monitor?

dot3StatsCarrierSenseErrors

bufferFail

ciscoEnvMonTemperatureState

cpmCPUTotal5min

ifOutDiscards

ciscoEnvMonFanState

bufferNoMem

locIfResets

locIfCollisions

locIfCollisions

ifOperStatus

ciscoMemoryPoolFree

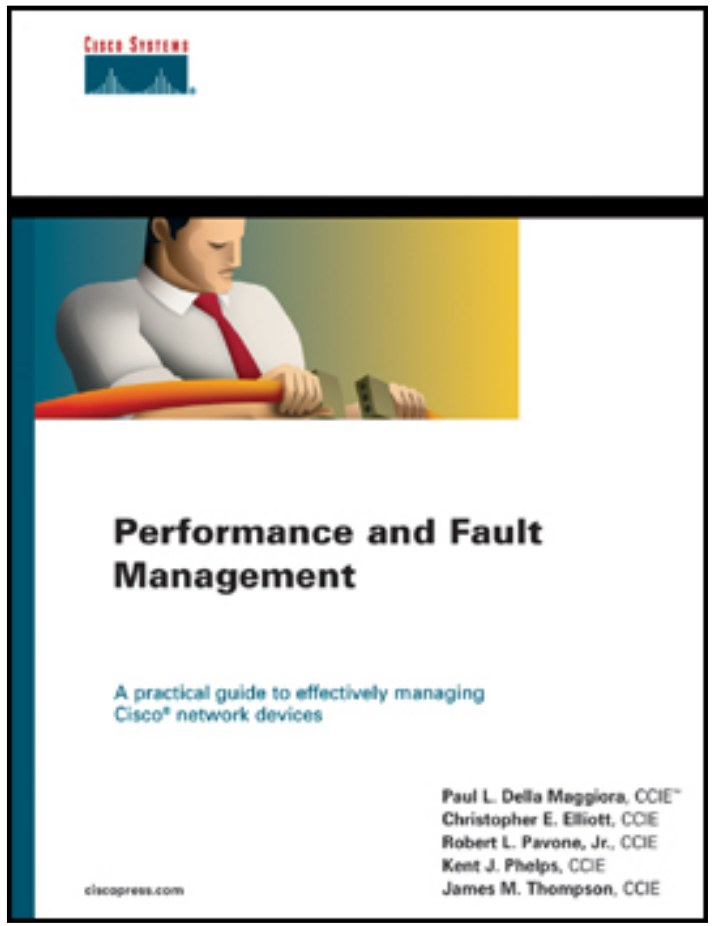
locIfInputQueueDrops

locIfCarTrans

locIfInCRC

bufferFail

locIfOutputQueueDrops



See the APPENDIX

Fault Management
Which MIB Variables to Monitor?

Interface

	Object Descr	OID	Poll Int	Thres-hold
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	

ifIndex and RMON Persistence

- **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

EVENT-MIB

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

Event-MIB

- 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: <>, =, <, <=, >, >=
- Event MIB proposed by Cisco to IETF DISMON Working Group, accepted standard track RFC-2981

Event-MIB Advantages vs. RMON Event and Alarm

- **EVENT MIB can monitor**
  - **Any MIB object (existence)**
  - **Any integer/counter (Boolean, threshold)**
- **RMON MIB can only monitor**
  - **Integer/counter (threshold)**
- **EVENT-MIB allows wildcarding**
- **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**

Cisco IOS Support

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

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800c391a.html

- **Only configuration support via SNMP so far: no CLI**

  Scriptable Interface for adding command line support in 12.3(7)T

  However “show management event” exists

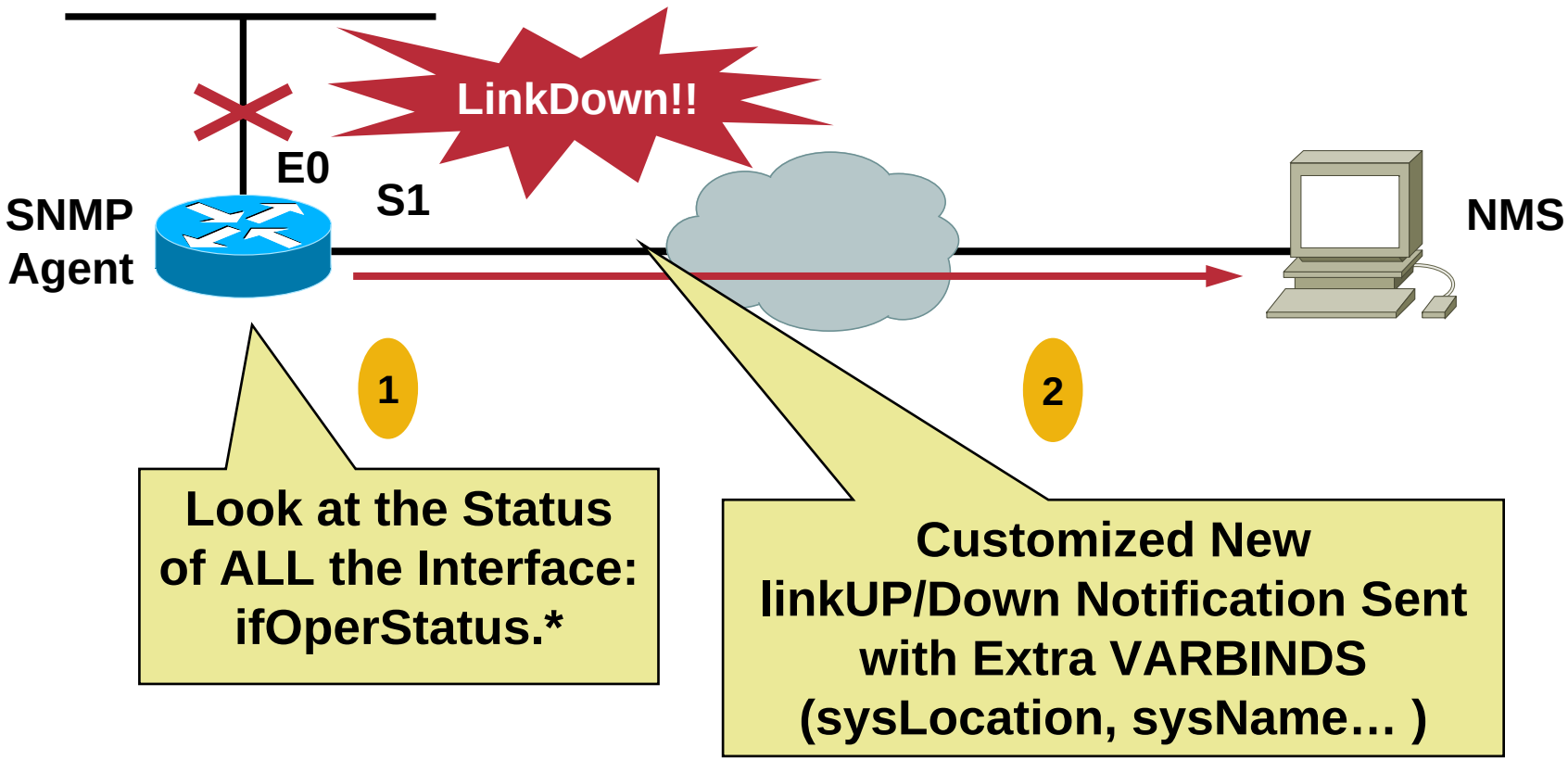
  However “debug management event mib” exists

