



Cisco
Networkers 2011
May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



Automations for Monitoring and Troubleshooting your Cisco IOS Network

Presented by Dan Jerome

An Analogy



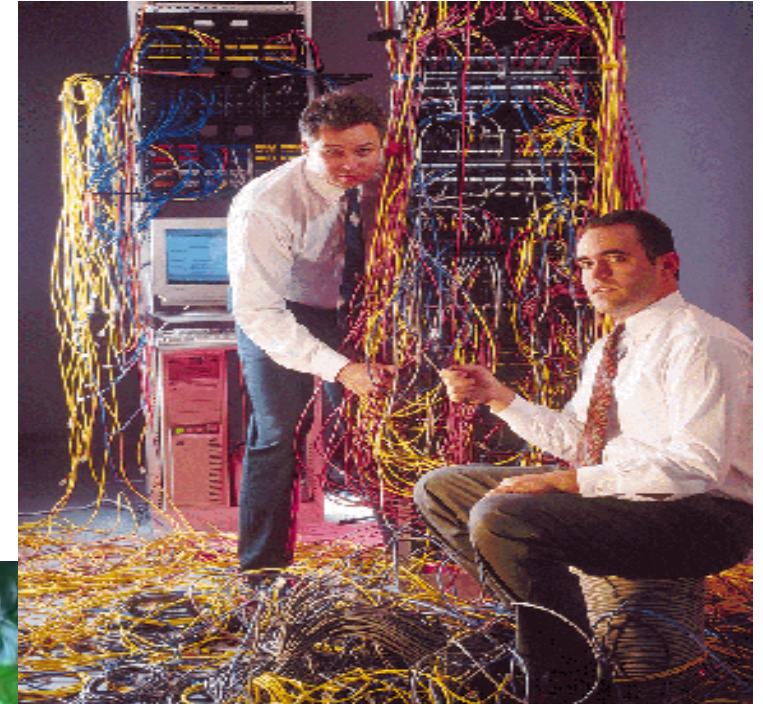
Airplane	Router
Instruments	Embedded Automations
21,000 sensors	OIDs in MIBs

With increasing scale, complexity, differentiation and availability requirements, operators rely on Embedded Automations

From: Full control by a single central authority

To: Operating a system of self-managing components

The Human Factor ...



Device Manageability Instrumentation



Cisco IOS® Device Manageability Instrumentation (DMI)

Fault

- § **IP OAM**—Ping, Trace, BFD, ISG per session
- § **802.3ah**—Link monitoring and remote fault indication
- § **802.1 ag**—Continuity check, L2 ping, trace, AIS
- § **MPLS OAM**—LSP ping, LSP trace, VCCV
- § **EEM**—Embedded Event Manager
- § **EVENT-MIB**—OID-based triggers, events, or SNMP Set, IETF DISMON
- § **EXPRESSION-MIB**—OID expression-based triggers, IETF DISMON
- § ...

Configuration

- § **Config CLI**—diff, logging, lock, replace, rollback
- § **E-LMI**—parameter and status signaling
- § **E-DI**—Enhanced Device Interface, CLI, Perl, IETF Netconf
- § **EMM** — Embedded Menu Manager
- § **NETCONF**—IETF NETCONF XML PI
- § **CNS** and **WSMA**
- § **TR-069**
- § **KRON**—command scheduler
- § **AutoInstall**—bootstrapping
- § **IOS.sh** —IOS Shell
- § **SmartInstall**
- § **Auto SmartPorts**
- § ...

Performance

- § **Auto IP SLA**—delay, jitter, loss probability
- § **CBQoS MIB**—class-based QoS
- § **NBAR**
- § **RMON**
- § **EPC** – Embedded Packet Capture
- § **ERM**—Embedded Resource Manager
- § **GOLD**—Generic Online Diagnosis
- § **Smart Call Home**—preventive maintenance
- § **VidMon**—Video Monitoring
- § ...

Accounting

- § **Flexible NetFlow**—IETF IPFIX
- § **BGP policy accounting** – includes AS information
- § **Periodic MIB bulk data collection and transfer**
- § ...

Security

- § **Auto Secure**—one-touch device hardening
- § **LDP Auth**—message authentication
- § **Routing Auth**—MD5 authentication, BGP, OSPF
- § ...

Device Manageability Instrumentation Has Evolved

Packaging Embedded Automations

Problem: Automations may consist of multiple elements – how to deploy them in a professional and efficient manner ?

Solution I: Write detailed requirements and step-by-step instructions

Solution II: Create an installable EASy package

- § Package Description
- § Pre-Requisite Verification
- § Pre-Installation Config
- § Pre-Installation Exec
- § Environment Variables
- § Configuration
- § Files
- § Post-Requisite Verification
- § Post-Installation Config
- § Post-Installation Exec
- § Uninstall

EASy Installer

=

Menu Guided Installation

+

MyPackage.tar



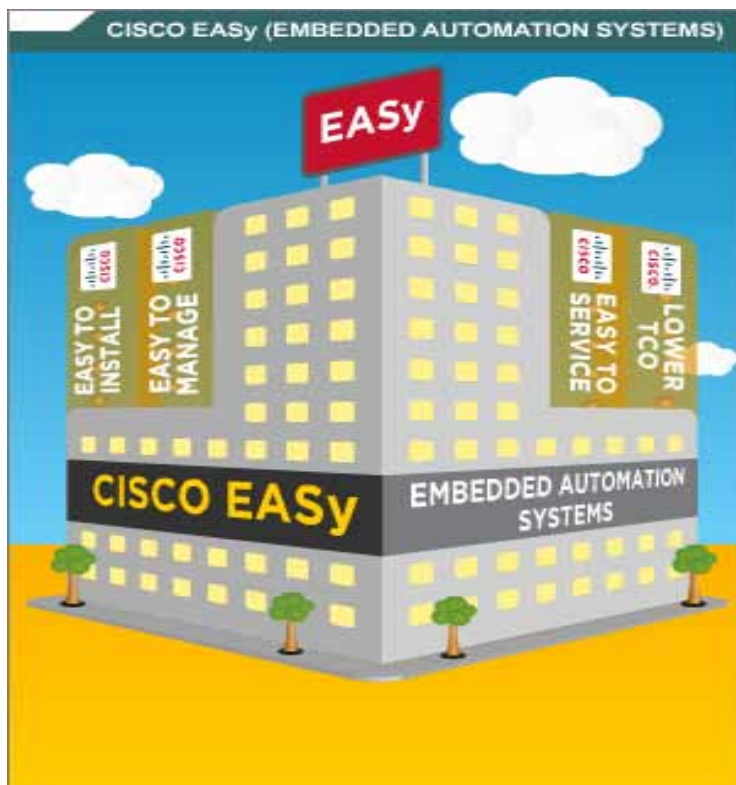
```
Router# easy-installer tftp://10.1.1.1/mypackage.tar flash:/easy
-----
Configure and Install EASy Package 'mypackage-1.03'
-----
1. Display Package Description
2. Configure Package Parameters
3. Deploy Package Policies
4. Exit

Enter option: 2
```

See: <http://www.cisco.com/go/easy>

See: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps10777/application_note_c27-574650.html

Embedded Automation Systems



Embedded Automation Systems (EASy)

1. Browse and Download EASy Packages
www.cisco.com/go/easy
2. Make Sure to also download EASy Installer
3. Browse Other Embedded Automations
www.cisco.com/go/ciscobeyond
4. Learn About The Technology Under The Hood
www.cisco.com/go/instrumentation
www.cisco.com/go/eem
www.cisco.com/go/pec
5. Discuss, Ask Questions, Suggest Answers
supportforums.cisco.com
6. Upload your own Examples to CiscoBeyond
www.cisco.com/go/ciscobeyond
7. Engage via ask-easy@cisco.com



Cisco
Networkers 2011
May 19, Toronto, Canada

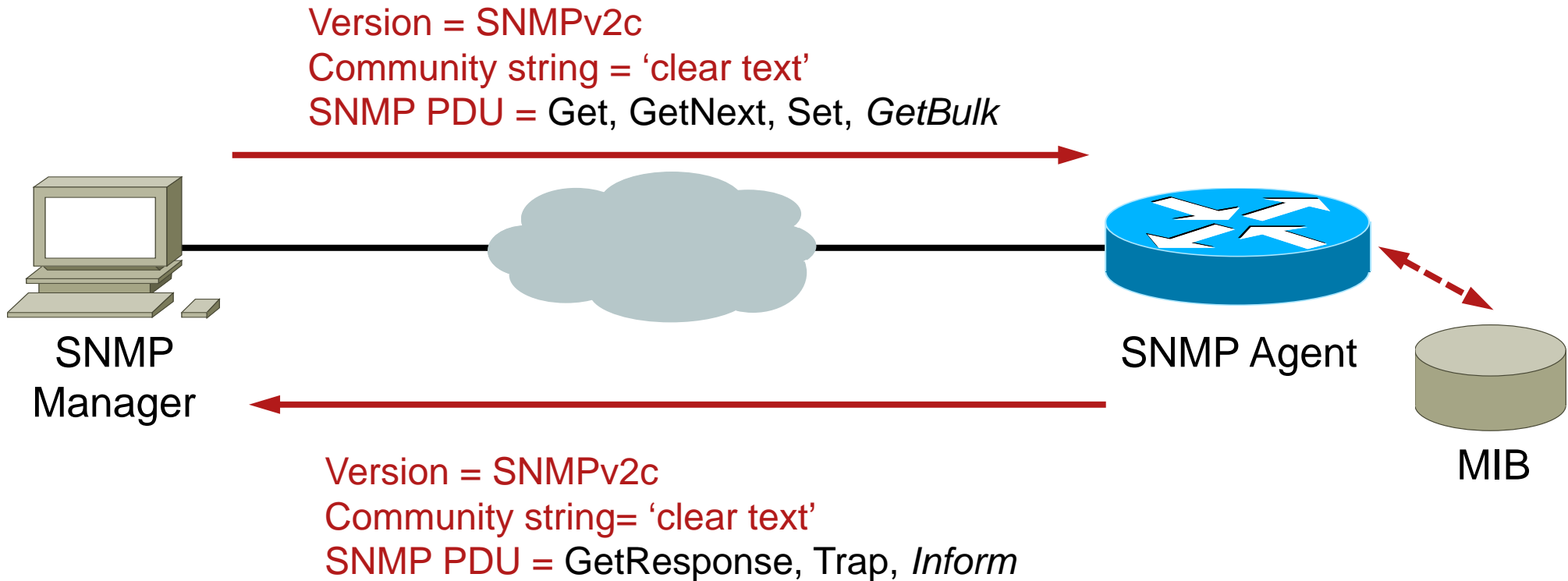
Knowledge
Is Power.
Learn. Share. Collaborate.



Agenda

- § Using SNMP for Monitoring
- § How to Analyze Transient Conditions?
- § What about the Service?
- § Who is doing What on the Network?
- § What if I need a Packet Capture?
- § Summary

SNMPv2c: Review



What's new in SNMPv3?

SNMPv3 defines two security-related capabilities:

§ The user-based security model (USM)

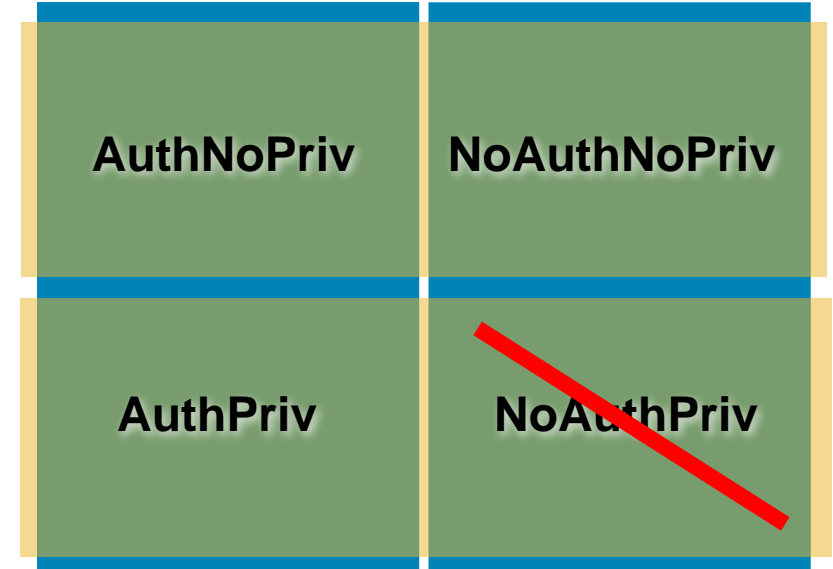
- provides authentication (user/password)
- privacy (encryption)

Note: operates at the message level

§ The view-based access control model (VACM)

- determines whether a given principal (user) is allowed access to particular MIB objects to perform particular functions

Note: operates at the PDU level



Available from: IOS 12.0(3)T, 12.0(6)S

See: http://www.cisco.com/en/US/partner/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

Where to start with MIBs?

