All You Ever Wanted to Know About Network Management in 90 Minutes

(More or Less)

Cisco University

Adopted from Cisco Networkers 2006

Chesapeake NETCRAFTSMEN

About the Speaker

- **Dr. Pete Welcher**
  - **Cisco CCIE #1773, CCSI #94014, CCIP**
  - **Specialties: Network Design, QoS, MPLS, Wireless, Large-Scale Routing & Switching, High Availability, Management of Networks**
  - **Customers include large enterprises, federal agencies, hospitals, universities, major hotel chain**
  - **MPLS w/ major city government optical + MPLS deployment**
  - **Several large MPLS VPN customers**
  - **MPLS VPN Security Risk Analysis for major retailer (1700+ stores)**
  - **Taught many of the Cisco router/switch courses**
  - **Reviewer for many Cisco Press books, book proposals**
  - **Presented (lab sessions) MPLS VPN at Networkers 2005, 2006**
- **Over 138 articles at http://www.netcraftsmen.net/welcher/**

Agenda

- Managing Network Management
- Managing via the Cisco IOS
- Syslog
- IP SLA
- NetFlow
- NBAR
- Net Mgmt Stories (as time permits)
- Summary, Q&A, References, Applause-O-Meter (if time)

Managing Network Management

Pete's Stages of Network Management

1. Gathering information to diagnose a problem (CLI, etc.)
2. Collecting SNMP trap & syslog information to assist
3. Automating configuration and IOS software management
4. Automated performance data gathering, reporting (baseline, capacity planning)
5. Performance threshold-based traps



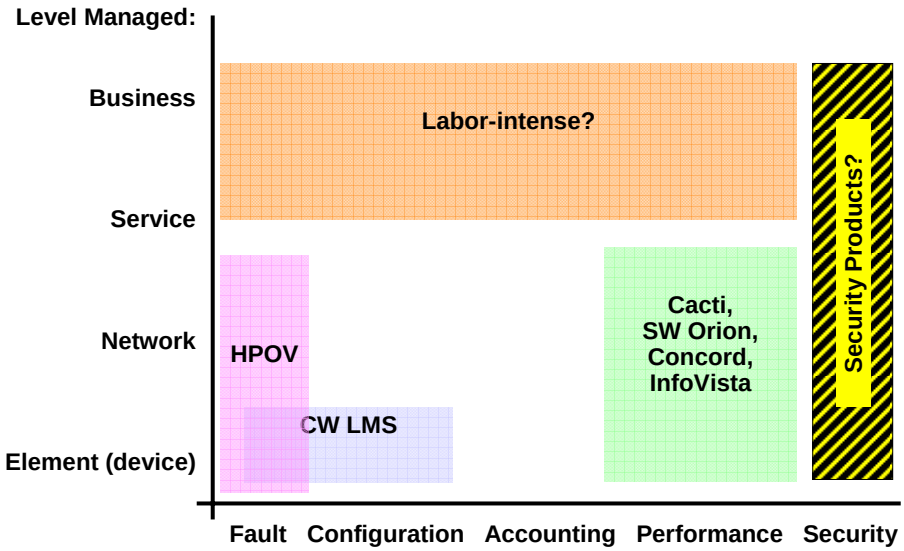
Plan Network Management

- Plan what you buy, and don't buy several products at one time
- Try the product before buying
  - –Demos always look great, but generally don't show what the product doesn't do well, or what is hard to admin
  - –Take the class: if it doesn't work in class…
  - –Demo it in-house: if you can't make it work…
- Consider a consultant
  - –Broader exposure to NM products, what people like and don't like, what seems to work…
- Focus: What problem are you trying to solve?