EVENT-MIB: Example 1
Wildcarding

- **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:**

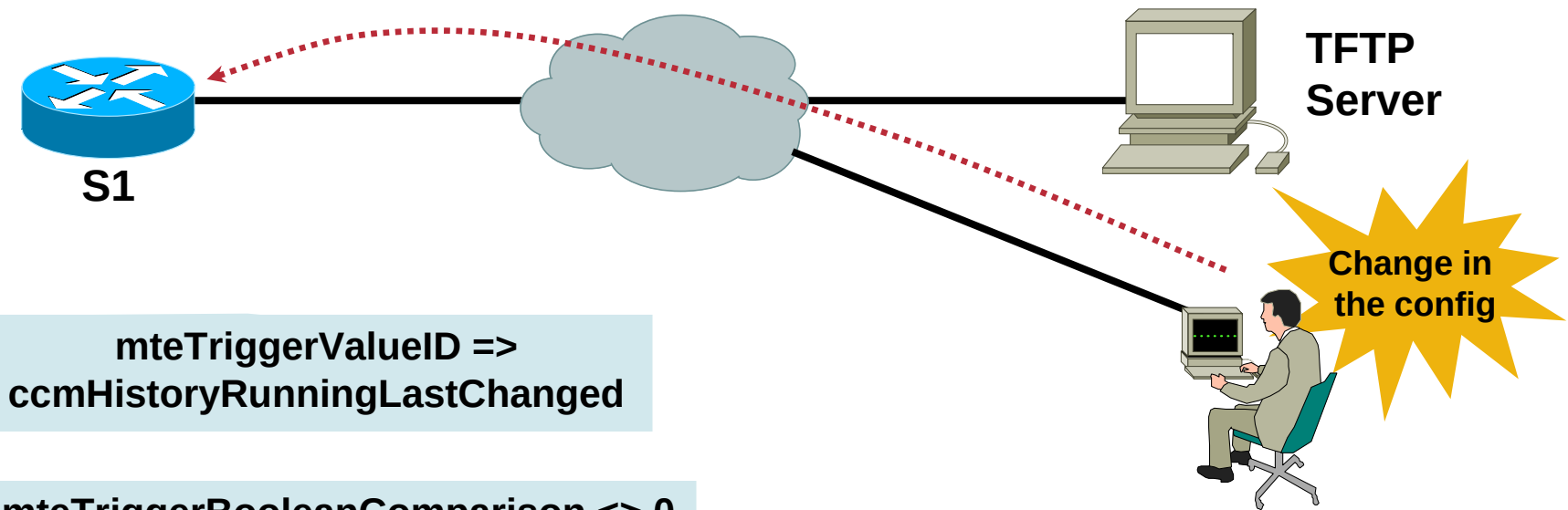
  Monitor ifInOctets for all interfaces; the EVENT-MIB is configured to monitor the delta values of ifInOctets for all interfaces once per minute; if any of the samples exceed the delta rising or falling triggers, a trap notification will be sent

EVENT-MIB: Example 2
Add Variable to Notification



EVENT-MIB: Example 3
SNMP Set

1. The Trigger **2. The Event** **3. The SNMPSet**



mteTriggerValueID =>
ccmHistoryRunningLastChanged

mteTriggerBooleanComparison <> 0
=> change in the config

SNMP Set, using CONFIG-COPY-MIB
to copy the config to TFTP server

How to Enable the EVENT-MIB?

Step 1: Any MIB Object Type

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

How to Enable the EVENT-MIB?

Step 2: Possibility: Sampling Type

- 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

How to Enable the EVENT-MIB?

Step 3: Test Type and Parameters

- **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

How to Enable the EVENT-MIB?

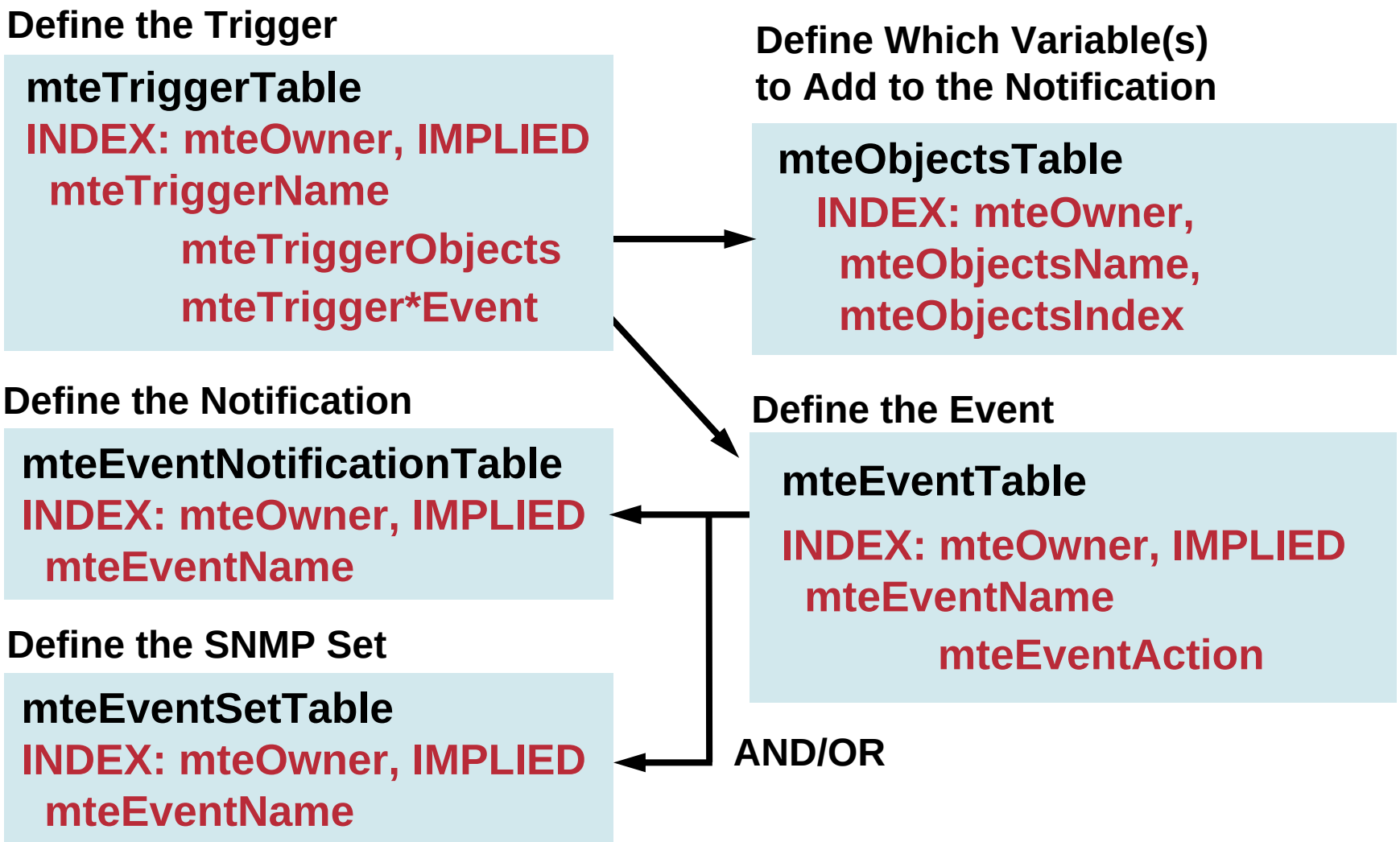
Step 4: Actions

- **This could be one or both of the following:**

  Notifications (Traps/Informs), with the possibility to add extra Object IDs to the notification

  SNMP set

How to Enable EVENT-MIB?