MIB Locator:

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

Image Information	Details	Download MIB
c1900-universalk9-mz.SPA.151-2.T.bin	Get list of features for this image from Cisco Feature Navigator	
MIBs Supported in this Image		
ADSL-DMT-LINE-MIB	V1	V2
ADSL-LINE-MIB	V1	V2
ATM-MIB	V1	V2
BGP4-MIB	V1	V2
BRIDGE-MIB	V1	V2
CISCO-AAA-SERVER-MIB	V1	V2
CISCO-AAL5-MIB	V1	V2
CISCO-ACCESS-ENVMON-MIB	V1	V2
CISCO-ADSL-DMT-LINE-MIB	V1	V2
CISCO-ATM-EXT-MIB	V1	V2

SNMP Object Navigator:
<http://www.cisco.com/go/mibs>

Which OIDs are actually being used?

Example: CiscoView polling

```
Router#show snmp statistics oid
```

time-stamp	#of times requested	OID
16:16:50 CET Jan 12 2005	97	sysUpTime
16:16:50 CET Jan 12 2005	9	cardTableEntry.7
16:16:50 CET Jan 12 2005	9	cardTableEntry.1
16:16:50 CET Jan 12 2005	4	cardTableEntry.9
16:16:50 CET Jan 12 2005	16	ifAdminStatus
16:16:50 CET Jan 12 2005	16	ifOperStatus
16:16:50 CET Jan 12 2005	6	ciscoEnvMonSupplyStatusEntry.3
16:16:50 CET Jan 12 2005	17	ciscoFlashDeviceEntry.2
16:16:50 CET Jan 12 2005	8	ciscoFlashDeviceEntry.10
16:16:50 CET Jan 12 2005	2	ltsLineEntry.1
16:16:50 CET Jan 12 2005	2	chassis.15
16:16:27 CET Jan 12 2005	11	ciscoFlashDeviceEntry.7
16:16:27 CET Jan 12 2005	2	cardIfIndexEntry.5
16:16:24 CET Jan 12 2005	1	ciscoFlashDevice.1

Available from: IOS 12.0(22)S, 12.4(20)T

Is there a way to quickly export SNMP Statistics?

Problem: Sometimes we need data from one or multiple MIBs, but

- we may not want to (re-)configure an NMS
- don't want to constantly poll
- need to gather data during temporary loss of connectivity

Solution: Use Bulk File MIB to define the data we need and periodically transfer it to a convenient location

- group data from multiple MIBs
- single, common polling interval
- buffer data
- transfer using RCP, FTP, TFTP
- format ASCII or Binary

Feature Name: Periodic MIB Data Collection and Transfer Mechanism

Available from: IOS 12.0(24)S, 12.2(25)S, 12.3(2)T, IOS XE 2.1, IOS XR 3.2

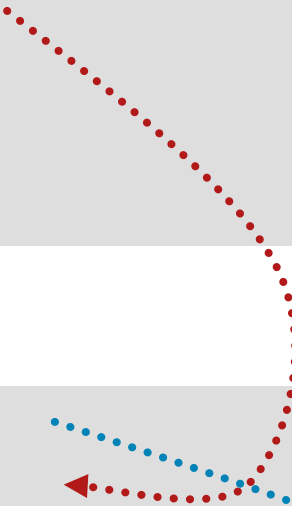
Platforms: ASR1k, x8xx ISR, x900x ISR, 72xx, 73xx, 76xx, 10xxx, ME3400, C4k, C6k, ...

See: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_mib_collect_trans.html

Service Planning Configuration – Example


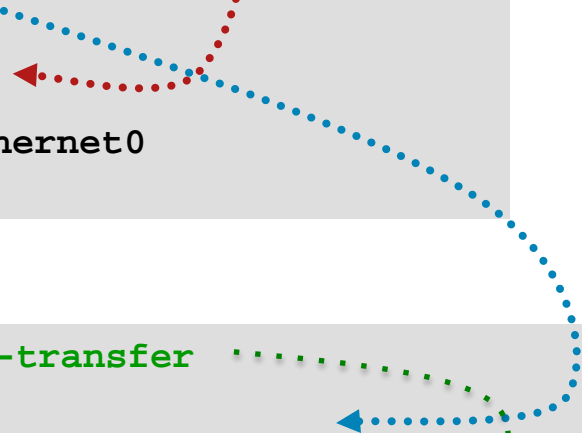
1. Define Lists of relevant OIDs (Names for IF-MIB, ASN.1 for all others)

```
Router(config)# snmp mib bulkstat object-list my-if-data
Router(config-bulk-objects)# add ifIndex
Router(config-bulk-objects)# add ifDescr
Router(config-bulk-objects)# add ifAdminStatus
Router(config-bulk-objects)# add ifOperStatus
Router(config-bulk-objects)# exit
```




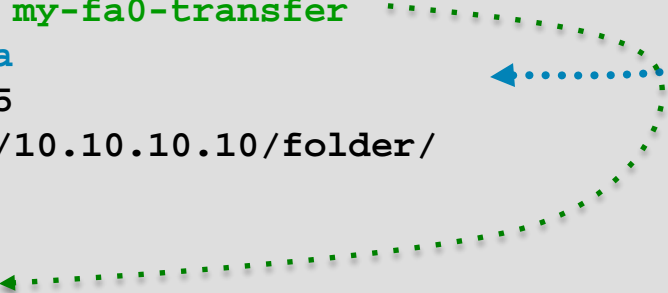
2. Specify Polling Schema

```
Router(config)# snmp mib bulkstat schema my-if-schema
Router(config-bulk-sc)# object-list my-if-data
Router(config-bulk-sc)# poll-interval 1
Router(config-bulk-sc)# instance exact interface FastEthernet0
Router(config-bulk-sc)# exit
```



3. Configure the Transfer Mechanism – and enable it !

```
Router(config)# snmp mib bulkstat transfer my-fa0-transfer
Router(config-bulk-tr)# schema my-if-schema
Router(config-bulk-tr)# transfer-interval 5
Router(config-bulk-tr)# url primary tftp://10.10.10.10/folder/
Router(config-bulk-tr)# retain 30
Router(config-bulk-tr)# buffer-size 4096
Router(config-bulk-tr)# enable
```



What if it's not in a MIB?

§ **Problem:** Collect data via SNMP, even if there is no MIB support currently available.

§ **Solution:** Expression-MIB provides the capability to process data into more relevant information via SNMP

- Expression-MIB can be configured using SNMP directly since 12.0(5)T.
- Initially Cisco Implementation was based on OID 1.3.6.1.4.1.9.10.22 but current Cisco implementation is based on RFC2982-MIB, OID 1.3.6.1.2.1.90.
- In 12.4(20)T Expression-MIB feature is enhanced to add CLIs to configure expressions.

§ Expression-MIB can gather data from Command Line Interface (CLI show commands), even if there is no MIB support

§ EVENT-MIB adds ability to send an event based on value of expression

§ EEM 3.1 provides similar capability without the need to involve Expression-MIB or Event-MIB

See: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_snmp_sup.html



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



How to Analyze Transient Conditions?

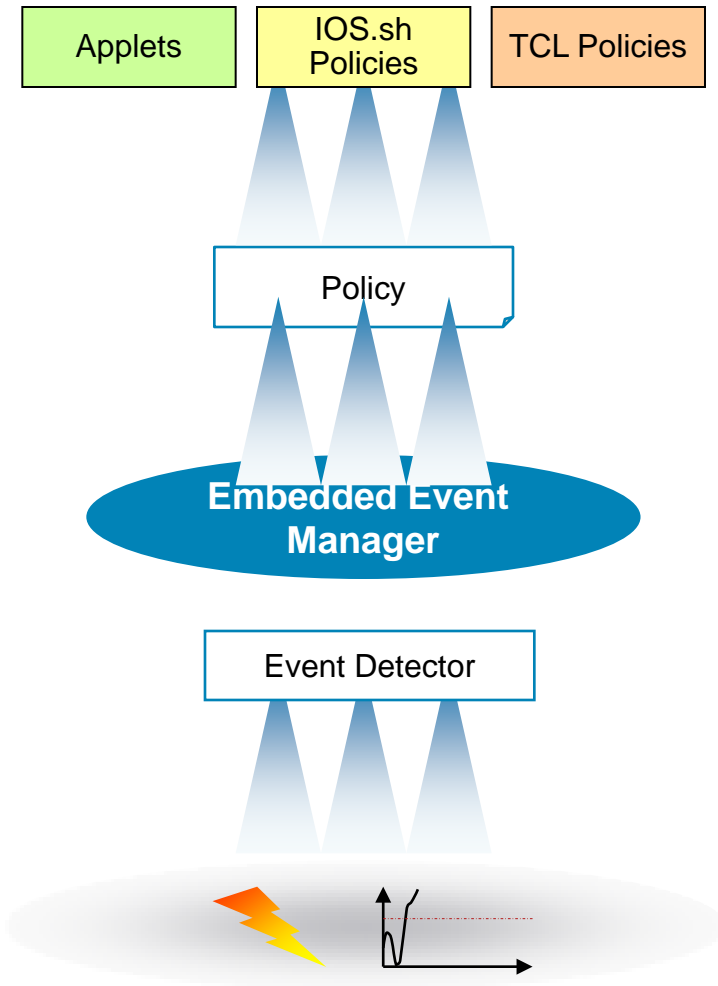
“Troubleshooting starts **before**
troubleshooting starts.

Be prepared.”

Source unknown



Embedded Event Manager (EEM)

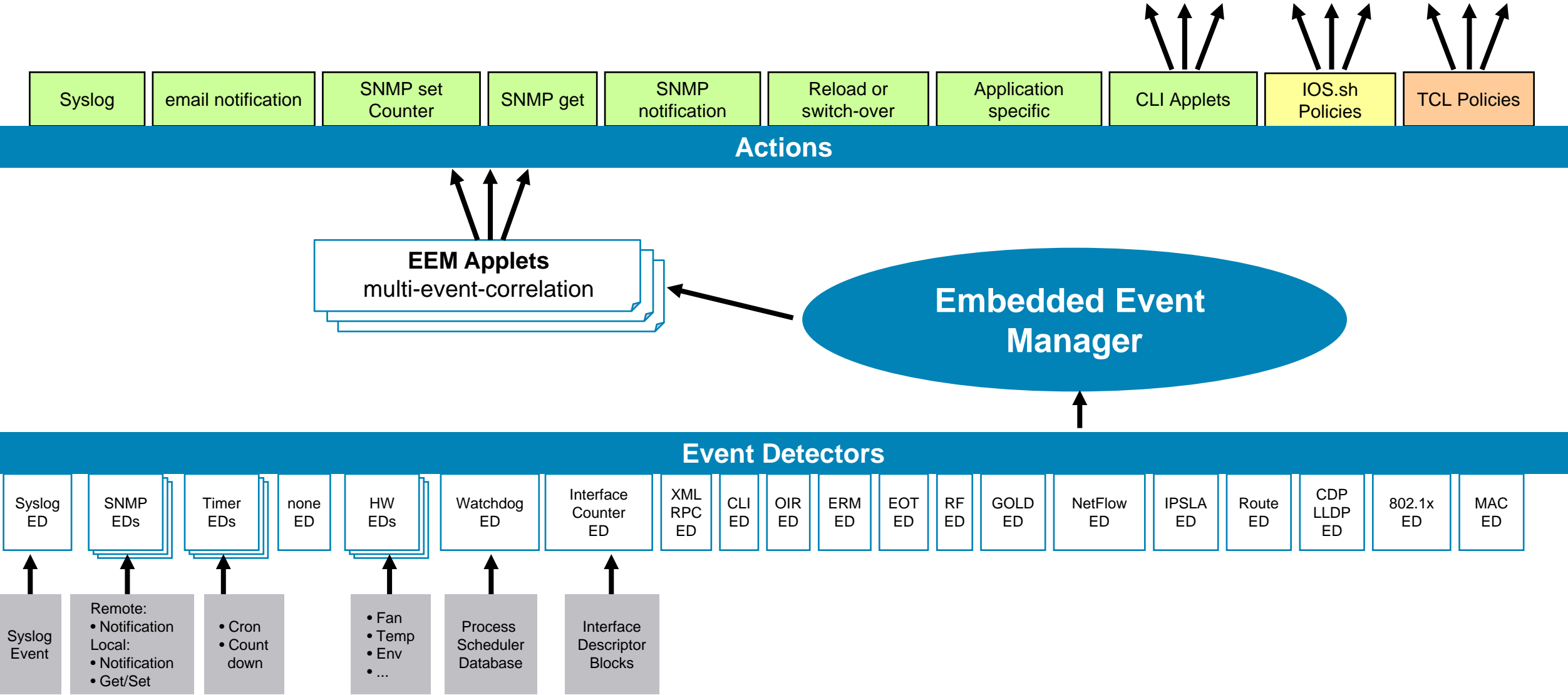


3. An EEM Policy is activated that initiates a pre-defined set of actions

2. An EEM Event Detector receives notification

1. Something happens on the  causing an Event to trigger

EEM Architecture



EEM Applets and Policies

CLI Applets

- § Part of the Cisco IOS Configuration
- § Based on CLI Commands
- § Simple Actions
- § Programmatic Applet Extensions

IOS.sh Policies

- § Separate ASCII File `my-policy.sh`
- § Based on Cisco IOS CLI and Shell Commands
- § Effective shell-like simple scripting
- § Registered via the Cisco IOS Config

TCL Policies

- § Separate ASCII File `my-policy.tcl`
- § Based on Cisco IOS CLI and Safe TCL Commands
- § Flexible and powerful scripting capabilities
- § Registered via the Cisco IOS Config

Embedded Event Manager (EEM) Versions

- § Embedded 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, a policy will trigger an action to be taken
- § Advantages: Local programmable actions, triggered by specific events – growing set of detectors and actions:
 - EEM 1.0 introduced in 12.0(26)S, 12.3(4)T
 - EEM 2.0 introduced in 12.2(25)S
 - EEM 2.1 introduced in 12.3(14)T
 - EEM 2.2 introduced in 12.4(2)T
 - EEM 2.3 introduced in 12.4(11)T
 - EEM 2.4 introduced in 12.4(20)T
 - EEM 3.0 introduced in 12.4(22)T
 - EEM 3.1 introduced in 15.0(1)M
 - EEM 3.2 introduced in 12.2(52)SE
 - stay tuned ...