Determine Management Priorities

- You can't do it all, especially in small-medium size organizations
- Network Management can get labor intense
  - –But staffing rarely gets larger
- Newton was right about INERTIA
  - –Existing process may focus on managing WAN links
  - –But data center, colo facility, etc. also need to be watched
  - –Services and response times, WAN SLA's, etc. also candidates for monitoring

2-Dimensional FCAPS



The New Age in Net Mgmt Tools

- 20 years ago, disks were costly
  - –Not any more, 1 TB USB drive for <$1K soon
- 10 years ago, CPU and bandwidth were costly
  - –Getting very cheap now, e.g. Intel Dual and Quad core processors
- Impact on Net Management:
  - –Smaller scale products are scaling further and further!
  - –Older products were (are) stingy with resources, like polling for data (uses CPU and bandwidth) and storing data (uses disk space)
  - –Recent products figure out “it’s a router” or “it’s a switch” and go collect a lot of useful info
  - –For years, I’ve disliked turning on polling one router or interface or <whatever>, ONE at a time – now we don’t have to!
  - –Do you really want to be reading MIBs and figuring out what variables would be useful to collect? The software should already know the important variables!
- The secret of test-driving a tool
  - –Look for what the vendor made hard to do (intentionally or unintentionally)
  - –Decide if you can live with it

Use “Sustainable” Tools

- Most organizations have had a lot of NM shelfware over time
  - –May explain current disinterest in (platform) products
- Base your tool selection on ease of product admin and size of your organization
  - –One person shop: Keep It Simple! (1-2 products)
  - –With the right mix of tools and a dedicated / good admin, you can get good value from several tools
  - –Net mgmt tool admin MUST be a tool user, not just a sys admin
- New generation of low admin hassle tools:

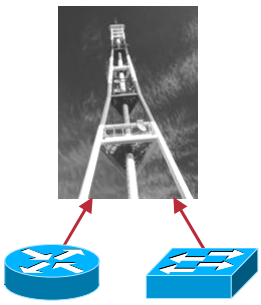
What’s Up Gold (displacing HP OV NNM?)	Cacti
Cisco NAM	NetMRI
SolarWinds Orion	Cisco SDM, ASDM, CSM
NetQoS products	

Managing via the Cisco IOS

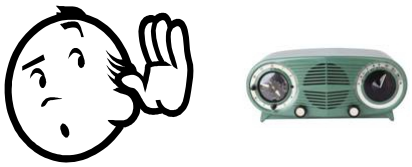
Cisco IOS Tools Help You Manage

- **Companies sometimes buy cheaper equipment, particularly access switches**
  - **This is a TCO issue!!**
  - **When something goes wrong, it can be CCIE-hard to figure out the problem and cause, if the device gives you no info or just RMON data**
- **Cisco IOS provides**
  - **Broad range of show commands**
  - **Show logging to see locally-retained syslog info after an event**
  - **Out of band management (reverse telnet / reverse SSH)**
  - **IP SLA and related show commands**
  - **NetFlow and related show commands**
  - **NBAR**
  - **ESM for "smart syslog" in 12.3 T and later**
  - **SNMP access to vast amounts of information**
  - **SDM, ASDM, web tools for managing single devices**
  - **CBQoS MIB (and many other SNMP MIBs are supported too!)**

Communicating with the Network



Managed Network Elements Are Waiting to Provide Us with Useful Information



Network Management Begins with an Understanding of How to Collect and Interpret This Information

Methods of Gathering Information

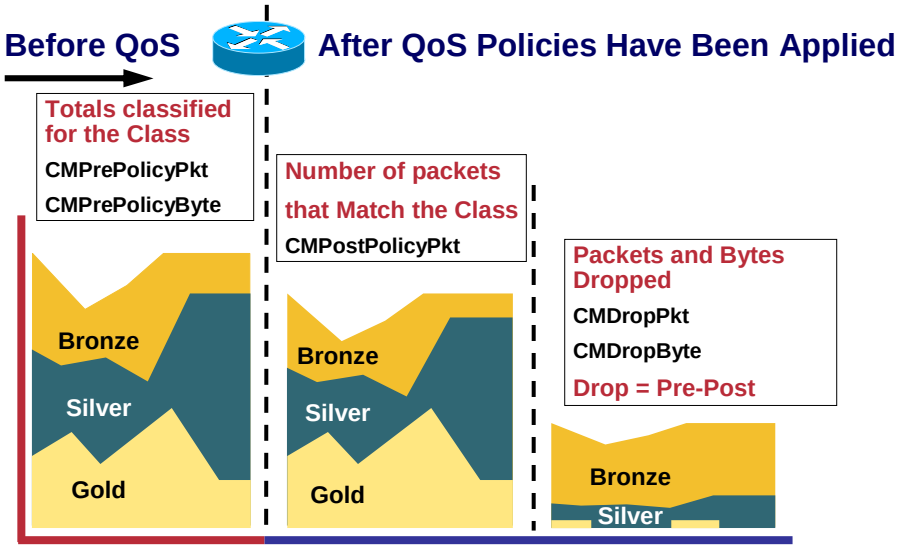
	Example	Security Options
Console	Terminal Server	Device Usernames TACACS/RADIUS
Telnet	TeraTerm, Putty	SSH
HTTP	Embedded Device Management (XML)	SSL (HTTPS)
SNMP	MRTG Multi Router Traffic Grapher	SNMPv1, 2c—Access Lists SNMPv3—Auth/Priv