EVENT-MIB Feature
MIB Persistence

- 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

Event MIB Summary

- **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**
- **Else the EVENT-MIB is your friend ☺**

EXPRESSION-MIB

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

EXPRESSION-MIB

- Allows you to create new SNMP objects based upon existing MIB variables and formulas
- Interesting when combined with the EVENT-MIB
- EXPRESSION MIB proposed by Cisco to IETF DISMON Working Group, accepted standard track RFC-2982
  - Cisco implementation based on IETF draft, again in the DISMON Working Group, and numbered in Cisco's namespace
- Only configuration support via SNMP so far: no CLI
  - Scriptable interface for adding command line support in 12.3(7)T
  - However "show management expression" exists
  - However "debug management expression mib" exists

EVENT-MIB and EXPRESSION-MIB
Example 1: Notification

- An access router would like to send a trap only for the high-speed interface
- Router A 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

EVENT-MIB and EXPRESSION-MIB
Example 1: Notification


```
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
```

e1exp in ASCII

.16=ifIndex Serial0

Absolute(1)

EVENT-MIB and EXPRESSION-MIB
Example 1: Notification

#N Characters for the mteOwner

mteOwner = tom

#mteTriggername = trigger1

```
mteTriggerEntry Index=3.116.111.109.116.114.105.103.103.101.114.49 = Y
mteEventEntry Index= 3.116.111.109.101.118.101.110.116.49 = Z
snmpset -v 2c -c private RouterA mteTriggerEntryStatus.Y integer 6
snmpset -v 2c -c private RouterA mteTriggerEntryStatus.Y integer 5
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

EVENT-MIB and EXPRESSION-MIB
Example 1: Notification


```
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)…

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

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

Create an expression

Expression-MIB

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

If utilization is above 50% of the bandwidth after one hour, generates an event

Event-MIB

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

- 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

ARP Table Entry Count
Show Command Example


```
Router# show management expression
  Expression: e1exp is active
   Expression to be evaluated is $1==3 where:
   $1 = ipNetToMediaEntry.4
   Object Condition is not set
   Sample Type is absolute
   ObjectID is wildcarded

   Expression: e2exp is active
   Expression to be evaluated is sum($1) where:
   $1 = ciscoExperiment.22.1.4.1.1.4.1.0.0
   Object Condition is not set
   Sample Type is absolute
   ObjectID is wildcarded
```

- This example specifies an expression e2exp that sums up all the static ARP entries

Expression MIB Feature
MIB Persistence

- 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 [expression]
```

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

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

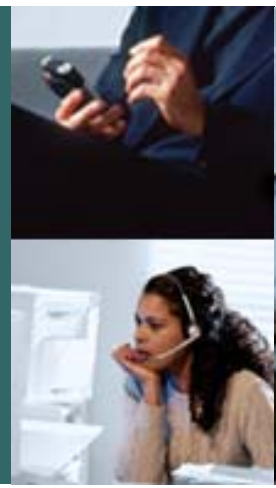
- Added in 12.2(4)T3

EVENT-MIB and EXPRESSION-MIB
Summary

- Very flexible and useful MIBs
- Not that easy to set up
- You should work from existing examples

  Drop me an email

SPECIFIC MIBS AND SCENARIOS



SPECIFIC INTERFACES,
MPLS/VPN SYSLOG & SNMP NOTIFICATION,
IP SLA & SNMP,
ENHANCED OBJECT TRACKING

Disabling the Logging of Some Interfaces

- **Limit the amount of output that is logged from the group-async interface and ISDN D channels**

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

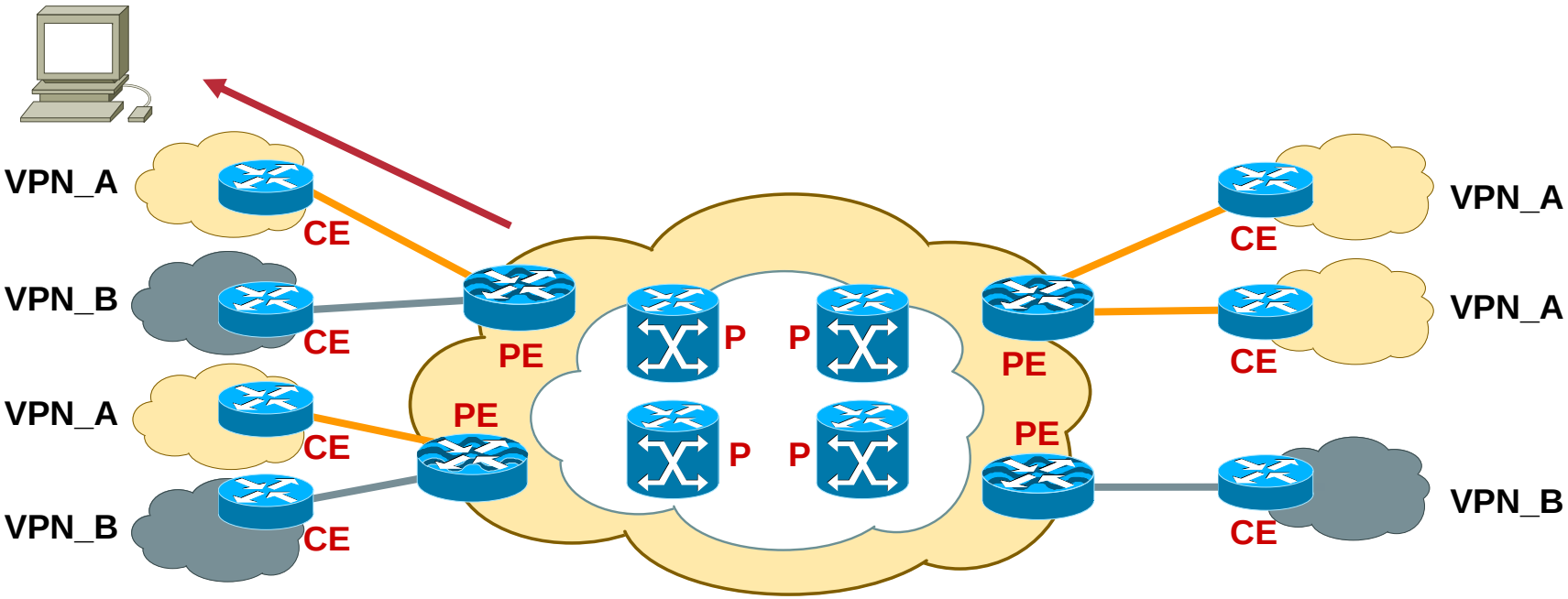
- **Depending on the layering…**

```
Router(config)# snmp ifmib trap throttle
Router(config-if)#no logging event subif-link-status
```

- **Depending on the encapsulation…**