Adds multi-event correlation



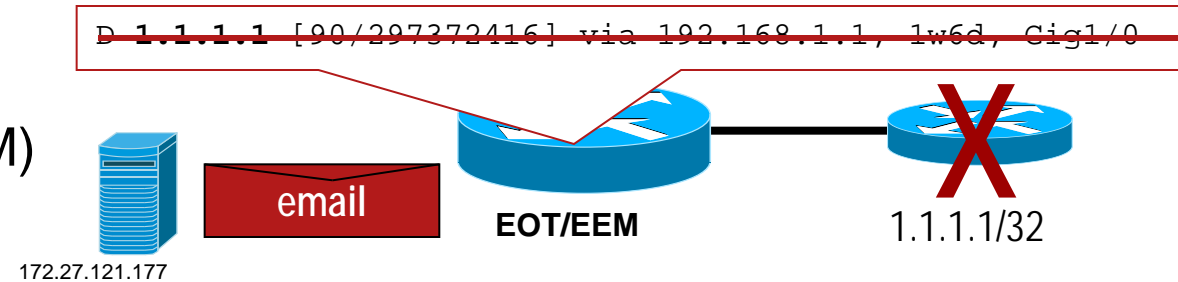
Adds programmatic Applets

Event Detector	Description (ED Triggers, based on ...)	EEM Version in IOS												IOS XR				IOS XE		NX-OS			
		1.0	2.0	2.1	2.2	2.3	2.4	3.0	3.1	3.2					3.6	4.0					2.1	2.2	4.0
Syslog	RegExp match of local syslog message	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
SNMP Notif	SNMP MIB Variable Threshold	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü										Ü	Ü	Ü	Ü
Watchdog	IOS process or subsystem activity events		Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
Interface Counter	(Interface) Counter Threshold		Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü										Ü	Ü	Ü	Ü
Timer	Designated Time or Interval		Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
Counter	Change of a designated counter value		Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
Application specific	An IOS subsystem or policy script		Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
CLI	RegExp match of input via command line interface			Ü	Ü	Ü	Ü	Ü	Ü	Ü										Ü	Ü	Ü	Ü
OIR	Hardware online insertion and removal OIR			Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü	Ü	Ü
none	No trigger, used in conjunction with exec command			Ü	Ü	Ü	Ü	Ü	Ü	Ü					Ü	Ü				Ü	Ü		
ERM	Embedded Resource Manager (ERM) events				Ü	Ü	Ü	Ü	Ü	Ü													
EOT	Enhanced Object Tracking variable (EOT) events				Ü	Ü	Ü	Ü	Ü	Ü										Ü	Ü	Ü	Ü
RF	IOS Redundancy Facility (switchover)				Ü	Ü	Ü	Ü	Ü	Ü										Ü	Ü		
GOLD	Generic Online Diagnostics (GOLD) events					Ü	Ü	Ü	Ü	Ü												Ü	Ü
SNMP Proxy	Incoming remote SNMP Notification							Ü	Ü	Ü	Ü												
XML RPC	Incoming XML message							Ü	Ü	Ü	Ü												
Routing	State change of Routing Protocols								Ü	Ü	Ü												
Netflow	Traffic Flow information from Netflow									Ü	Ü	Ü											
IPSLA	IPSLA events (supersedes EOT for EEM / IPSLA)									Ü	Ü	Ü											
CLI enhanced	Integrates CLI Ed with the XML PI									Ü	Ü	Ü											
SNMP Object	Intercept SNMP GET/SET requests										Ü	Ü											
Neighbor Disco	CDP, LLDP, Link up/down events											Ü											
Identity	802.1x and MAB authentication events											Ü											
MAC	MAC Address Table entry changes											Ü											
Hardware	Register for environmental monitoring hardware														Ü	Ü							
Statistics	Threshold crossing of a statistical counter														Ü	Ü							
Sysmgr	Process start and stop events														Ü	Ü							
Fan (absent / bad)	Presence and State of a Fan																					Ü	Ü
Module failure	Occurrence of a Module Failure Event																					Ü	Ü
Storm Control	Occurrence of a Storm Control Event																					Ü	Ü
Temperature	Temperature Sensor Thresholds																					Ü	Ü

EEM 2.0: EOT Event Detector

Problem: A Notification is required upon failure of a specific route

Solution: Track the Route using Enhanced Object Tracking (EOT) and Embedded Event Manager (EEM)

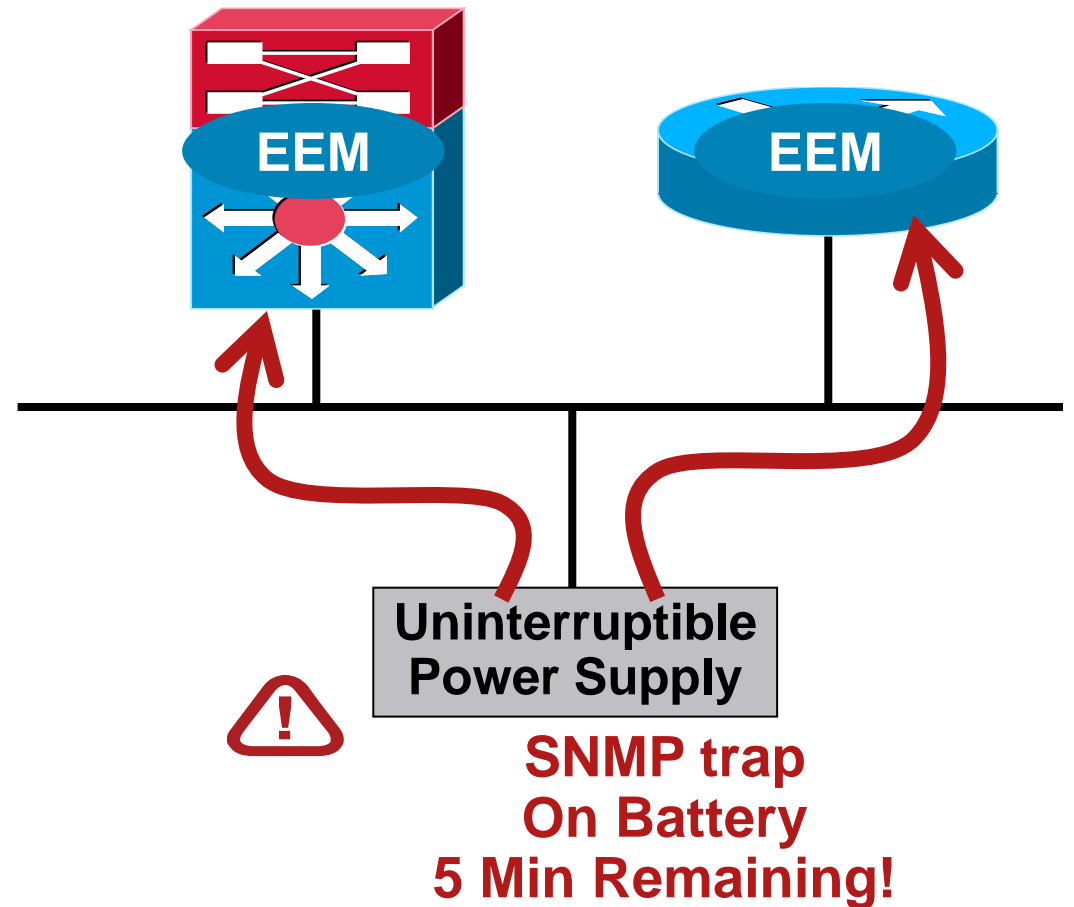


```
track 400 ip route 1.1.1.1/32 reachability
  delay down 10 up 10
!
event manager environment my_server 172.27.121.177
event manager environment my_from router-abc@customer.com
event manager environment my_to attach@cisco.com
event manager environment my_route 1.1.1.1/32
!
event manager applet email_track_iproute
event track 400 state down
action 1.0 syslog msg "Prefix to [$my_route] has been withdrawn!"
action 1.1 mail server "$my_server" to "$my_to" from "$my_from"
  subject "EEM: Prefix to Remote Site [$my_route] is DOWN" body ""
action 1.2 syslog msg "EEM: Path Failure alert email sent!"
```

Note: New Routing Event Detector in EEM 3.0

EEM 2.4: Proxy Event Detector

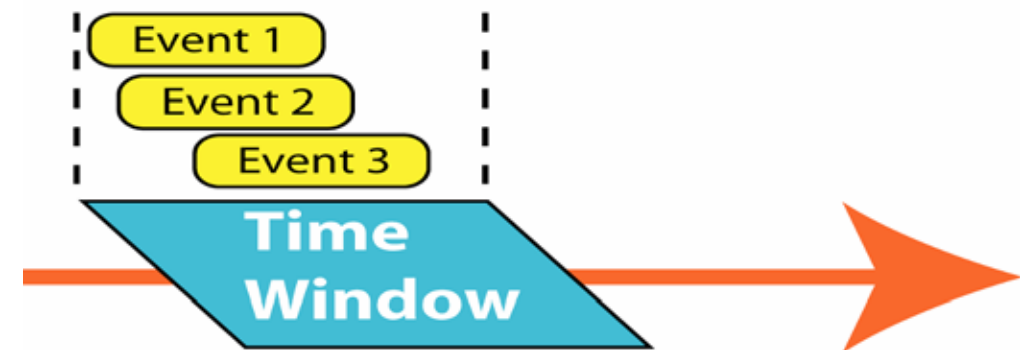
- § Router or switch can RECEIVE an SNMP trap
- § EEM event upon trap receipt
- § Execute (trigger) EEM script to take local action
- § Script sees varbind info in trap
- § Example:
 - UPS on battery backup
 - ====> Shut non-critical POE ports to conserve power
 - Only 5 minutes remaining
 - ====> Shutdown service modules gracefully
- § Example: managed Services



EEM 2.4: Multiple Event Correlation

- § Previous to EEM v2.4, there was a one-to-one correspondence between a single event and the triggered policy
- § In other words, a policy could only be triggered by a single event and any event correlation had to be coded by the user
- § ***Multiple Event Support ushers in an event correlation specification such that multiple events may be considered together to trigger a policy***
- § For example:
 - If (Event 1 OR Event 2) AND Event 3, then Trigger Policy A

Event Correlation Capabilities



EEM 2.4: Multiple Event Correlation

Problem: A Syslog message is required upon state change of either Ethernet1/0 or Ethernet1/1

Solution: Use Embedded Event Manager (EEM) Multiple Event Correlation with a correlate statement within the trigger block to define the logic between individual events and optional occurs clauses to define the number of times a specific event must be raised before being used in the correlation (inner level), or the number of times the total correlation must be true before invoking the action (outer level):

```
event manager applet example
  event tag e1 syslog pattern ".*UPDOWN.*Ethernet1/0.*"
  event tag e2 syslog pattern ".*UPDOWN.*Ethernet1/1.*"
  trigger occurs 1
    correlate event e1 or event e2
    attribute e1 occurs 1
    attribute e2 occurs 1
  action 1.0 syslog msg "Critical interface status change"
  set 2.0 _exit_status 0
```