Cacti updates MRTG

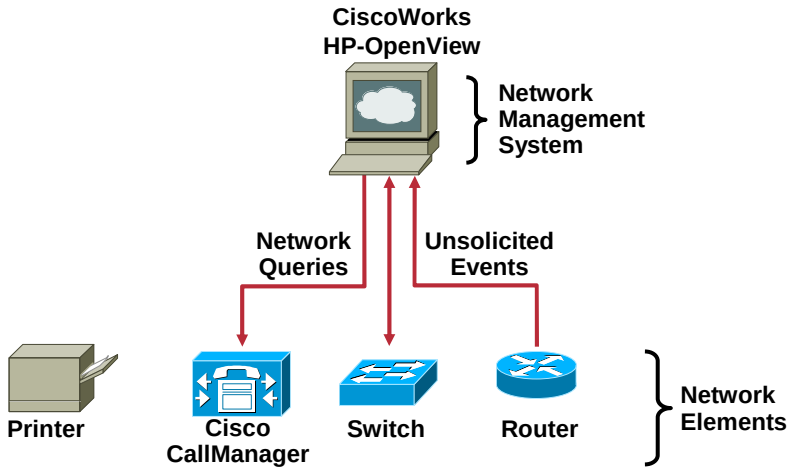
Methods of Communication (Event Driven)

Example	Function
Syslog	Operation Changes Change audit
Netflow	Usage Flow reporting Accounting
Embedded Event Manager	Scriptable Event Driven Reporting
SNMP Traps	Event Driven or Threshold Driven

CISCO-CLASS-BASED-QOS MIB
Class-Map Stats Table (cbQosCMstats)



Two-Tier Management Communication



Network Management Tips

- **Configure for manageability (and security)**
  - **One of my articles contains a sample manageability configuration template**
  - **http://www.netcraftsmen.net/welcher/papers/snmptemplate.html**

Syslog

Syslog

- **Very basic reporting mechanism, “standard” (esp. on UNIX)**
- **Text messages on UDP port 540**
- **Easy to implement clients**
- **All ASCII (easy to manipulate)**
- **Think of it as a Flight Recorder: maximize the STP and other info captured when you have a problem**

```
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83450 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83451 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83452 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83453 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83454 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83455 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83456 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83457 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83458 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83459 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83460 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83461 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
2005-07-07 08:32:23  Local7.Info  KiwiPIX(Inside)  %PIX-6-302015: 83462 Built outbound UDP connection 0 for outside:17.82.254.11(bm1.asia.apple
```

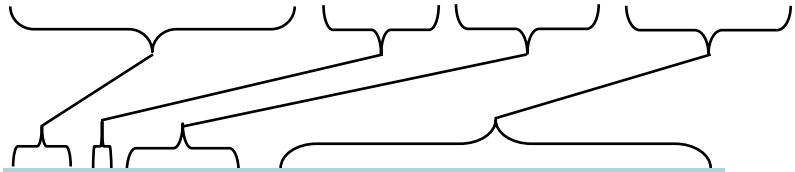
Syslog Problems

- It's not reliable (yet)
- It's not secure (yet)
  - –Not much worse than SNMPv1/v2c notifications
- One way: no query capability
- Priority isn't consistently used
  - –Fairly accurate on Cisco routers, PIX maybe not
- Can be verbose
  - –No argument there! Especially security devices!!!
- Tools: Syslog-NG, Kiwi Syslog, freeware…