```
Router(config-if)#no logging event dlci-status-change
```

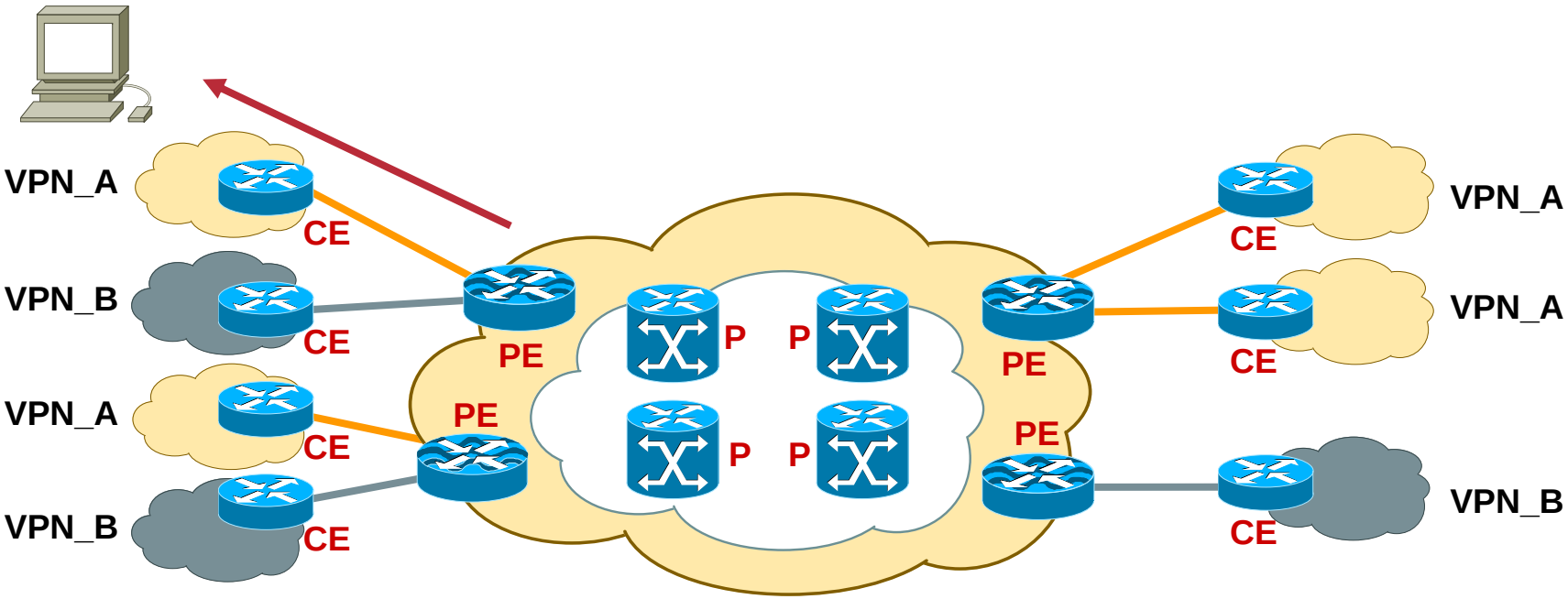
VRF Aware Notifications



Notifications sent to a receiver in a VRF

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

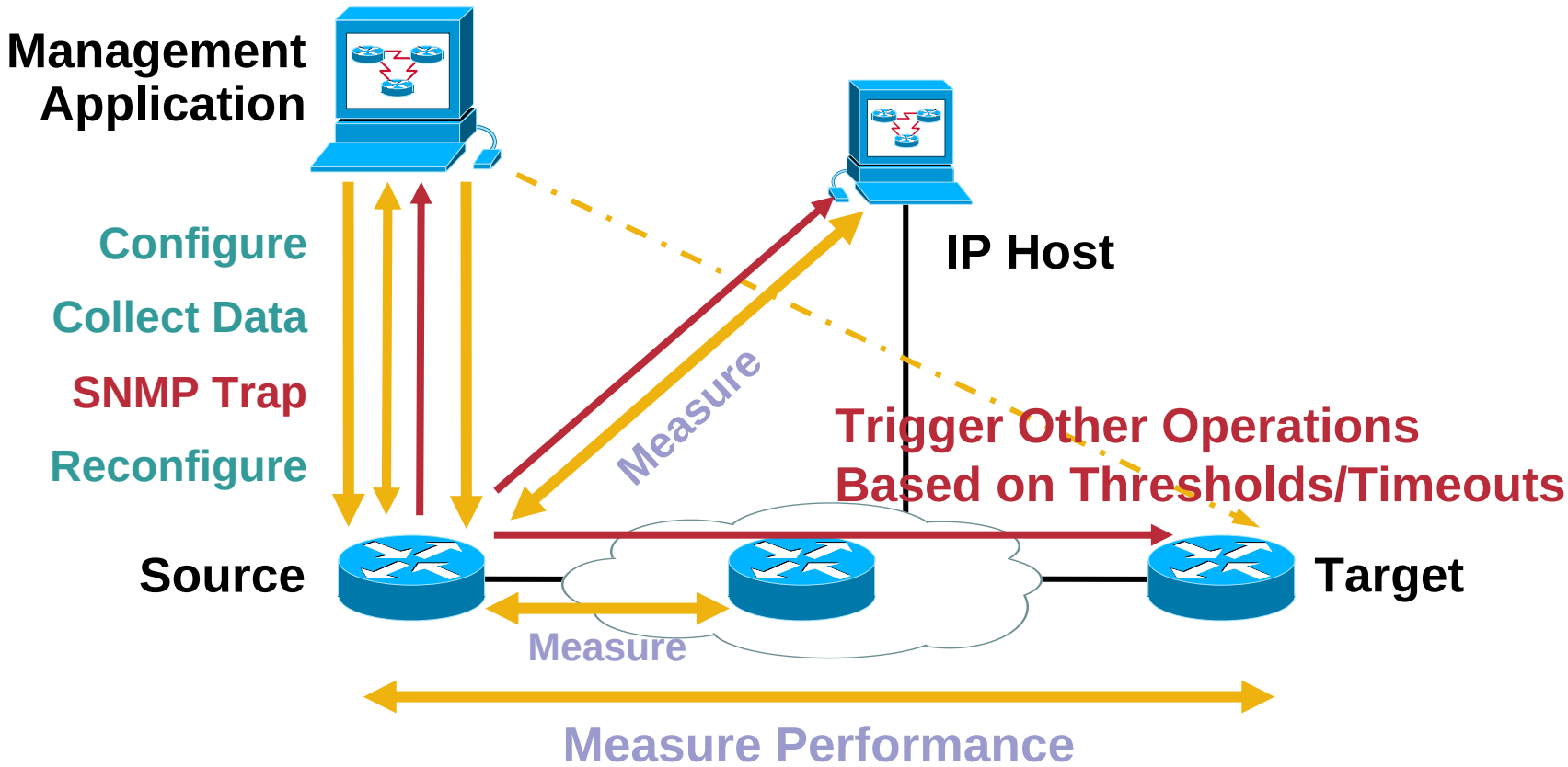
VRF Aware Syslog



- Syslog messages sent to a server in a VRF
- New in 12.2(24)S

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

Monitoring Service
IP SLA



IP SLA, Previously Service Assurance Agent

Monitoring Service with IP SLA
VoIP Example

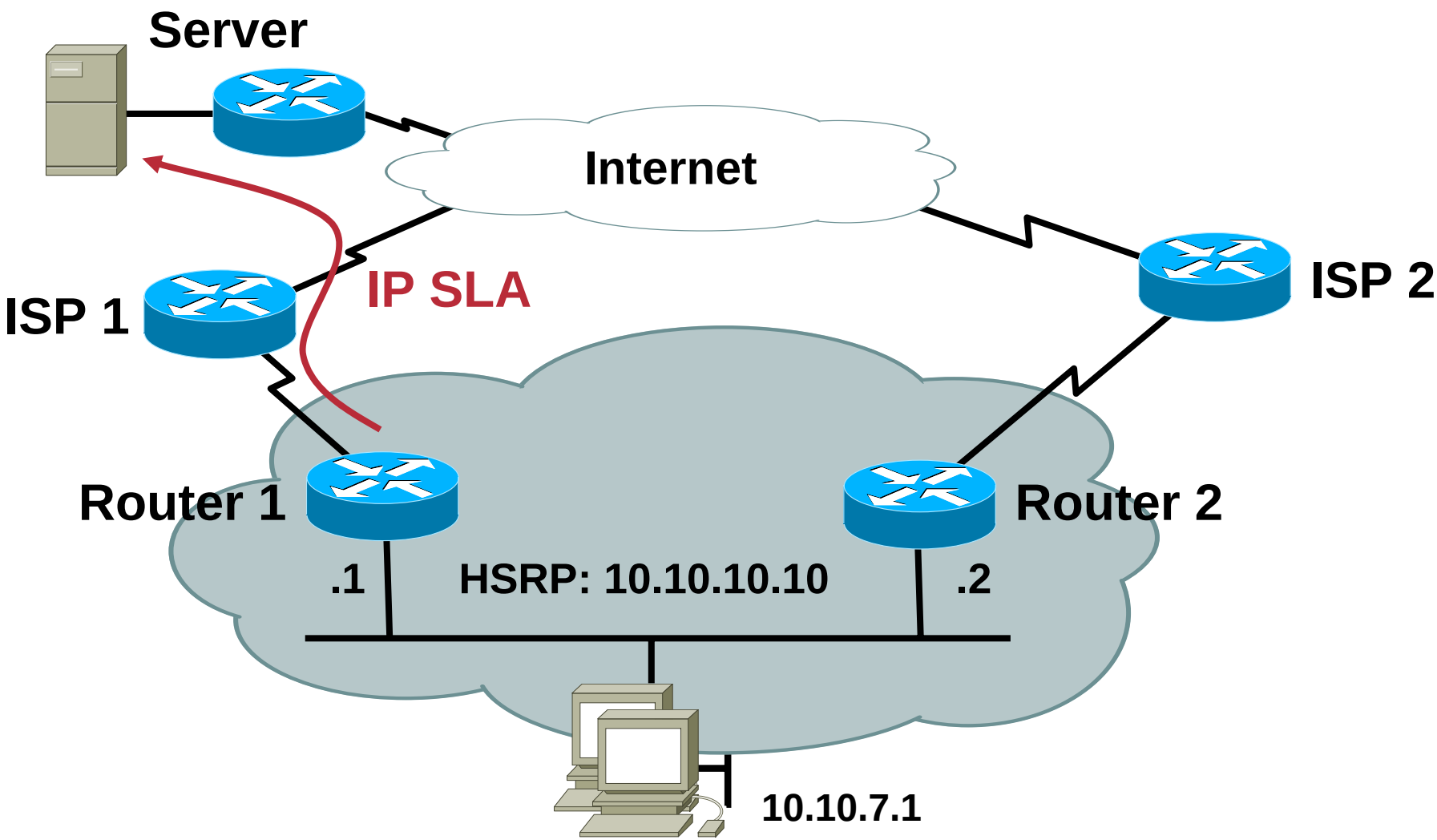