EEM 3.0: Programmatic Applet Example

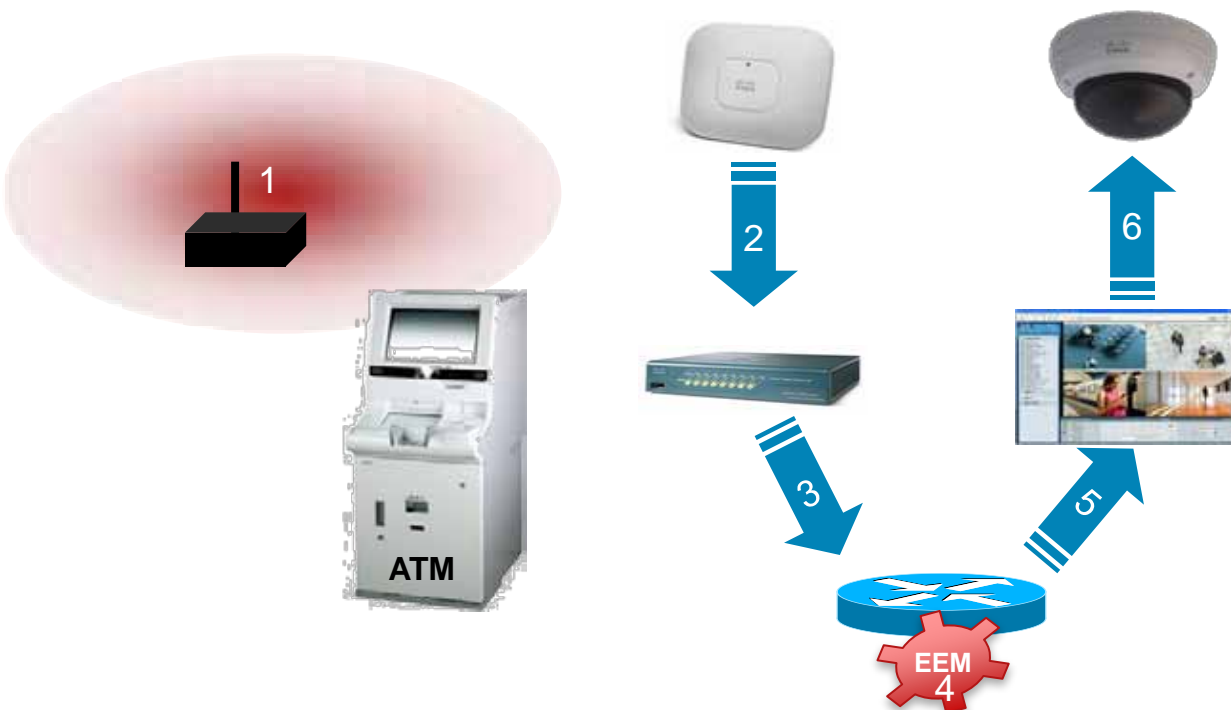
```
event manager applet route-watch
  event routing network 10.1.1.0/24 type add protocol ospf
  action 001 cli command "enable"
  action 002 set done 0
  action 003 while $done eq 0
  action 004   wait 5
  action 005   cli command "ping ip 10.1.1.1"
  action 005   regexp "!!!!!" "$_cli_result"
  action 006   if $_regexp_result eq 1
  action 007     cli command "config t"
  action 008     cli command "int Tunnel0"
  action 009     cli command "shut"
  action 010     cli command "end"
  action 011     set done 1
  action 012   end
  action 013 end
```

- § The applet will trigger when the route 10.1.1.0/24 is learned via OSPF
- § The applet will try and ping host 10.1.1.1, and when it is successful, it will take down the backup tunnel interface

Example: Integrating CleanAir and Security

Problem: A new rogue WLAN device in sensitive areas should be detected by Cisco CleanAir and automatically focus/pan/zoom a security camera.

Solution: Use Network Automation based on Cisco IOS Embedded Event Manager to receive an SNMP Notification from WLC and trigger the Video Operations Manager via HTTP



1. Rogue WLAN Device added
2. Rogue Device detected by CleanAir AP
3. WLC sends SNMP Notification
4. EEM triggers upon SNMP Notification
5. EEM notifies VSOM via HTTP
6. Security Camera Focus/Pan/Zoom

Using EEM step-by-step

1. Which problem do you want to solve?
2. Which event detector and action do you need?

– Upgrade to the right IOS image

```
show event manager detector <detector-type> detailed
```

3. Check whether a suitable script/applet is available already

- <http://www.cisco.com/go/ciscobeyond>
- <http://www.cisco.com/go/eem>
- <http://www.cisco.com/go/easy>

4. Work from an existing example

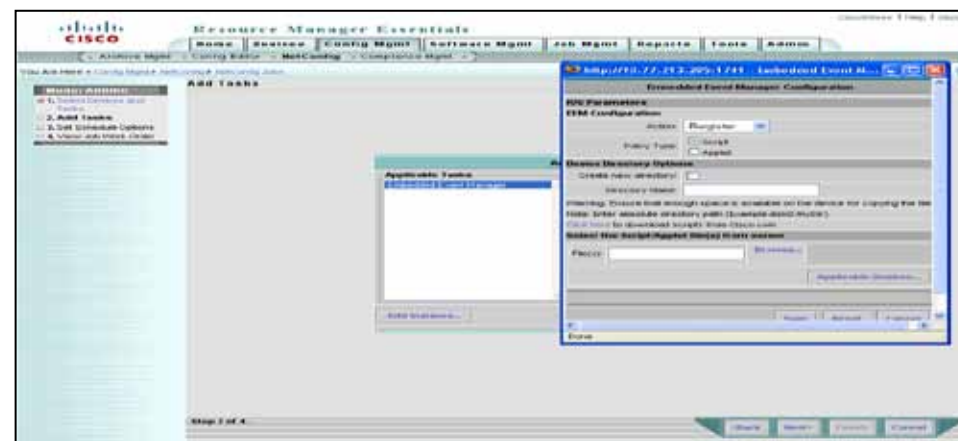
5. Deploy and Monitor

- CiscoWorks LMS (from 3.1) via RME
<http://www.cisco.com/go/lms>
- Davra Networks EEMLive
<http://www.davranetworks.com/>

6. If customization/new development/testing is required

- “Network Programming Advisors“ <http://www.progrizon.com/>
- Cisco Advanced Services

7. Don't forget to ask to (and share with) the EEM forum





Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



What about the Service?

IP Service Level Agreements (IP SLA)

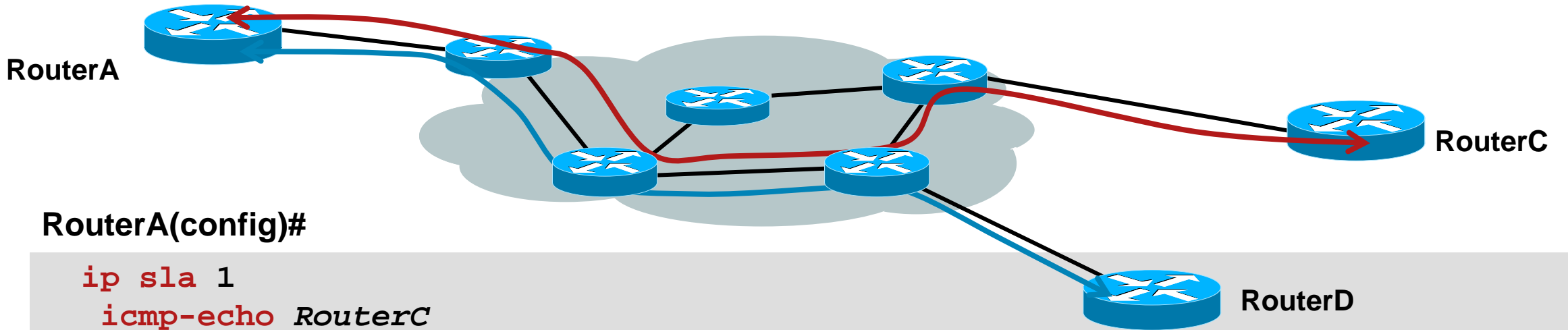
- § Active probing by injecting synthetic test traffic
- § Experience and Adoption across markets and technology domains
- § Vast range of Cisco and 3rd Party NMS tool support

Metrics	Latency		Jitter			Packet Loss			Connectivity		
Domains	IP	Ethernet		MPLS	VoIP		Services		Medianet		
Operations	ICMP Echo	ICMP Jitter	UDP PathEcho	TCP Connect	802.1ag Jitter	LSP Trace	PWE3 VCCV	H.323 GD	SIP GD	HTTP	DNS
	ICMP PathEcho	UDP Echo	UDP Jitter	802.1ag Echo	LSP Ping	LSP Tree	H.323 CS	SIP CS	DHCP	FTP	



See: www.cisco.com/go/ipsla

IP SLA – ICMP and UDP Jitter Examples



RouterA(config)#

```
ip sla 1
  icmp-echo RouterC
  timeout 500
  frequency 10
ip sla schedule 1 start-time now
```

```
ip sla 10
  udp-jitter RouterD 16384 num-packets 1000 interval 20
  request-data-size 172
  tos 20
  frequency 60
ip sla schedule 10 start-time now
```

IP SLA – ICMP Echo Operation

```
Router#show ip sla sta mon 1
Round trip time (RTT)    Index 1
      Latest RTT: 1 ms
Latest operation start time: *05:26:00.226 UTC Fri Jan 4 2008
Latest operation return code: OK
Number of successes: 1
      Number of failures: 0
Operation time to live: 188 sec
```

```
Router#sh ip sla sta 1 detail
Round trip time (RTT)    Index 1
      Latest RTT: 1 ms
Latest operation start time: *05:26:30.224 UTC Fri Jan 4 2008
Latest operation return code: OK
Over thresholds occurred: FALSE
Number of successes: 2
      Number of failures: 0
Operation time to live: 155 sec
Operational state of entry: Active
Last time this entry was reset: Never
```

IP SLA – UDP Jitter Operation

```
Router#sh ip sla statistics 10
Round trip time (RTT)    Index 10
    Latest RTT: 1 ms
Latest operation start time: *05:43:28.720 UTC Fri Jan 4 2008
Latest operation return code: OK RTT Values
    Number Of RTT: 10
    RTT Min/Avg/Max: 1/1/1 ms
Latency one-way time milliseconds
    Number of one-way Samples: 0
    Source to Destination one way Min/Avg/Max: 0/0/0 ms
    Destination to source one way Min/Avg/Max: 0/0/0 ms
Jitter time milliseconds
    Number of Jitter Samples: 9
    Source to Destination Jitter Min/Avg/Max: 20/20/23 ms
    Destination to Source Jitter Min/Avg/Max: 22/21/24 ms
Packet Loss Values
    Loss Source to Destination: 0          Loss Destination to Source: 0
    Out Of Sequence: 0          Tail Drop: 0          Packet Late Arrival: 0
Number of successes: 1
Number of failures: 0
Operation time to live: 3567 sec
```

Taking the next step

Network Automation with IP SLA

Problem

- § Need to monitor IP SLA
- § Trigger actions upon violation of SLA

Solutions

- § IP SLA Reaction Thresholds
- § Using EEM and the EOT Event Detector
- § Using EEM 3.x and the IP SLA Event Detector

Solution 1:

IP SLA Reaction Thresholds

```
RouterA(config)#
ip sla 10
  icmp-echo 3.3.3.3
  frequency 10
ip sla reaction-configuration 10 react timeout threshold-type consecutive 3 action-type trapAndTrigger
ip sla schedule 10 life forever start-time now
ip sla reaction-trigger 10 20

logging on
ip sla logging trap
snmp-server host nms_server version 2c public
snmp-server enable traps syslog
```

Send an SNMP trap after 3 consecutive timeouts and trigger IP SLA operation 20

Solution 2: Enhanced Object Tracking and EEM

IP SLA

```
ip sla 10  
icmp-echo 3.3.3.3  
timeout 500  
frequency 3  
ip sla schedule 10 life forever start-time now
```

Enhanced Object Tracking (EOT)

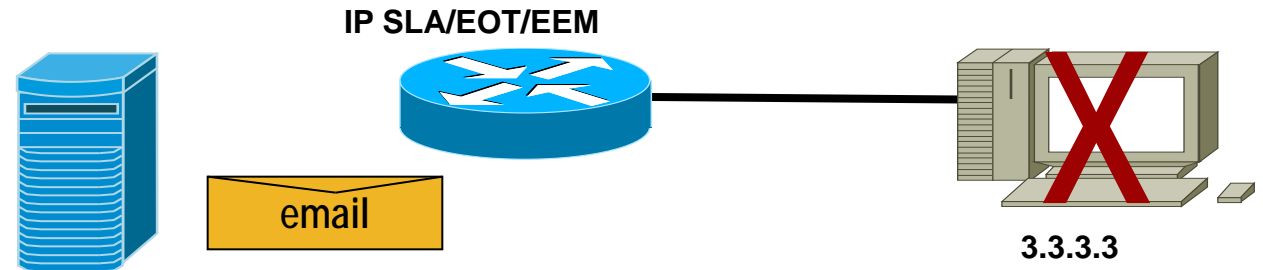
```
track 10 rtr 10 reachability  
delay down 10 up 20
```

Environment Variables

(\$_* variables to be defined)

EEM Applet

```
event manager applet email_server_unreachable  
event track 10 state down  
action 1.0 syslog msg "Ping has failed, server unreachable!"  
action 1.1 cli command "enable"  
action 1.2 cli command "del /force flash:server_unreachable"  
action 1.3 cli command "show clock | append server_unreachable"  
action 1.4 cli command "show ip route | append server_unreachable"  
action 1.5 cli command "more flash:server_unreachable"  
action 1.6 mail server "$_email_server" to "$_email_to" from "$_email_from" subject "Server Unreachable: ICMP-Echos  
Failed" body "$_cli_result"  
action 1.7 syslog msg "Server unreachable alert has been sent to email server!"
```



Solution 3:

IP SLA Event Detector in EEM 3.0

```
Router(config)# ip sla 10
Router(config-ip-sla)# icmp-echo 3.3.3.3

Router(config)# ip sla enable reaction-alerts

Router(config)# ip sla reaction-config 10 react timeout threshold-type consecutive 3 action-type none

Router(config)# ip sla schedule 10 start now

Router(config)# event manager applet test
router(config-applet)# event ipsla operation-id 10 reaction-type timeout
router(config-applet)# action 1.0 syslog priorities emergencies
    msg "IP SLA operation $_ipsla_oper_id to server XYZ has timed out"
```

Trigger an Embedded Event Manager Applet after 3 consecutive timeouts of the IP SLA operation

Auto IP SLA – Don't touch your Hub

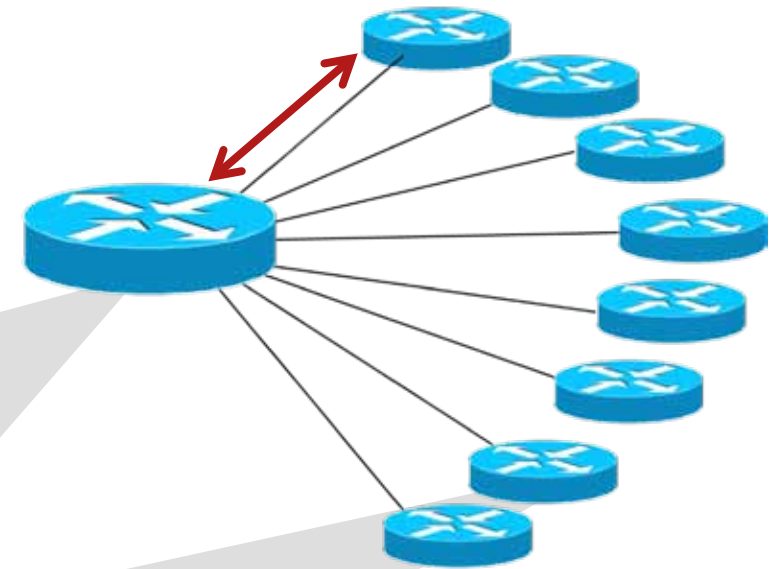
Some IP SLA Topologies ...

§ ... are naturally Hub and Spoke

§ ... have a large number of Spokes with similar IP SLA requirements

§ ... consist of dynamically joining / disappearing Spokes

```
ip sla auto template type ip udp-jitter my-ipsla-template
  parameters
    request-data-size 64
    num-packets 1000
ip sla auto schedule my-ipsla-schedule
  frequency 45
  start-time now
ip sla auto endpoint-list type ip my-ipsla-endpoints
  discover
    ageout 36000
ip sla auto group type ip my-ipsla-group
  schedule my-ipsla-schedule
  template udp-jitter my-ipsla-template
  destination my-ipsla-endpoints
```

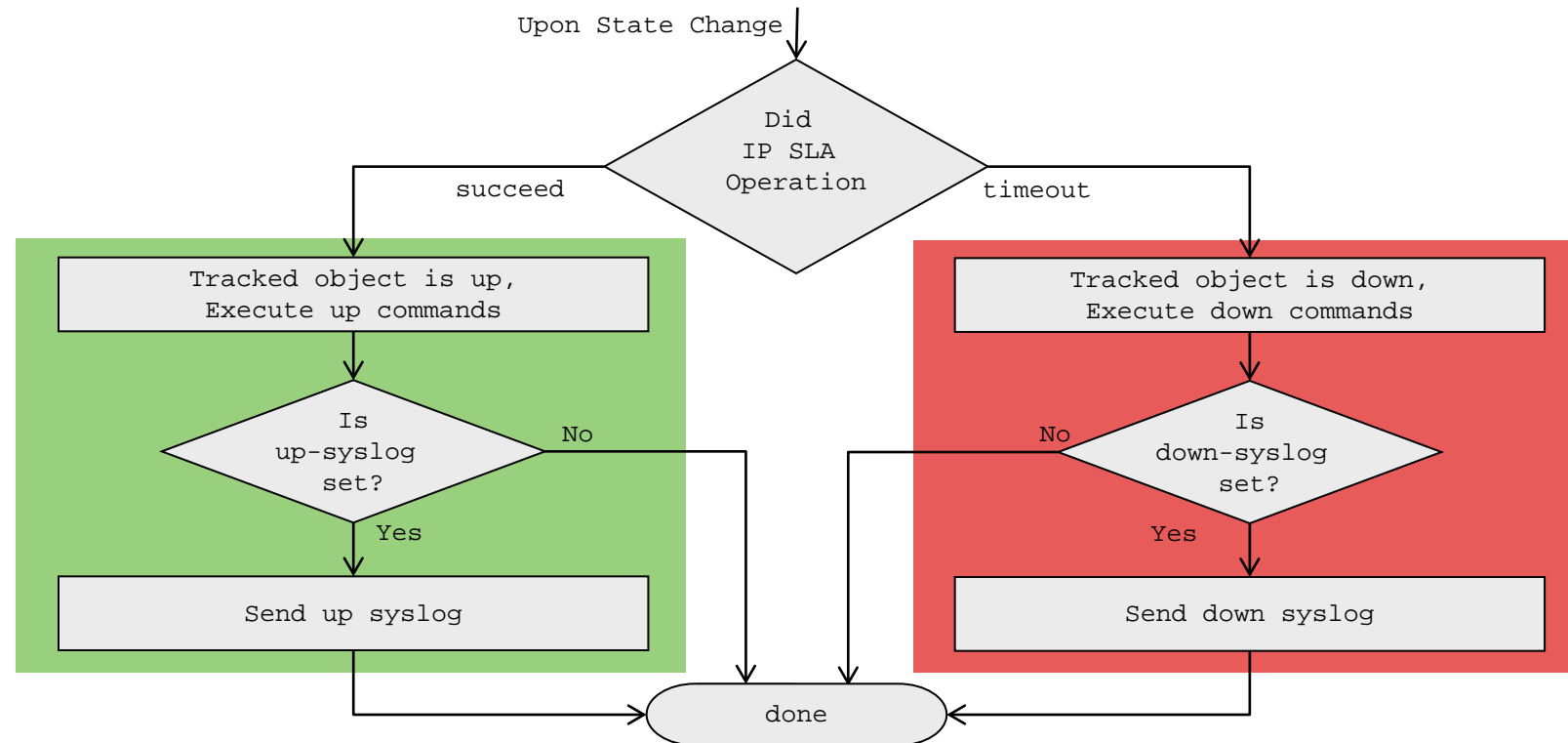


```
ip sla responder auto-register 10.10.10.2 endpoint-list my-ipsla-endpoints
```

EASy Package: Custom High-Availability

Problem: We need a failover from primary to secondary link – but with flexibility and custom notification beyond what a simple routing protocol based solution provides

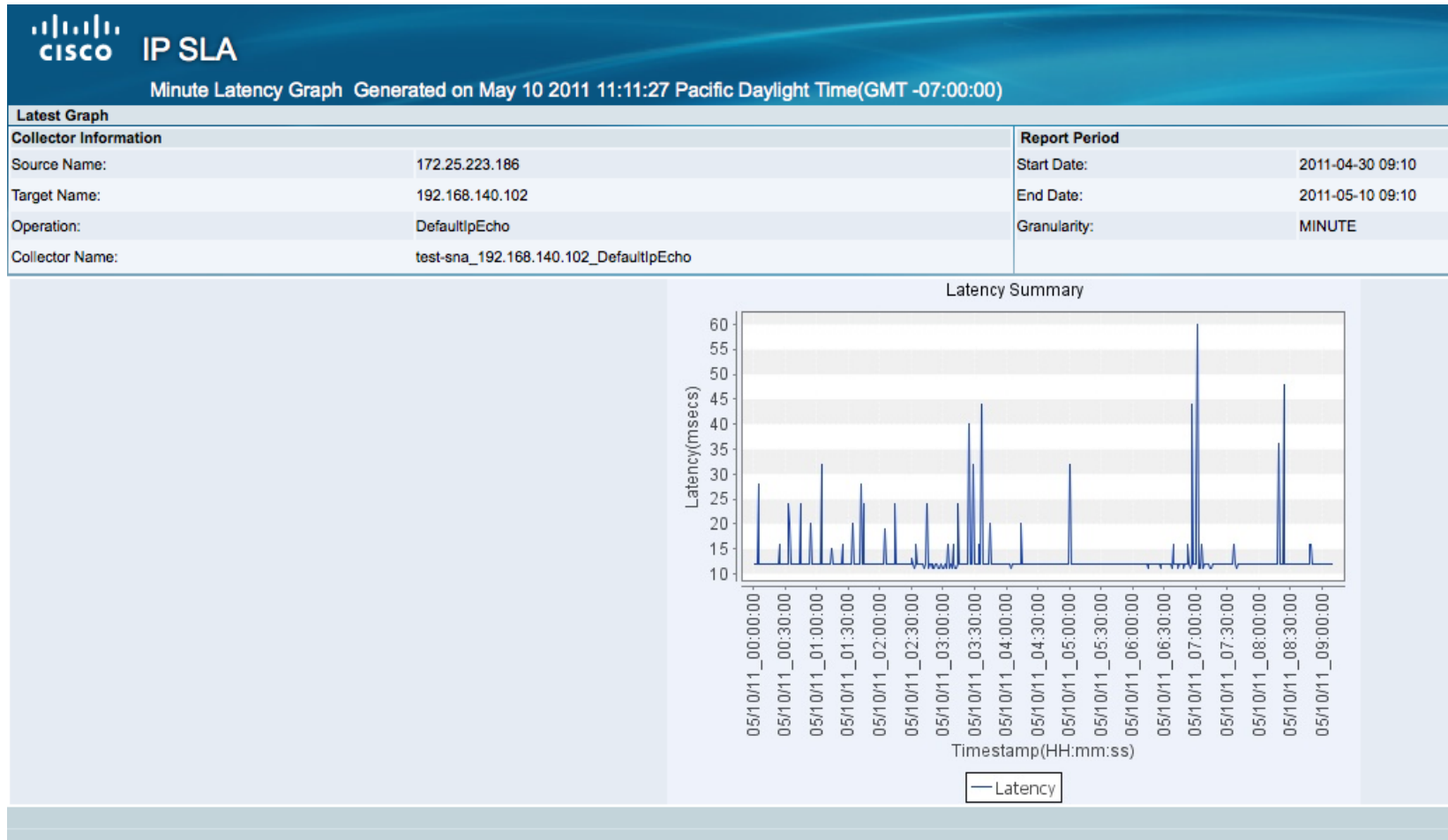
Solution: Automate based on IP SLA, EOT and Embedded Event Manager



See: Available as an EASy Package:

<http://www.cisco.com/go/easy>

IP SLA Support in LMS 4.0



See: www.cisco.com/go/lms

IP SLA Support in Unified Operations Manager 8.0

Create Node-to-Node Test

Test Type:

Source

- CS@cdictmecucms2
- OM@cdictmecucms2

Name:

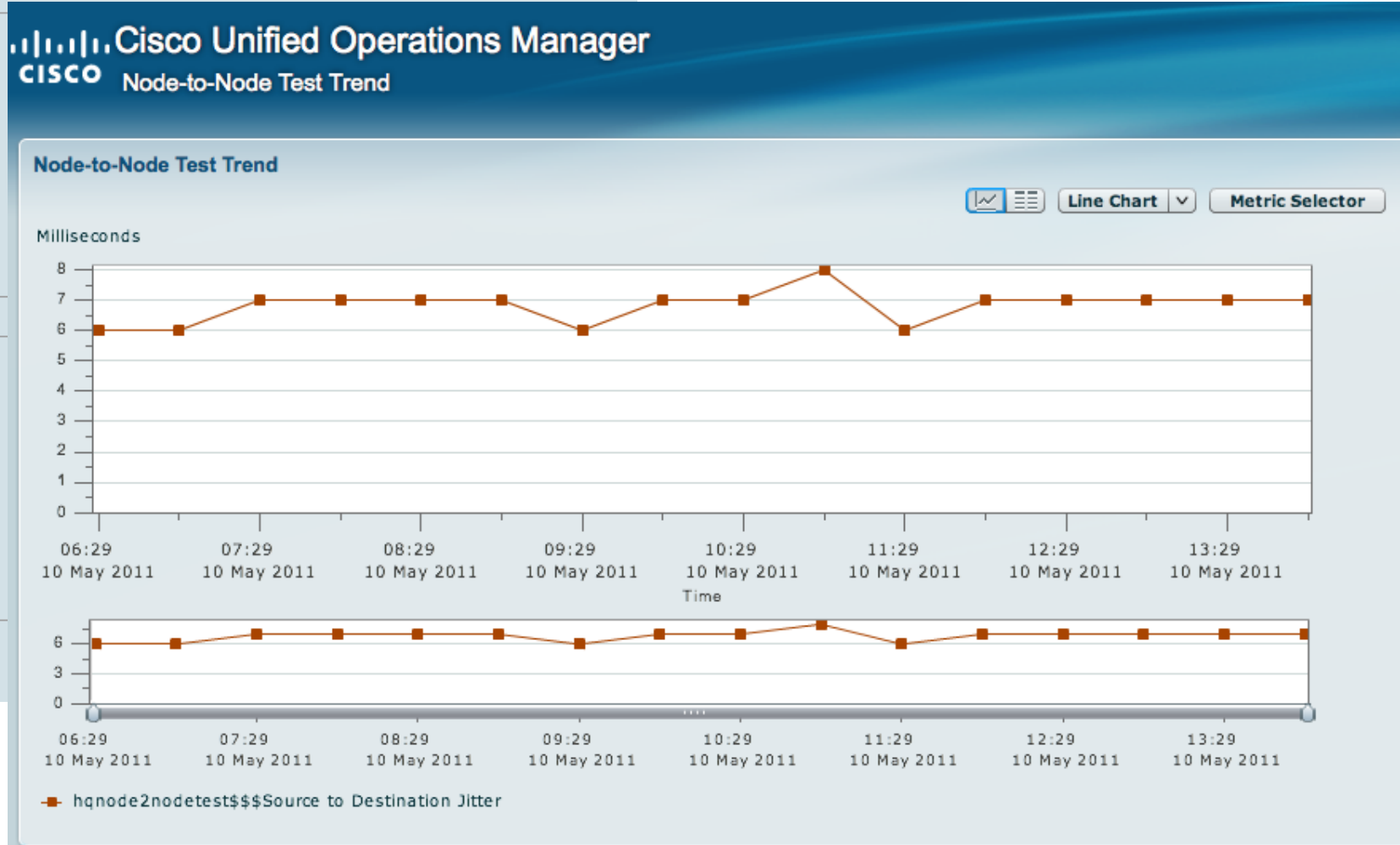
Interface:

Destination

- CS@cdictmecucms2
- OM@cdictmecucms2

Name:

UDP Port:



See: www.cisco.com/go/ucmanagement



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



Who is doing What on the Network

What is NetFlow ?

- § Developed and patented at Cisco® Systems in 1996
- § NetFlow is the defacto standard for acquiring IP operational data
- § Provides network and security monitoring, network planning, traffic analysis, and IP accounting
- § NetFlow v9 (RFC3954) serves as the basis for IETF IPFIX Standard (RFC5101 & RFC5102)

Network World article – NetFlow Adoption on the Rise:

<http://www.networkworld.com/newsletters/nsm/2005/0314nsm1.html>



Flexible NetFlow (FNF)

§ Traditional NetFlow with the v5, v7, or v8 NetFlow export

§ NetFlow Version 9 (RFC3954)

Advantages: **extensibility**

Integrate new technologies/data types quicker
(MPLS, IPv6, BGP next hop, etc.)

Integrate new aggregations quicker

Basis for IETF IPFIX Standard (RFC5101 & RFC5102)

**Exporting
Process**

§ Flexible NetFlow

Advantages: cache and export content **flexibility**

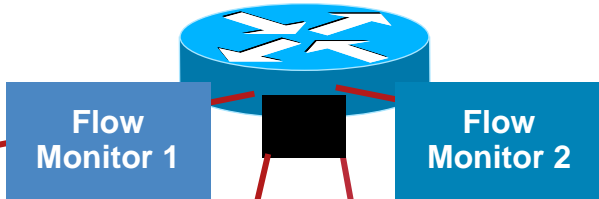
User selection of flow keys

User definition of the records

**Metering
Process**

See: www.cisco.com/go/netflow, www.cisco.com/go/fnf

Flexible NetFlow Multiple Monitors with Unique Key Fields



Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non-Key Fields
Packets
Bytes
Timestamps
Next Hop Address

Key Fields	Packet 1
Source IP	3.3.3.3
Dest IP	2.2.2.2
Input Interface	Ethernet 0
SYN Flag	0

Non-Key Fields
Packets
Timestamps

Traffic Analysis Cache

Source IP	Dest. IP	Source Port	Dest. Port	Protocol	TOS	Input I/F	...	Pkts
3.3.3.3	2.2.2.2	23	22078	6	0	E0	...	1100

Security Analysis Cache

Source IP	Dest. IP	Input I/F	Flag	...	Pkts
3.3.3.3	2.2.2.2	E0	0	...	11000

Flexible NetFlow Configuration – Example

1. Configure the Exporter

```
Router(config)# flow exporter my-exporter  
Router(config-flow-exporter)# destination 1.1.1.1
```

2. Configure the Flow Record

```
Router(config)# flow record my-record  
Router(config-flow-record)# match ipv4 destination address  
Router(config-flow-record)# match ipv4 source address  
Router(config-flow-record)# collect counter bytes
```

3. Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor  
Router(config-flow-monitor)# exporter my-exporter  
Router(config-flow-monitor)# record my-record
```

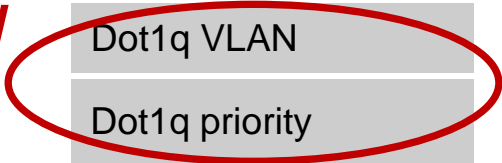
4. Apply to an Interface

```
Router(config)# interface s3/0  
Router(config-if)# ip flow monitor my-monitor input
```

Flexible Flow Record: Key Fields

Flow	IPv4	IPv6
Sampler ID	IP (Source or Destination)	IP (Source or Destination)
Direction	Prefix (Source or Destination)	Prefix (Source or Destination)
Interface	Mask (Source or Destination)	Mask (Source or Destination)
Input	Minimum-Mask (Source or Destination)	Minimum-Mask (Source or Destination)
Output	Protocol	Protocol
Layer 2	Fragmentation Flags	Traffic Class
Source VLAN	Fragmentation Offset	Flow Label
Dest VLAN	Identification	Option Header
Dot1q VLAN	Header Length	Header Length
Dot1q priority	Total Length	Payload Length
Source MAC address		
Destination MAC address		

NEW



Flexible Flow Record: Key Fields

NEW

Routing
src or dest AS
Peer AS
Traffic Index
Forwarding Status
IGP Next Hop
BGP Next Hop
Input VRF Name

Transport
Destination Port
Source Port
ICMP Code
ICMP Type
IGMP Type*
TCP ACK Number
TCP Header Length
TCP Sequence Number
TCP Window-Size
TCP Source Port
TCP Destination Port
TCP Urgent Pointer

TCP Flag: ACK
TCP Flag: CWR
TCP Flag: ECE
TCP Flag: FIN
TCP Flag: PSH
TCP Flag: RST
TCP Flag: SYN
TCP Flag: URG
UDP Message Length
UDP Source Port
UDP Destination Port

Application
Application ID*

Multicast
Replication Factor*
RPF Check Drop*
Is-Multicast

NEW

***: IPv4 Flow only**

Flexible Flow Record: Non-Key Fields

Counters
Bytes
Bytes Long
Bytes Square Sum
Bytes Square Sum Long
Packets
Packets Long

Timestamp
sysUpTime First Packet
sysUpTime First Packet

IPv4
Total Length Minimum (*)
Total Length Maximum (*)
TTL Minimum
TTL Maximum

IPv4 and IPv6
Total Length Minimum (**)
Total Length Maximum (**)

§ Plus any of the potential “key” fields: will be the value from the first packet in the flow

(*) IPV4_TOTAL_LEN_MIN, IPV4_TOTAL_LEN_MAX
(**) IP_LENGTH_TOTAL_MIN, IP_LENGTH_TOTAL_MAX

Service Planning

Flexible NetFlow Top Talkers - Examples

§ Top ten IP addresses that are sending the most packets

```
Router# show flow monitor <monitor> cache
      aggregate ipv4 source address
      sort highest counter bytes top 10
```

§ Top five destination addresses to which we're routing most traffic from the 10.10.10.0/24 prefix

```
Router# show flow monitor <monitor> cache
      filter ipv4 destination address 10.10.10.0/24
      aggregate ipv4 destination address
      sort highest counter bytes top 5
```

§ 5 VLAN's that we're sending the least bytes to:

```
Router# show flow monitor <monitor> cache
      aggregate datalink dot1q vlan output
      sort lowest counter bytes top 5
```

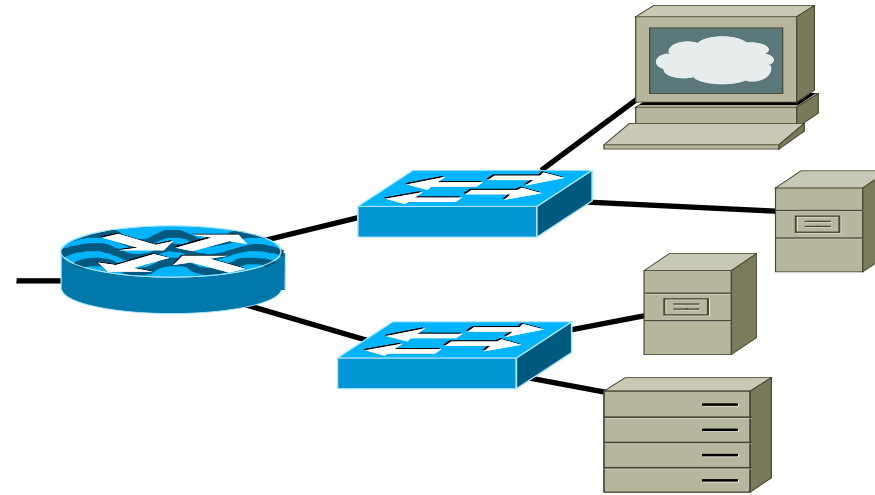
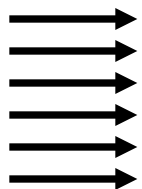
§ Top 20 sources of 1-packet flows:

```
Router# show flow monitor <monitor> cache
      filter counter packet 1
      aggregate ipv4 source address
      sort highest flow packet top 20
```

Service Planning

Flexible NetFlow Top Talkers – Example

TCP
SYN
attacks



**Servers' network
10.10.10.0/24**

```
Router# show flow monitor <monitor> cache
      filter ipv4 destination address 10.10.10.0/24
            counter packet regex[1-2]
      aggregate ipv4 source address
                ipv4 destination address
      sort highest flow top 100
```

§ The top 100 pairs of IP addresses with one or two packet(s) that are destined for my servers' network

Example: Monitor low-TTL Traffic

Problem: We want to know about low-TTL traffic

Solution: Use Flexible Netflow and Embedded Event Manager 3.0 to detect traffic flows with TTL < 5

1. Configure flexible Netflow to match on TTL, Source- and Destination Address

```
flow record my-ttl-record
  match ipv4 ttl
  match ipv4 source address
  match ipv4 destination address
:
flow monitor my-ttl-monitor
  record my-record
:
```

- Top (unexpected) Talkers with low-TTL traffic ?
- Deviation from Normal ?
- Senders with many low-TTL flows ?
- Take Actions (block suspicious senders) ?

2. Configure the Netflow Event Detector in EEM to notify upon a new flow record

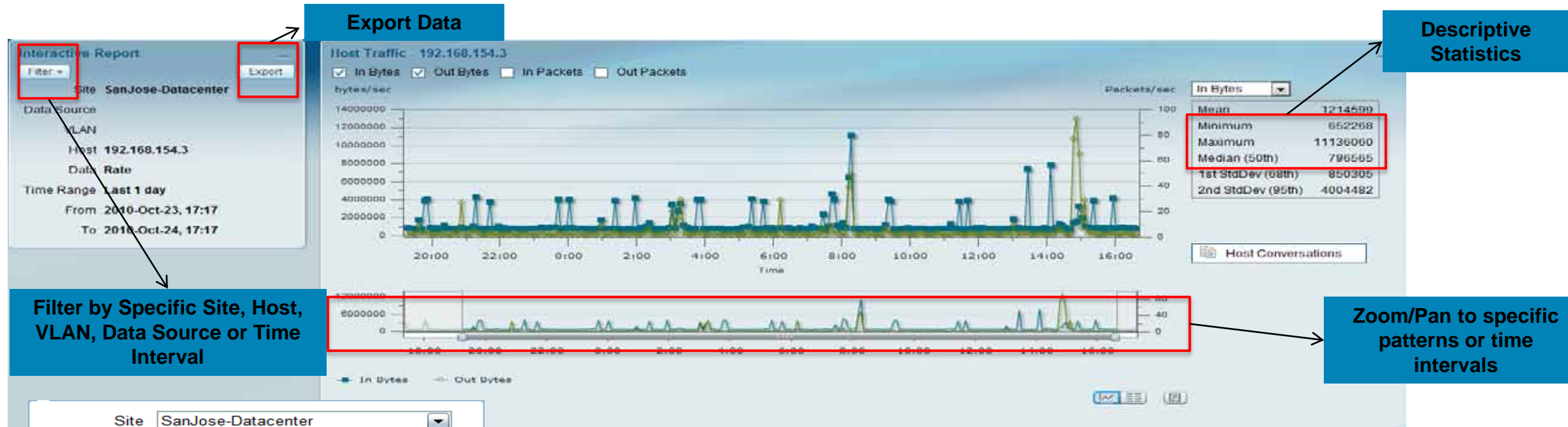
```
event manager applet my-ttl-applet
  event nf monitor-name my-ttl-monitor event-type create event1
  entry-value "5" field ipv4 ttl entry-op lt
  action 1.0 syslog msg "Low-TTL flow from $_nf_source_address"
```

3. Syslog message and/or use show flow monitor my-ttl-monitor cache command