For New Smart Ways to Process Syslogs on Device, See NMS-3011: Getting the Right Events from Network Elements

There Is a Cisco IOS Message Standard for Syslog

%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text



```
%SYS-5-CONFIG_I: Configured from console by
cwr2000 on vty0 (192.168.64.25)
```

- Documentation for each release explains the meaning of many of these events
- Severity maps to Syslog level—i.e., how critical of a message it is
- Facility here is not the same as Syslog facility; e.g., local7

IP SLA

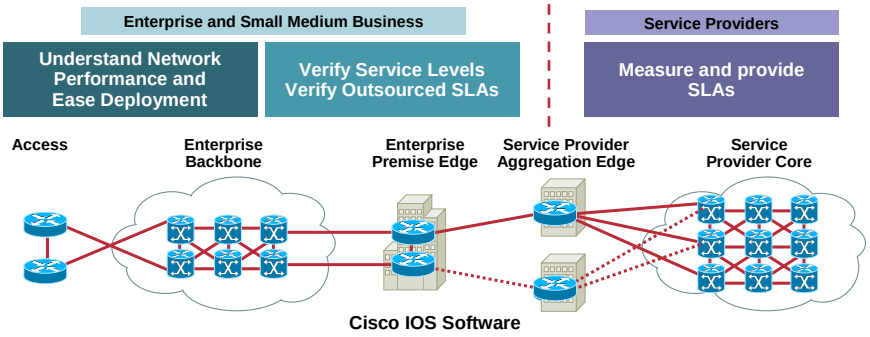
Multimedia QoS Requirements (Examples)

Traffic Type	Maximum Packet Loss	Maximum One-Way Latency	Max. Jitter
VoIP	1 %	200 ms	30 ms
Video-conferencing	1 %	200 ms	30 ms
Streaming video	2 %	5 s	N/A

Cisco IOS IP Service Level Agreement: A New Direction

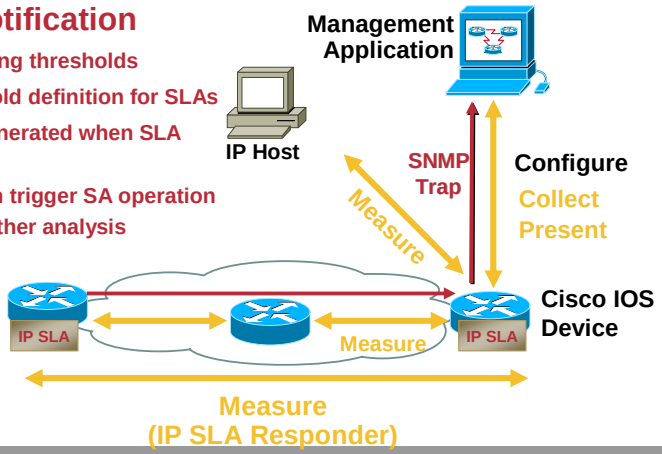
Cisco Solution that Assures IP Service Levels, Proactively Verifies Network Operation, and Accurately Measures Network Performance

- Comprehensive hardware support
- Committed Cisco partner support
- Cisco IOS Software, the world's leading network infrastructure software



How Does It Work?