```
ip sla 11
   udp-jitter 198.198.198.1 3000 codec g711alaw

ip sla reaction-configuration 11 react connectionLoss
threshold-type immediate action-type trapOnly
ip sla reaction-configuration 11 react jitterDSAvg
threshold-value 10 5 threshold-type immediate action-
type trapOnly
ip sla reaction-configuration 11 react jitterSDAvg
threshold-value 10 5 threshold-type immediate action-
type trapOnly
ip sla reaction-configuration 11 react mos threshold-
value 390 220 threshold-type immediate action-type
trapOnly

ip sla schedule 11 start-time now
```

Enhanced Objects Tracking for IP SLA

- The Enhanced Object Tracking feature separates the tracking mechanism from the protocol and creates a separate standalone tracking process that can be used by any other process
- Subset of the Enhanced Object Tracking Cisco IOS feature:

  Track the output from the IP SLA objects and use the provided information to trigger an action
- Aspects of an IPSLA operations which can be tracked: state and reachability
- Introduced in 12.3(4)T and 12.2(25)S

Example: HSRP and IPSLA Tracking

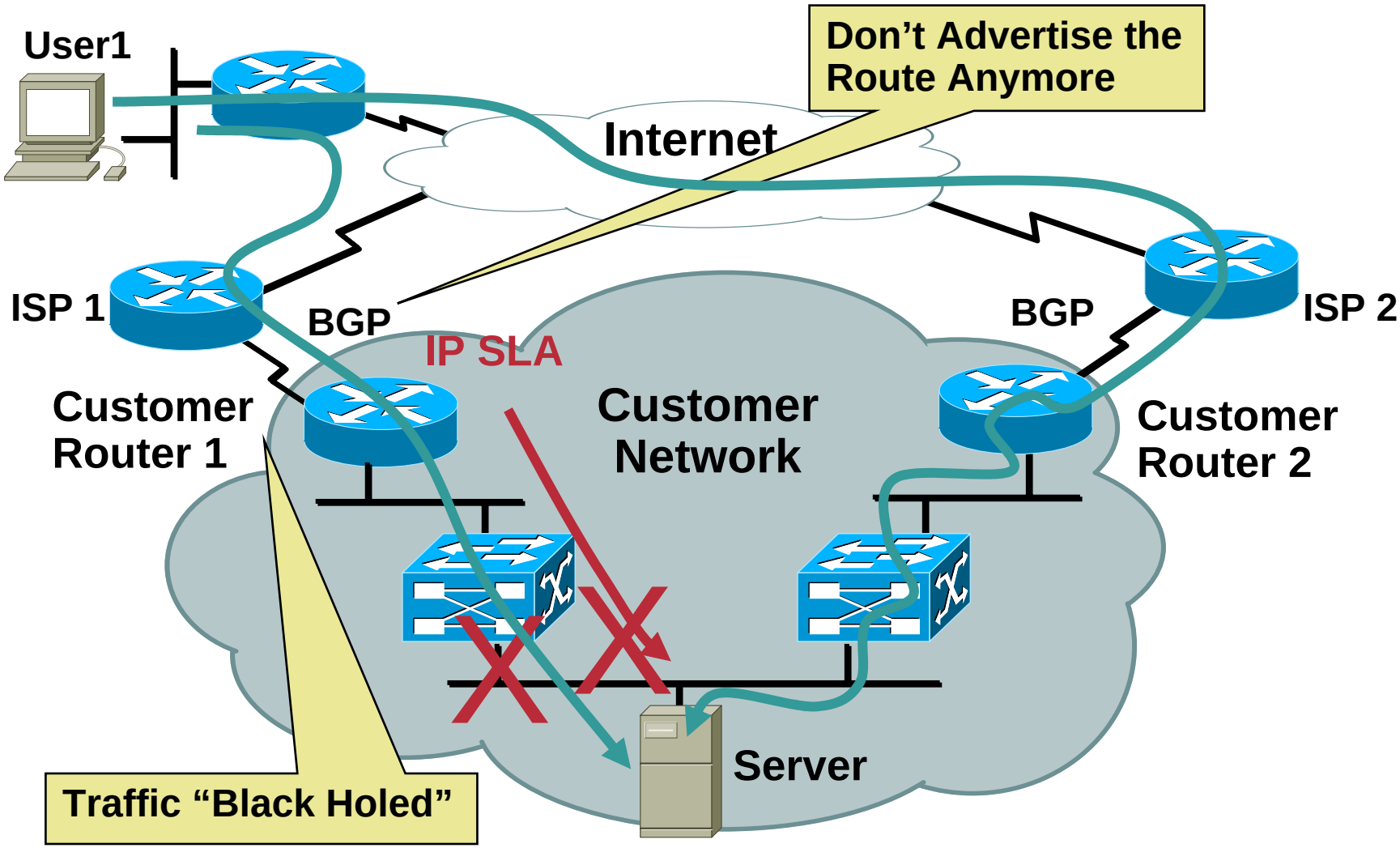


Example: HSRP and IP SLA Tracking


```
Router1(config)#
     ip sla 18
        icmp-echo <server>
     ip sla schedule 18 start-time now life forever
     track 100 rtr 18 state
     interface FastEthernet0/0
        ip address 10.10.10.1 255.255.255.224
        standby 1 ip 10.10.10.10
        standby 1 priority 105
        standby 1 preempt
        standby 1 track 100 decrement 10
```

Without Enhanced Object Tracking:
"Standby 1 track serial 0"
With Enhance Object Tracking:
The Object 100 Is Tracked

Example 2: Injecting Routes and IP SLA



Example 2:
Injecting Routes Into Routing Tables