```
*Dec 2 17:39:31.221: %HA_EM-6-LOG: my-ttl-applet: Low-TTL flow from 192.168.2.248
```

NAM 5.0 Interactive Reports

Analyze Performance/Usage Trends and Patterns



- Analyze data over last month or more
- Define custom time interval for analysis
- Export data in raw format for consumption by external management application
- Drill-down to analyze related trends to support planning decisions

Site: SanJose-Datacenter

Data Source: [Dropdown]

VLAN: [Input]

* Host: 192.168.154.3

* Data: Rate (per second) Cumulative

* Time Range: Last 1 day

From: Last 5 minutes
Last 15 minutes

To: Last 1 hour
Last 4 hours
Last 8 hours
Last 1 day
Last 1 week
Last 1 month
Custom

Filter Name: [Input]

See: www.cisco.com/go/nam



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



What if I need a Packet Capture?

Embedded Packet Capture (EPC)

Problem: Sometimes a Packet Capture would be useful for Troubleshooting, Security or Application Analysis, Baselineing, etc.

BUT: deploying Packet Sniffers are **slow, expensive** and **require local skills** and **equipment** ...

Solution: Make use of IOS Embedded Packet Capture to capture PCAP format data and/or analyze on the device

1. Defining a capture buffer on the device

```
Router# monitor capture buffer ...
```

2. Defining a capture point

```
Router# monitor capture point ...
```

3. Associate capture point to buffer

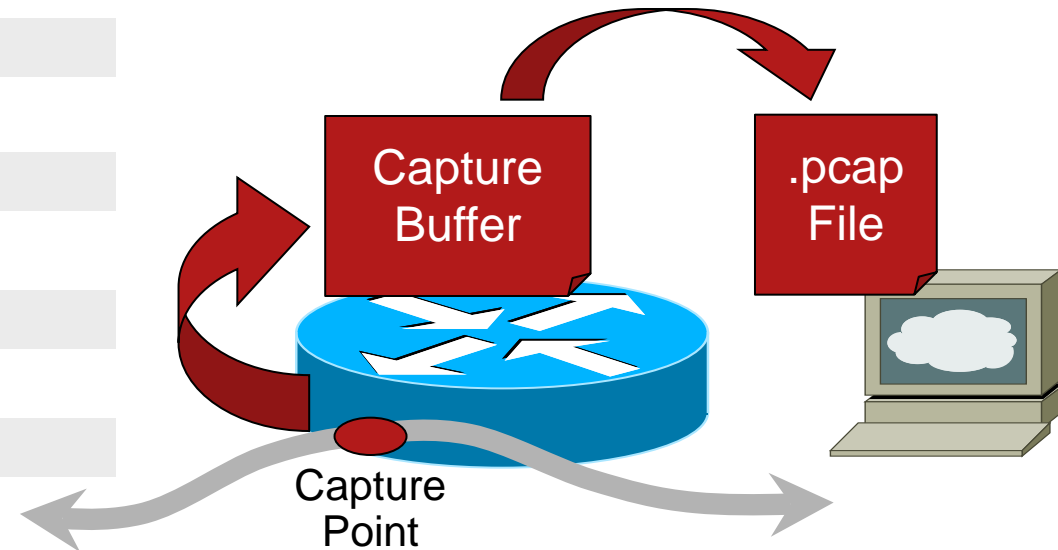
```
Router# monitor capture point associate ...
```

4. Start / Stop capture points

```
Router# monitor capture point start ...
```

5. Show and/or Export the content of the buffer

```
Router# monitor capture buffer <tracename> export
```



See: <http://www.cisco.com/go/epc>

Available from: IOS 12.4(20)T

Platforms: 8xx, 18xx, 28xx, 38xx ISRs, 72xx

Example: Analyze process-switched traffic

We want to capture process-switched traffic:

1-3. Define a capture buffer, capture point and associate the two

```
Router# monitor capture buffer my-buffer size 100 max-size 1000 circular
Router# monitor capture point ip process-switched my-capture in
Router# monitor capture point associate my-capture my-buffer
```

4. Start capturing traffic

```
Router# monitor capture point start all
*Nov 25 10:00:58.990: %BUFCAP-6-ENABLE: Capture Point my-capture enabled.
```

5. Show / Analyze on the router ...

```
Router# show monitor capture buffer all parameters
Capture buffer my-buffer (circular buffer)
Buffer Size : 102400 bytes, Max Element Size : 1000 bytes, Packets : 28
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : my-capture, Status : Active
Configuration:
monitor capture buffer my-buffer size 100 max-size 1000 circular
monitor capture point associate my-capture my-buffer
```

We have some traffic

```
Router# show monitor capture buffer my-buffer dump
10:14:05.914 UTC Nov 25 2008 : IPv4 Process      : Fa0/0 None
66A3C5B0:          FFFFFFFF FFFF0001 64FF4C01      .....d.L.
66A3C5C0: 080045C0 00300000 00000111 0B5AACAA1  ..E@.0.....Z,!
66A3C5D0: 0103FFFF FFFF02C7 02C7001C 85F60001  ....G.G...v..
66A3C5E0: 0010AC12 01020000 5D4C0F03 0004AC12  ..,.....]L.....
```

Off-line Analysis

5. ... or export as PCAP file and analyze externally

```
Router# monitor capture buffer my-buffer export tftp://10.10.10.10/my pcap
```

The screenshot shows the Wireshark interface with a packet capture of an SNMP GET-NEXT request. The packet list pane shows several packets, with packet 32 selected. The packet details pane shows the structure of the packet, including the Internet Protocol, User Datagram Protocol, and Simple Network Management Protocol (SNMP) fields. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
23	4.920000	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
24	4.920000	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
25	5.620003	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
26	5.620003	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
27	5.620003	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
28	5.620003	10.10.10.66	10.10.10.255	NBNS	Name query NB DOMAINSERVER <00>
29	8.576003	10.48.74.215	255.255.255.255	TFTP	TFTP Read Request
30	10.784001	172.20.250.254	10.48.75.2	TELNET	Telnet Data ...
31	12.576003	10.48.74.215	255.255.255.255	TFTP	TFTP Read Request
32	13.688002	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
33	13.708002	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
34	13.732002	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
35	13.752002	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
36	13.776001	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
37	13.796001	144.254.10.207	10.48.75.2	SNMP	GET-NEXT
38	13.820001	144.254.10.207	10.48.75.2	SNMP	GET-NEXT

Frame 32 (74 on wire, 74 captured)
Raw packet data
Internet Protocol, Src Addr: 144.254.10.207 (144.254.10.207), Dst Addr: 10.48.75.2 (10.48.75.2)
User Datagram Protocol, Src Port: 35645 (35645), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 1
Community: public
PDU type: GET-NEXT
Request Id: 0x1bab0690
Error Status: NO ERROR
Error Index: 0
Object identifier 1: 1.3.6.1.4.1.9.9.244.1.8
value: NULL

```
0000  45 00 00 4a 46 f5 40 00 fa 11 48 ae 90 fe 0a cf  E..JF.@. ..H.....
0010  0a 30 4b 02 8b 3d 00 a1 00 36 dd 55 30 2c 02 01  .OK... ..6.U0,..
0020  00 04 06 70 75 62 6c 69 63 a1 1f 02 04 1b ab 06  ...publi c.....
```

EPC – Additional Considerations

§ Capture stop criteria:

- manual stop
- after a specified time interval
- after given number of packets

§ Capture point:

- IPv4 or IPv6
- CEF (drop, punt) or process switching
- interface specific or all interfaces
- Direction: in, out, both, from-us (process-switched specific)
- multicast: only ingress packets are captured, not the replicated egress packets
- MPLS: does not capture MPLS encapsulated frames today

§ Buffer can be defined as linear or circular

§ Buffer filter based on an access-list