- Hop-by-hop analysis
- Edge-to-Edge measurement
- Proactive Notification
  - Rising and falling thresholds
  - Robust threshold definition for SLAs
  - SNMP traps generated when SLA violated
  - Thresholds can trigger SA operation activation for further analysis



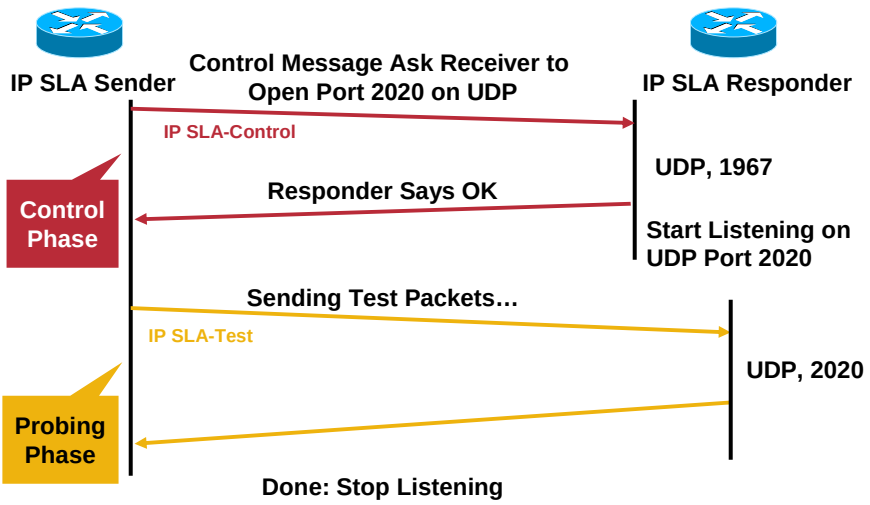
IP SLA Sender

- Cisco IOS device that sends probe packets
- Operation configuration takes place on the sender only
- Once the operation is finished, all the results are to be polled off the sender
- Target is another host (IP Host, or IP SLA Responder)
- Some operations require the target to run the IP SLA responder (Jitter for instance), some other are working with a simple IP Host (ICMP Ping)

IP SLA Responder

- Runs on Cisco IOS
- Configure 'ip sla monitor responder', or set rttMonApplResponder.0=1 with SNMP
- Sender uses the IP SLA Control Protocol to communicate with responder before sending the test packets
- Responder knows the type of operation, the port used, the duration
- Communication can be authenticated with MD5, not encrypted (offers integrity)
- Responder inserts in/out timestamps in packet payload (measures CPU time spent)