```
Router1(config)#
   ip sla 1
      icmp-echo <server>
   ip sla schedule 1 start-time now life forever

   track 123 rtr 1 reachability
   ip route <server_network> 255.255.255.0 Null0 track 123
      (more specific routes will be used to forward packets)
   router bgp 65505
     redistribute static
```

The static route, advertised by BGP, will only exit if the reachability to the server Is OK!

EMBEDDED EVENT MANAGER

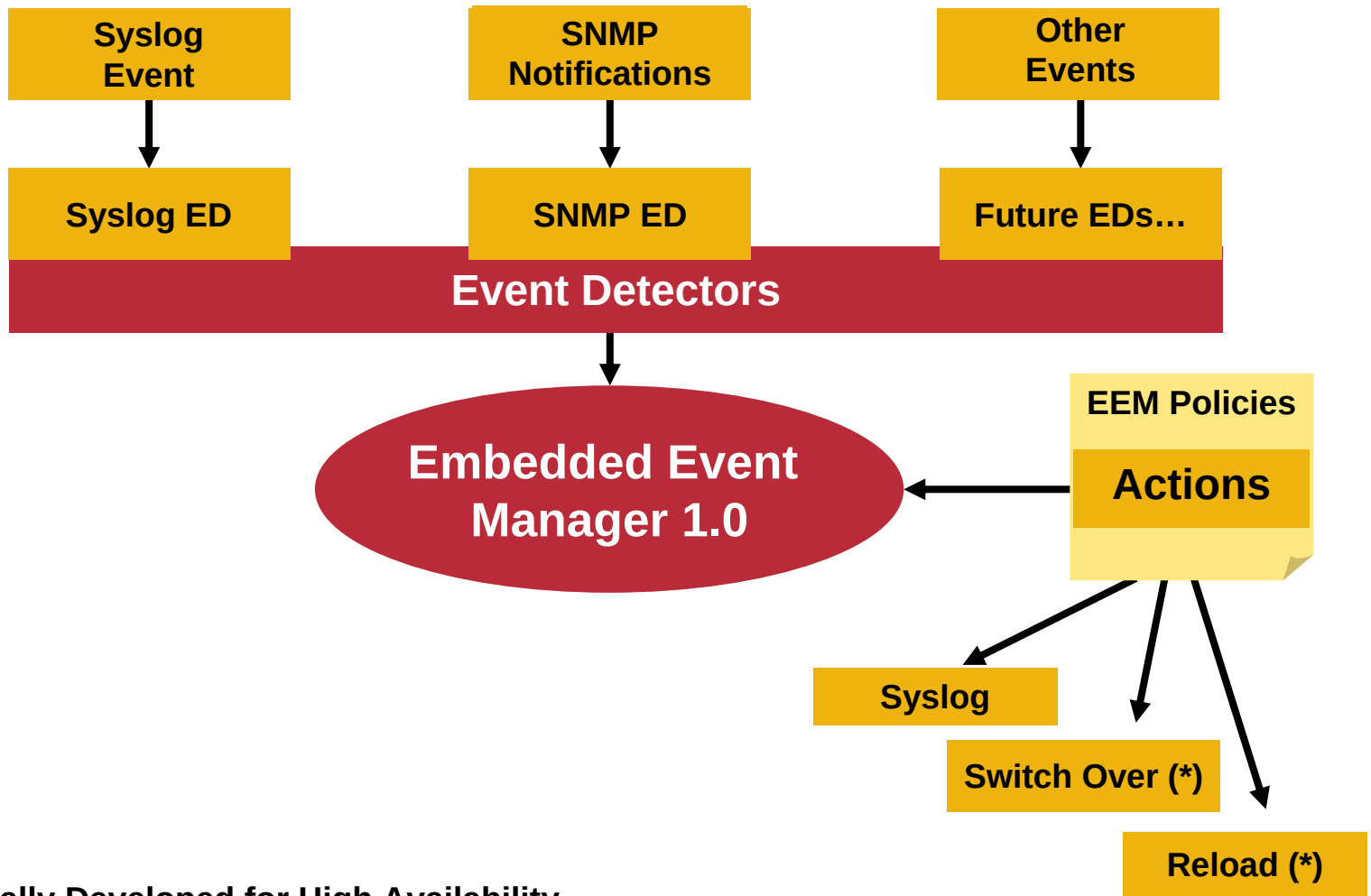
THE NEWEST IN CISCO IOS

Embedded Event Manager (EEM)

- 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; based on this, an action can be taken
- Advantages:

  Local programmable actions, triggered by specific events
- Version 1.0 introduced in 12.0(26)S, 12.3(4)T
- Version 2.0 introduced in 12.2(25)S
- Version 2.1 introduced in 12.3(14)T
- Version 2.2 introduced in 12.4(2)T

Embedded Event Manager (EEM) 1.0
The Framework



(*) Initially Developed for High Availability

Embedded Event Manager 1.0
Example 1: Syslog ED

- 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 emergencies msg “New
   syslog $_syslog_msg“
```

- Example: causes an emergency-level Syslog message when a log message indicates that the FastEthernet0/0 port changed state to either up or down

Embedded Event Manager 1.0
Example 2: Notification ED

ciscoMemoryPoolFree

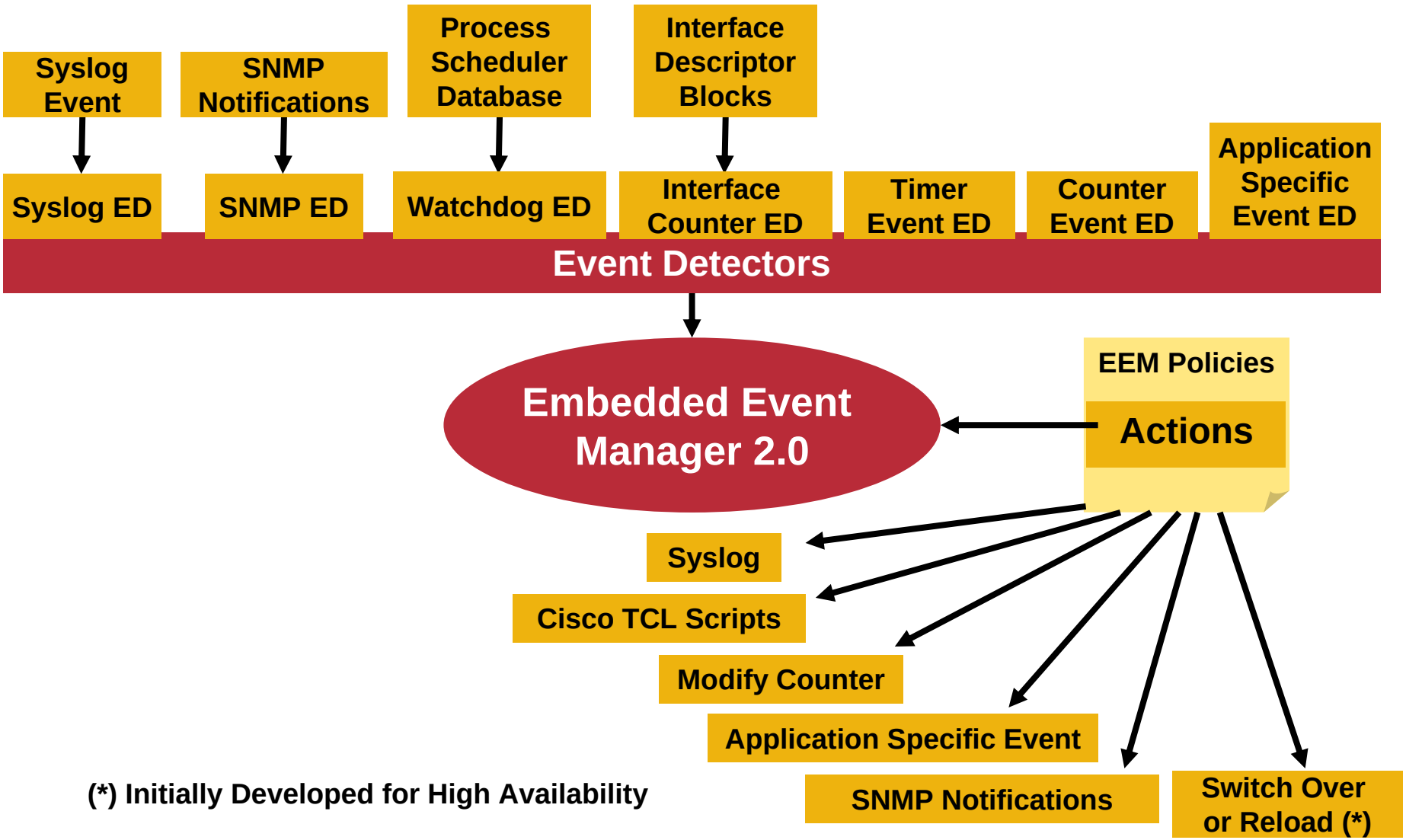
```
event manager applet memory-demo
 event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-
  type exact entry-op lt entry-val 512000 poll-
  interval 10
 action 1.0 syslog priority critical msg "Memory exh
  austed; current available memory is $_snmp_oid_val
   bytes"
 action 2.0 force-switchover
```