```
Router# monitor capture buffer my-buffer filter access-list 10
```

§ Buffer export options: FTP, HTTP, HTTPS, RCP, SCP, or TFTP

Note: exec mode commands only, nothing in the configuration



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



What if I need a Packet Capture? II

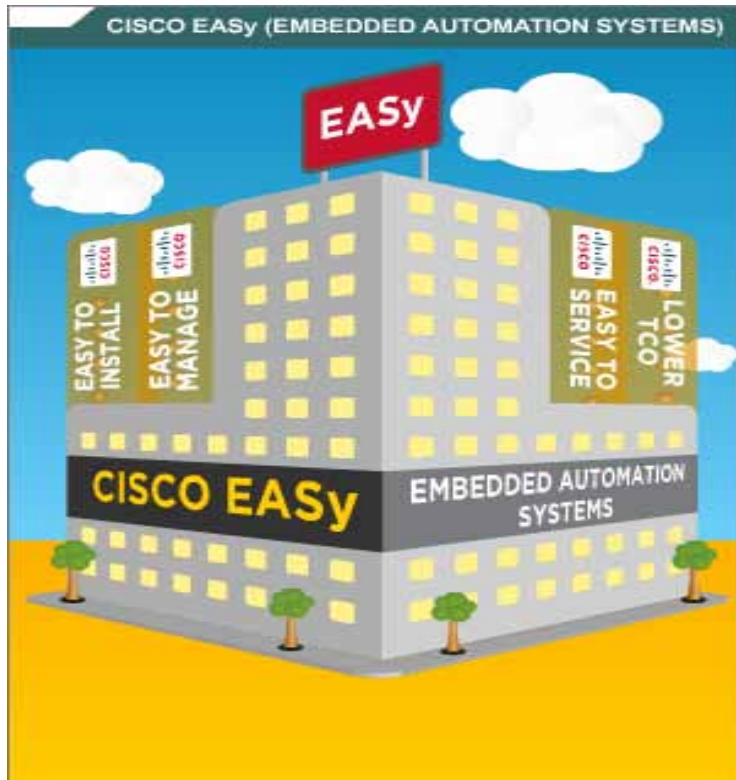
Diagnosing Transient Problems

Problem: you are seeing VPN tunnel drops on your VPN head-end router at 3:00 am every day. The tunnels continue to flap until the physical interface is reset. You want to analyze the traffic on the wire at that time.



3:00 AM

EPC – EASy Package



Embedded Automation Systems (EASy)

EPC EASy Package Supports:

- § Interactive Installation
- § Timed or manual capture start
- § Linear or circular buffer
- § Buffer Export

To use the Package:

1. Browse and Download EPC EASy Package
www.cisco.com/go/easy
2. Make Sure to also download EASy Installer
3. Watch VOD and/or read documentation
www.cisco.com/go/easy
4. Customize and tailor to your needs
5. Install and Use



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



What if I need a Packet Capture? III

NAM 5.0: Smart Capture Analysis

Highlights observed anomalies in packet traces

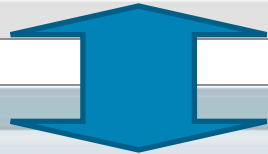
The screenshot shows the NAM Traffic Analyzer - Packet Decoder interface. At the top, it displays 'Capture Session ID: 0' and 'Packets: 13594-14593 of 40178'. Below this is a table of captured packets. Packet 13594 is highlighted, and its details are shown in a pane below the table. The details include: Ethernet II, VLAN 002.1Q Virtual LAN, IP (128.107.191.112 to 192.168.153.131), UDP (5654 to 6004), and T38 (ITU-T Recommendation T.38). A 'MALFOR' (Malformed Packet: T.38) error is reported, along with 'EXPERT' messages indicating an exception occurred. The packet data is shown in hexadecimal and ASCII format.

Pkt	Time (s)	Size	Source	Destination	Protocol	Info
13594	0.000	68	128.107.191.112	192.168.153.131	T.38	UDP: UDPTL Packet Seq=44372, data: unknown
13595	0.000	68	128.107.191.112	192.168.153.131	T.38	UDP: UDPTL Packet Seq=44372, data: unknown
13596	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13597	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13598	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13599	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13600	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13601	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13602	0.000	222	2.2.2.20	1.1.1.20	UDP	Source port: 1609 Destination port: 3275
13603	0.000	222	2.2.2.20	1.1.1.20	UDP	Source port: 1609 Destination port: 3275

Packet Number: 13594 - Arrival Time: Oct 20, 2010 11:48:26.000391000 - Frame Length: 68 bytes - Capture Length: 68 bytes

- + ETH Ethernet II, Src: 00:18:73:b5:7a:3f (00:18:73:b5:7a:3f), Dst: 00:11:5d:03:b8:00 (00:11:5d:03:b8:00)
- + VLAN 002.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 32
- + IP Internet Protocol, Src: 128.107.191.112 (128.107.191.112), Dst: 192.168.153.131 (192.168.153.131)
- + UDP User Datagram Protocol, Src Port: 5654 (5654), Dst Port: 6004 (6004)
- + T38 ITU-T Recommendation T.38
- + MALFOR [Malformed Packet: T.38]
- EXPERT [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
- EXPERT [Message: Malformed Packet (Exception occurred)]
- EXPERT [Severity level: Error]
- EXPERT [Group: Malformed]

0000 00 11 5d 03 b8 00 00 18 73 b5 7a 3f 81 00 00 20 ..1.....s.s?...
0010 08 00 45 00 00 24 70 d2 00 00 77 11 39 e1 00 6b ..E..\$p...w.0..k
0020 bf 70 e0 a8 99 83 16 16 17 74 00 10 06 e6 ad 54 ..p.....t.....T
0030 9b 02 75 6c 73 32 00 00 00 00 00 00 00 00 00 ..u1s2.....



Expert info

Filter

Packet Id	Protocol	Severity	Group	Description
13594	eth:vlan.ip:udp.t38	Error	Malformed	Malformed Packet (Exception occurred)
13595	eth:vlan.ip:udp.t38	Error	Malformed	Malformed Packet (Exception occurred)

NAM enables:

- § Packet trace analysis highlighting observed protocol/packet level anomalies
- § One-click targeted packet captures
- § Combined application visibility, traffic analysis and smart packet capture analysis

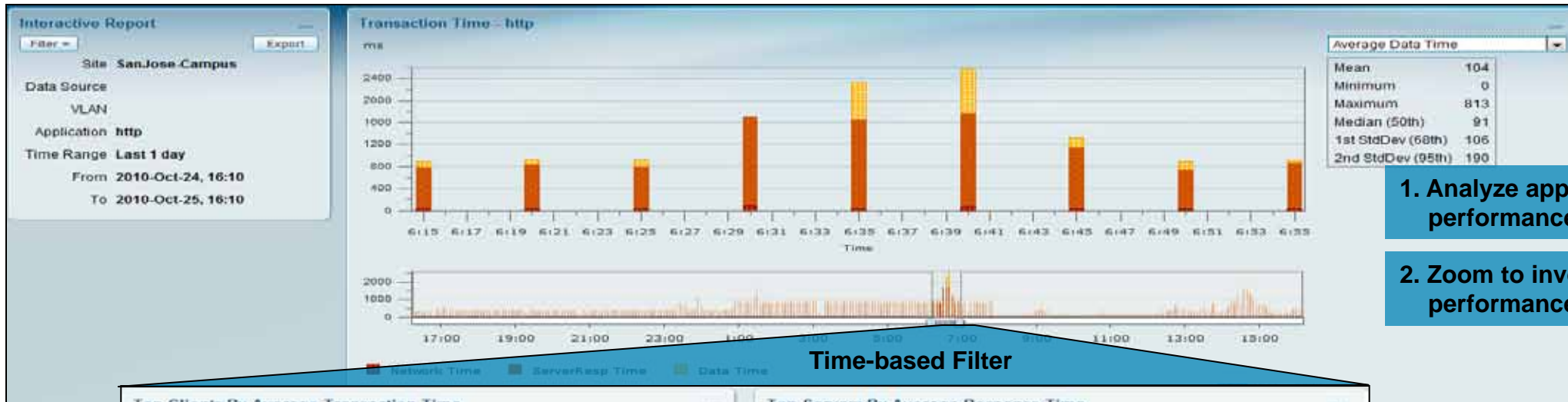
NAM benefits:

- § Improves operational efficiency with on-demand captures
- § Smart analysis pinpoints root-cause much faster than manually analyzing or scanning the packet traces

See: www.cisco.com/go/nam

NAM 5.0: Troubleshooting Workflow

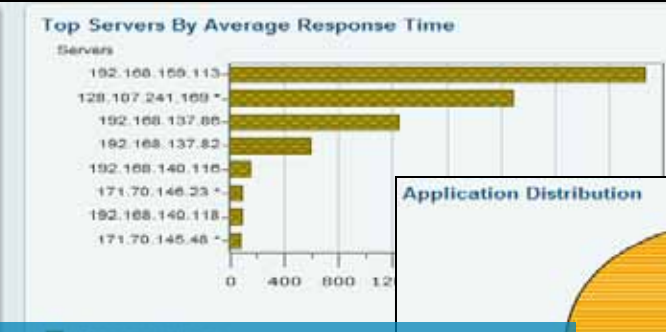
Isolate Source of Application Performance Degradation



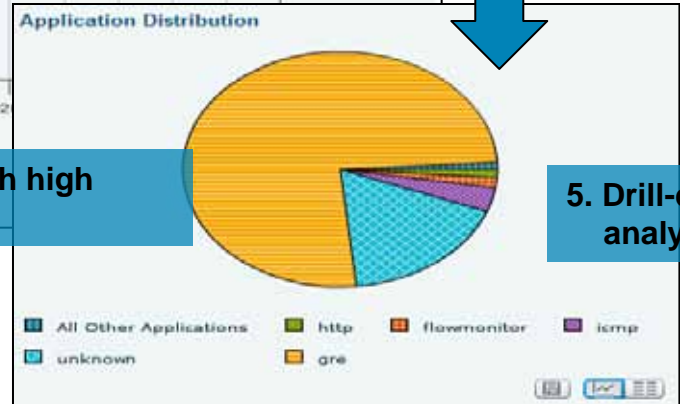
- 1. Analyze application performance over time
- 2. Zoom to investigate specific performance issues



- 3. Identify the Top N clients affected by the degradation



- 4. Isolate the servers with high response time



- 5. Drill-down to select server to analyze activity

NAM 5.0: WAN Optimization Analysis

Monitor Client Experience and Optimization Improvements

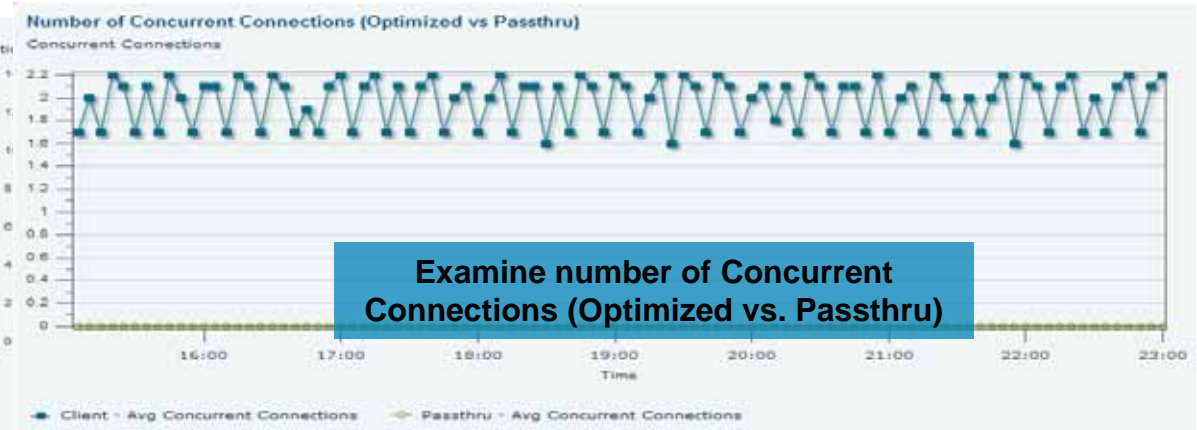


Select Branch Site, Server Site/Server, Application, and Reporting Interval

Analyze performance application traffic (Optimized vs. Passthru)



Examine Traffic Volume (Client, WAN) and achieved Compression Ratio



Examine number of Concurrent Connections (Optimized vs. Passthru)



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.



Summary

You have many tools at your disposal!

- § The embedded instrumentation in Cisco devices is an invaluable partner in helping to monitor and troubleshoot the network
- § Features such as SNMP, NetFlow, IP-SLA and EPC provide many valuable monitoring and troubleshooting capabilities
- § Combining these features with EEM unleashes the power of network automation
- § There are many online resources such as EASy and CiscoBeyond to help you get started

- § And, ... Cisco NMS products such as LMS, NAM and Unified Operations Manager bring these instrumentation features to life

References – Instrumentation

Device Manageability Instrumentation (DMI) www.cisco.com/go/instrumentation

- § Embedded Event Manager (EEM): www.cisco.com/go/eem
- § Embedded Packet Capture (EPC): www.cisco.com/go/epc
- § Flexible NetFlow: www.cisco.com/go/netflow and www.cisco.com/go/fnf
- § IPSLA (formerly SAA, formerly RTR): www.cisco.com/go/ipsla
- § Network Analysis Module: <http://www.cisco.com/go/nam>
- § CiscoWorks LAN Management Solution: <http://www.cisco.com/go/lms>
- § Unified Operations Manager: <http://www.cisco.com/go/ucmanagement>

- § **Feature Navigator:** www.cisco.com/go/fn
- § **MIB Locator:** www.cisco.com/go/mibs

Help is just a click away ...

www.cisco.com/go/easy

Cisco Embedded Automation Systems - Customized Solutions Downloads

Highly efficient Cisco embedded automation technologies reduce:

- Embedded Event Manager (IEM)
- Cisco IP Service Level Agreements (SLAs)
- Expressway Web
- Network-Based Admission (Registration)
- Packet Tracer
- Embedded (Event) Tracing
- Cisco IOS IPv6 (IPv6)

These solutions are based on Cisco routers and switches. Besides these powerful technologies, these Cisco services feature and associated products for providing customized solutions in all environments integrated into the operational environment.

The following solutions use these powerful technologies. They can be used as-is or further customized to address additional challenges. All the solutions require the Cisco Embedded Automation Systems software.

Package Name	Description	Downloads
Cisco Embedded Automation System (IEM)	Related to IEM a Toolset designed to run within the Cisco IOS with associated Cisco IOS software to help Embedded Automation System packages using a common, data-driven interface. Includes a sample configuration.	Download Package (101 - 14 KB) Download Documentation (PDF - 452 KB)
Embedded Packet Capture	Helps with the configuration and capture of packet data using Embedded Packet Capture.	Download Package (101 - 14 KB) Download Documentation (PDF - 452 KB)
IP Service Level Agreements	Toolset generates an event when a SLA failure occurs.	Download Package (101 - 14 KB)

www.cisco.com/go/ciscobeyond

Browse Scripts

Script Title	Summary	Category	Date Published	Rating
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	User Interface	Nov 09, 2009 10:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Network Management	Nov 09, 2009 11:45 AM PST	4 stars
Script Title: [Link]	Sample script to capture data on link	High Availability	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Security	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Security	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Network Management	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	User Interface	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Network Management	Nov 09, 2009 11:45 AM PST	5 stars
Script Title: [Link]	Sample configuration for IPv6 using IEM and IPv6 IPv6	Routing	Nov 09, 2009 11:45 AM PST	5 stars

Management Instrumentation

Cisco IOS Software provides a rich set of features that enable customers to efficiently manage their networks. Benefits of this embedded instrumentation functionality include: lowered operating and maintenance costs, rapid configuration of new network services and devices, management of the network as an integrated system, reduced downtime by proactive fault management, and measurable and visible differentiated services.

Product Literature

- Cisco Embedded Automation Systems
- Cisco Enhanced Device Interface
- Cisco Generic Online Diagnostics (GOLD)
- Cisco IOS Diagnostic Tools for Commercial
- Cisco IOS Embedded Event Manager (IEM)
- Cisco IOS Embedded Packet Capture
- Cisco IOS IP Service Level Agreements (SLAs)
- Cisco IOS NetFlow
- Cisco IOS Service Diagnostics

Technical Support and Documentation

Review additional information about **Management Instrumentation** in the Technical Support site area.

- Download Software
- Latest Cisco IOS Management Instrumentation Documentation
- Cisco IOS Service Diagnostics - Bandwidth Management Protocol (BMP)
- Portlet Path, First and Only of Service Diagnostics Users Guide
- Cisco IOS Embedded Event Manager Data Sheet
- Cisco IOS Flexible NetFlow Technology (FNF)
- Cisco IOS Flexible NetFlow Dashboard
- Cisco IOS Embedded Packet Capture Dashboard
- Cisco IOS Flexible NetFlow Technology White Paper

www.cisco.com/go/instrumentation

Cisco Support Community

Search the Support Community

Cisco Support Home | Top Rated | Ask the Experts | Product Reviews

Support Communities

- Network Infrastructure
- IP Addressing
- Network Management
- Network Security
- Network Troubleshooting
- Other Network Infrastructure Subsites

What Do You Think?

Network Infrastructure

- IP Addressing
- Network Management
- Network Security
- Network Troubleshooting
- Other Network Infrastructure Subsites

supportforums.cisco.com

See NMS Product Demos at the NMS Booth

Cisco Prime – A Strategy for Innovative Management

§ LAN Management Solution (LMS)

Simplified management of borderless networks

§ Network Analysis Module (NAM)

Consistent performance visibility across borderless networks

§ Collaboration Manager

Manage and troubleshoot video collaboration services

§ Network Control System

Converged wired/wireless access management



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.



Q & A

#CNSF2011



Cisco
Networkers 2011
May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



For conference presentations visit:

www.networkerssolutionsforum.com

Please take a moment to complete the
Networkers Conference Event Evaluation Form

Thank you.