IP SLA Operation With Responder

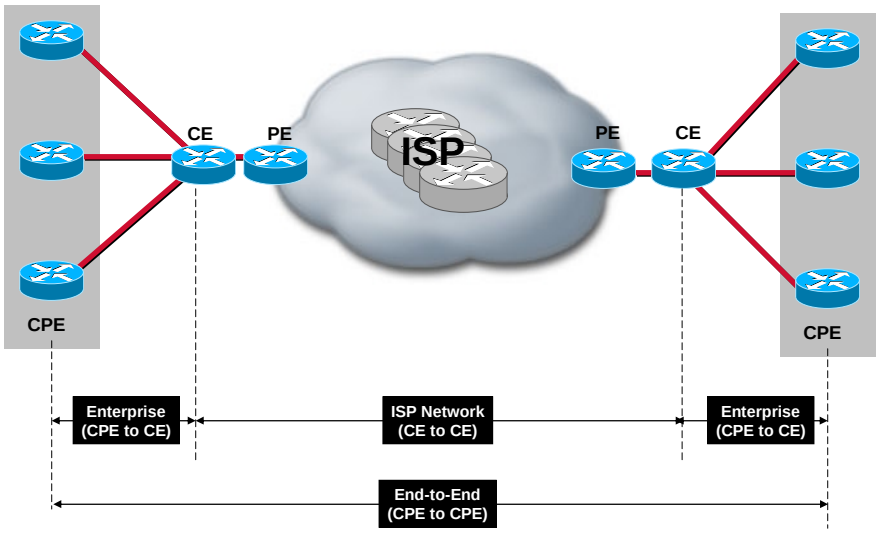


Cisco IOS IP SLAs and CISCO-RTTMON-MIB

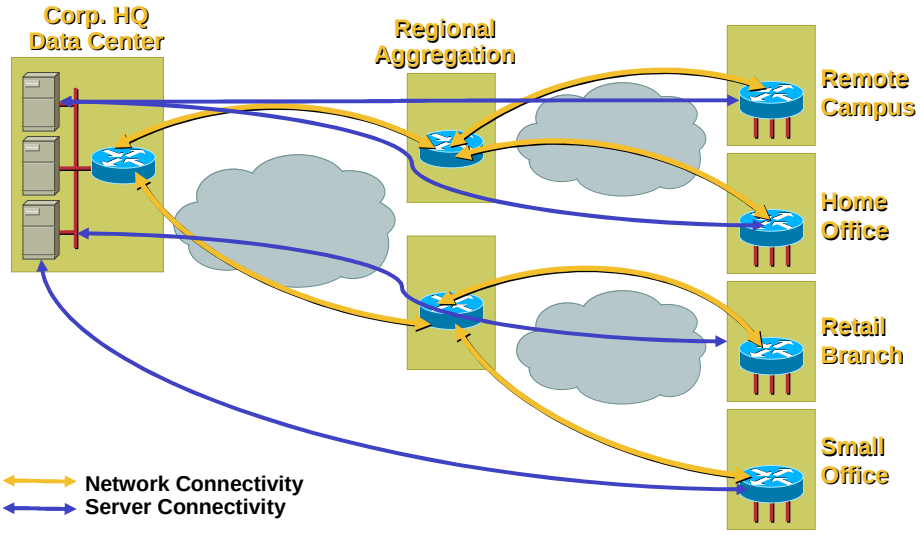
- IP SLAs (a.k.a. Service Assurance Agent—SAA, formerly RTR)
- IP SLAs is an active measurement tool, unlike NetFlow which is passive
- Generates availability and threshold traps
- Also collects statistics
- Information can be retrieved by SNMP

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

Scenario 2: Enterprise WAN
ISP SLA Monitoring



Scenario 2: Enterprise WAN
Hierarchical Monitoring



Cisco IOS IP SLA Uses and Metrics

	*Data Traffic	*VoIP	*Service Level Agreement	*Availability	**Streaming Video
Requirement	• Minimize delay, packet loss • Verify QoS	• Minimize delay, packet loss, jitter	• Measure delay, packet loss, jitter • One-way	Connectivity testing	• Minimize delay, packet loss
IP SLA Measurement	• Jitter • Packet loss • Latency • Per QoS	• Jitter • Packet loss • Latency • MOS voice Quality score	• Jitter • Packet loss • Latency • One-way • Enhanced accuracy • NTP	• Connectivity tests to IP devices	• Jitter • packet loss • Latency

Benefits of Using IP SLA

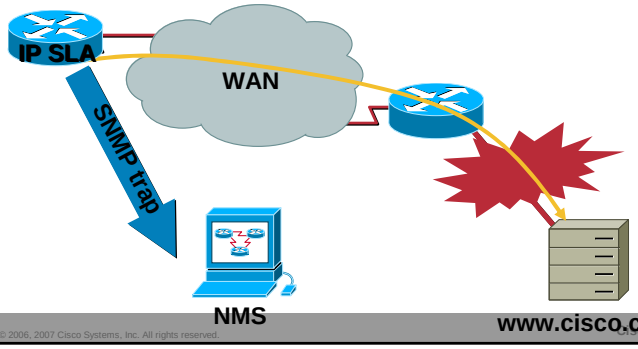
- Flat learning curve (Cisco IOS technology)
- No additional equipment, nor vendor
- Can be deployed on customer site (CPE) and measure end-to-end SLAs
- Activate at the production router (CPE, CE, PE) or as a dedicated “shadow-router”
- Can be managed with existing router management tools (e.g. CiscoWorks IPM)

IP SLA Technical Overview

- Wide measurement capabilities (UDP, TCP, ICMP,…)
- Near millisecond precision
- Accessible using CLI and SNMP
- Proactive notification
- Historical data storage
- Flexible scheduling options
- Already in Cisco IOS (available on most platforms)
- Almost all interfaces supported, physical, and logical