- **Example: the applet will run when the available memory on the primary RP falls below the specified threshold of 512000 bytes**

Embedded Event Manager 1.0
Environment Variables

- 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
- A lot more environment variables in the version 2.0, 2.1, and 2.2 → check the documentation

Embedded Event Manager 2.0
The Framework



(*) Initially Developed for High Availability

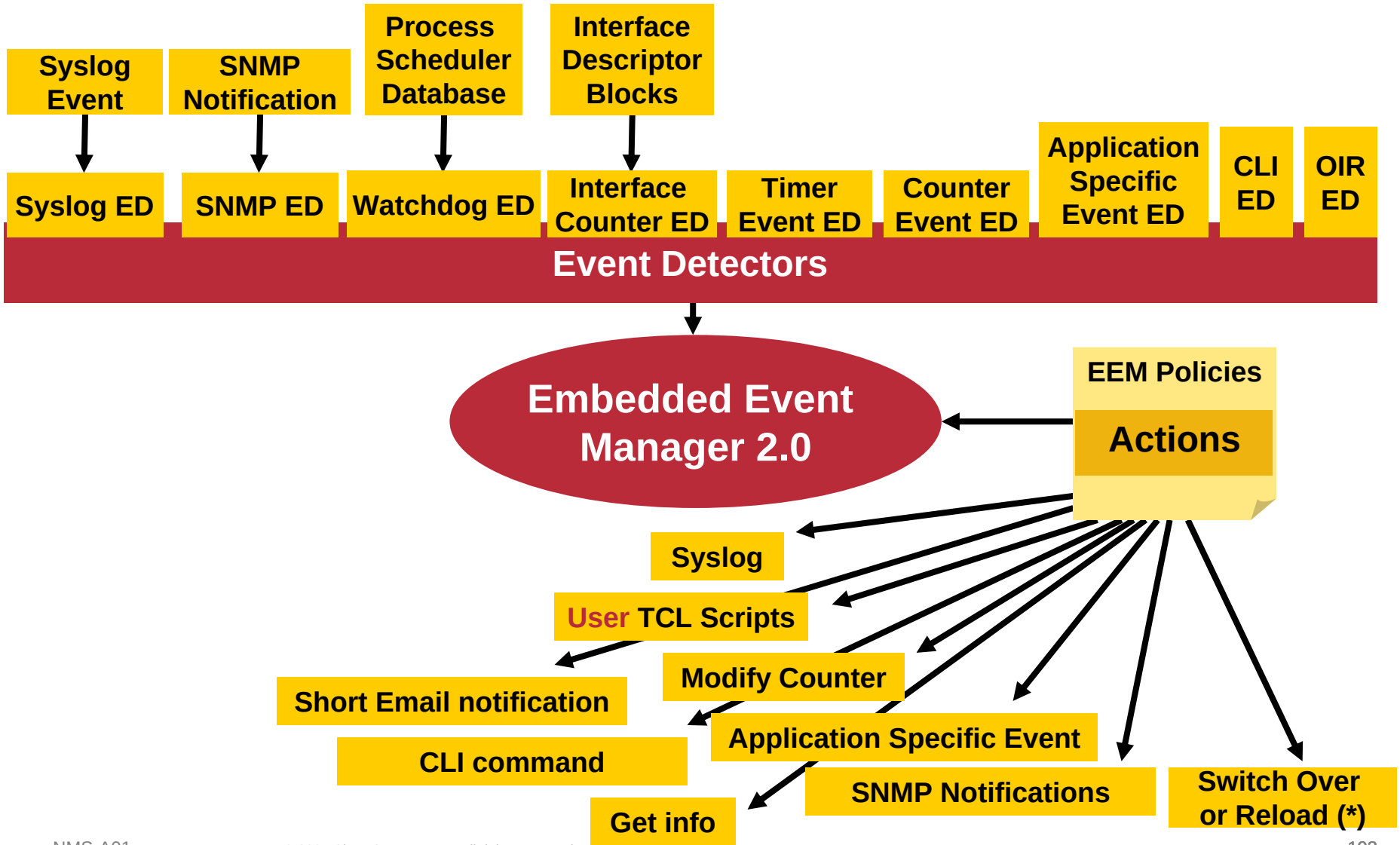
Embedded Event Manager 2.0
Example 3: Watchdog ED


```
event manager applet IOSWD_SNMPENGINE
  event ioswdsysmon sub1 cpu-proc taskname "SNMP
   ENGINE" op ge val 20 period 10
  action 2.0 snmp-trap intdata1 20 strdata "SNMP
   Engine above 20%"
snmp-server enable traps event-manager
```

- **Watchdog event detector example:**

  Monitor the “SNMP engine” process from “show processes cpu”; sent a trap if the CPU is above 20% for 10 seconds

Embedded Event Manager 2.1
The Framework



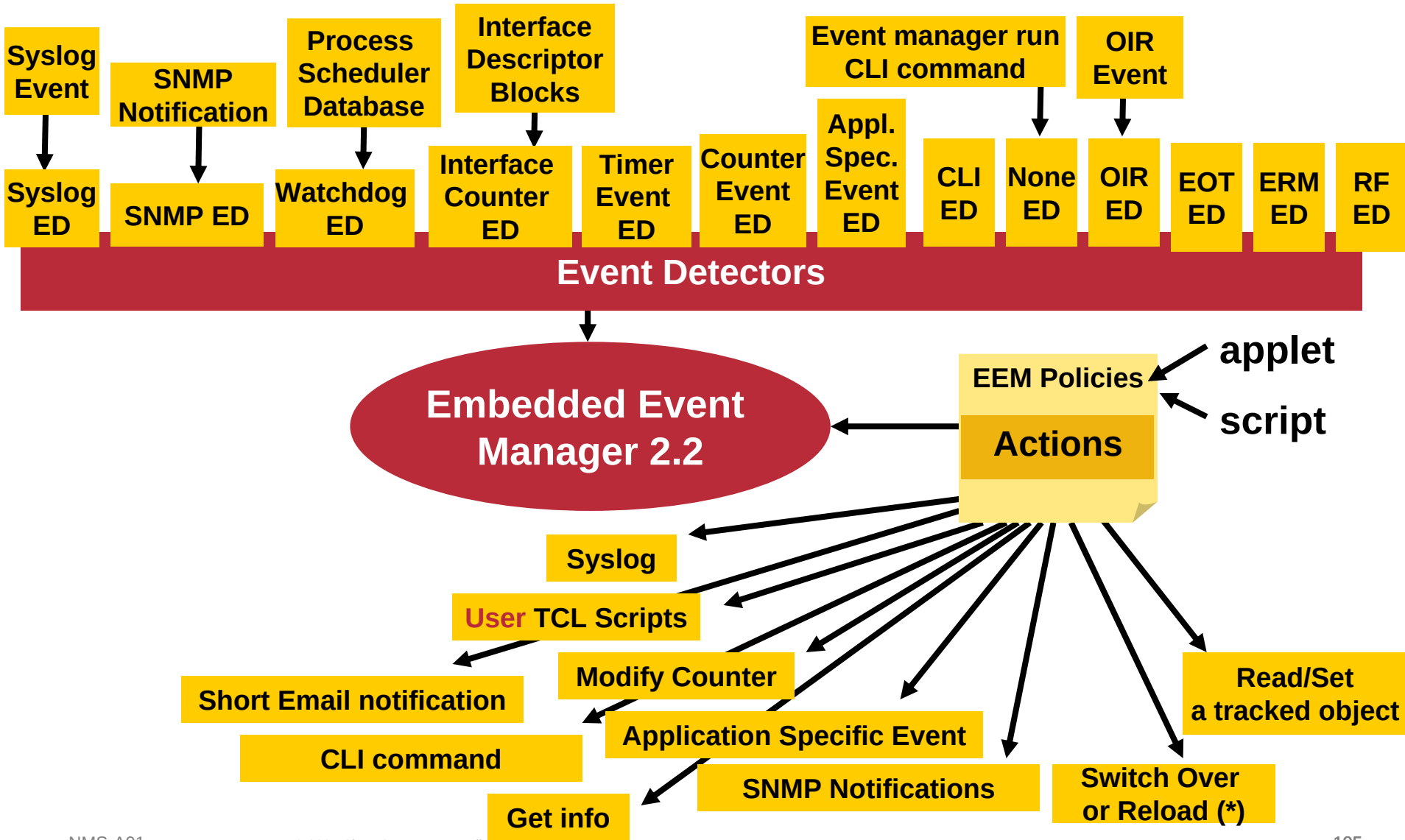
Embedded Event Manager 2.1
Example 4: CLI ED


```
event manager applet cli-match
   event cli pattern "router bgp 1" sync no skip no occurs 1
   action 1.0 syslog priority critical msg "$_cli_msg /
         configured at $_event_pub_time"

Router(config)#router bgp 1
Router(config-router)#
*Nov 22 12:05:59.047: %HA_EM-2-LOG: cli-match: router bgp 1
  configured at Nov 22 12:05:59.047
```

- **Command Line Interface (CLI) event detector example:**

  When the “router bgp 1” CLI command is entered, a syslog message is sent

Embedded Event Manager 2.2
The Framework



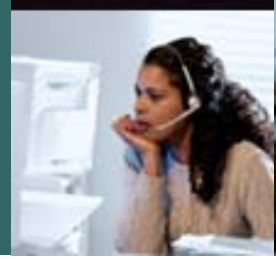
Embedded Event Manager 2.2

- **Amongst others, Enhanced Object Tracking Event Detector**
- **Advantages:**
  - **IP SLA state/reachability is supported by EOT**
  - **EOT now supported by EEM**
  - **EEM has got an implicit IP SLA Event Detector**

Embedded Event Manager Advantages

- More and more event detectors
- Automated local action triggered by events
  - TCL: scripting for Cisco written policies
  - Control is in the customer's hands: full customization
- Customized notifications, syslog, and email
  - Environment variables, redefined syslog priority level, etc.
- Can define your own applications in the router
- Some examples in the documentation
- My personal view:
  - EOT used for object tracking
  - + EEM for the action/fault management
  - + TCL for the customized action/fault management
  - = the perfect framework for any policy-based management

SUMMARY



Principles of Fault Management in Cisco Devices

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

Other Network Management Sessions

Cisco.com

- NMS-A02 Advanced Network Performance measurement with Cisco IOS IPSLA
- NMS-A03 Advanced NetFlow Usage
- NMS-A04 Advanced IOS Management Tools
- NMS-A05 Managing the MPLS core and MPLS VPNs
- NMS-A06 Operating your MPLS Core and IP VPNs
- NMS-D01 Zero Touch Provisioning and Configuration Management
- NMS-D02 Performance Measurement with Cisco Devices
- NMS-D03 Securely Managing Your Network and SNMPv3
- NMS-D04 Cisco Accounting Techniques
- NMS-D05 Management of Cisco IOS-XR platforms
- NMS-D06 Management of IP Telephony (for Enterprises)
- NMS-T01 CiscoWorks LMS 2.5 - A Practical Guide
- NMS-T02 MPLS Operations and Management: A Practical Guide

Recommended Reading

- Continue your Networkers learning experience with further reading from Cisco Press.
- Visit the on-site Cisco company store, where the full range of Cisco Press books is available for you to browse.

Management & Operations

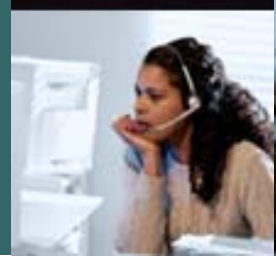
- Benoit Claise – Distinguished Service Engineer
- Bruno Klaser – Consulting Systems Engineer
- David Melton – Systems Engineer
- Monique Morrow – Distinguished Consulting Engineer
- Emmanuel Tychon – Software Engineer
- Anders Viden – Product Marketing Manager






Q and A

APPENDIX



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 Redundancy Checksum Errors	.1.3.6.1.4.1.9.2.2.1.1.12	15 Min	

Fault Management
Which MIB Variables to Monitor?

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	
locIfInputQueue Drops	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
locIfOutputQueue Drops	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		

Fault Management
Which MIB Variables to Monitor?

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

Fault Management
Which MIB Variables to Monitor?

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	

Fault Management
Which MIB Variables to Monitor?

Environment

	Object Descr	OID	Poll Int	Threshold
ciscoEnvMon FanState	The Current State of the Fan Being Instrumented	.1.3.6.1.4.1.9.9.13.1.4.1.3	15 Min	>= 1
ciscoEnvMon SupplyState	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

Fault Management
Which MIB Variables to Monitor?

Miscellaneous

	Object Descr	OID	Poll Int	Threshold
cpmCPUTotal 5min	Overall CPU Busy Percentage in the Last 5 Min Period; this Object Deprecates the avgBusy5 Object from the OLD-CISCO-SYSTEM-MIB	.1.3.6.1.4.1.9.9.109.1.1.1.1.5X	5 Min	< 30000
sysUpTime	System Uptime in 1/100ths of Seconds	.1.3.6.1.2.1.1.3	5 Min	< 30000

Recommended Reading

- Continue your Networkers learning experience with further reading from Cisco Press.
- Visit the on-site Cisco company store, where the full range of Cisco Press books is available for you to browse.

Management & Operations

- Benoit Claise – Distinguished Service Engineer
- Bruno Klauser – Consulting Systems Engineer
- David Melton – Systems Engineer
- Monique Morrow – Distinguished Consulting Engineer
- Emmanuel Tychon – Software Engineer
- Anders Viden – Product Marketing Manager