Proactive Notification

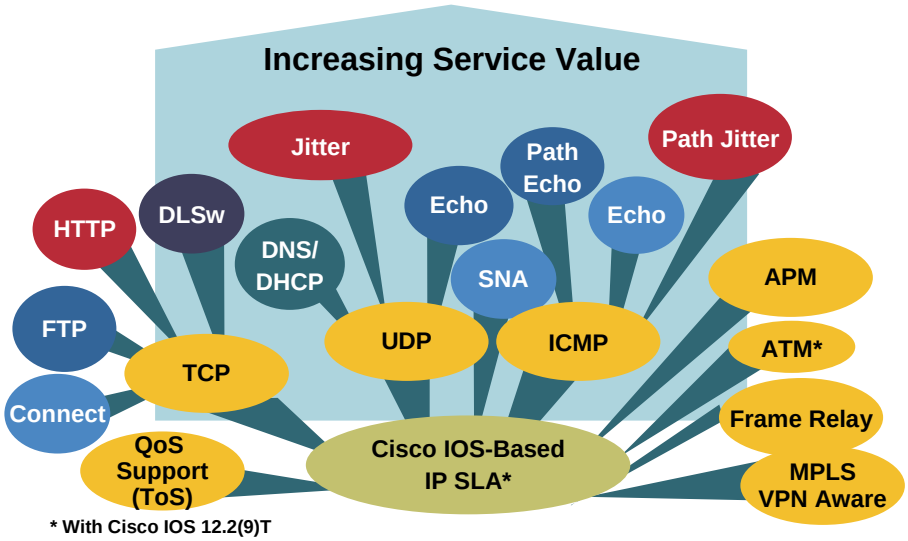
- Can send SNMP traps when certain “triggering” events occur (e.g., when rising and falling thresholds are passed)
- Can trigger another IP SLA operation for further analysis (e.g., when ping fails, a path echo operation starts)



Historical Data Storage

- Stores previous results
- Not supported on all operations
- New enhanced history enables configuration of IP SLA to store aggregated measurements in "buckets"
  - –e.g., store 48 buckets, and each bucket maintains 15 minutes of the aggregated measurements; with this configuration, it can store 12 hours of performance information

IP SLA Today



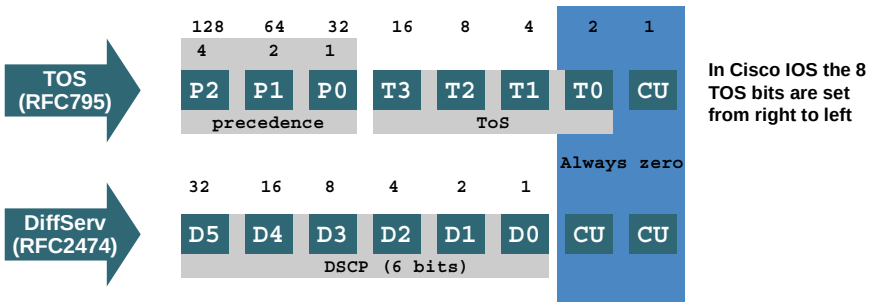
* With Cisco IOS 12.2(9)T

TOS Marking

- Probes can be TOS marked to match the target class
- Only TOS setting is supported, no diffserv (see next slide to perform translation)

```
ip sla monitor 11
 type jitter dest-ipaddr 10.52.130.68 dest-port 16384 \
       interval 20 num-packets 1000
 tos 0x20
 frequency 60
 request-data-size 172
ip sla monitor schedule 11 start-time now
```


Converting Between TOS and DiffServ



In Cisco IOS the 8 TOS bits are set from right to left

Binary	ToS	DSCP	Precedence
101 000	160 (0xA0)	40	5
101 100	176 (0xB0)	44	5
001 110	56 (0x38)	14	1

Uses for IP SLA Operations

Operations Supported	What can it be used for ?
UDP Jitter for VoIP	For IP Backbones that carry voice traffic
UDP Echo	Accurate measurement of UDP response time
UDP Jitter	For IP Backbones that carry voice/video traffic
TCP Connect	Server and Application performance monitoring
DNS	DNS performance monitoring & troubleshooting
DHCP	Response time to a DHCP server
FTP	FTP get performance monitoring
HTTP	Web site performance monitoring
ICMP	Trouble-shooting and availability measurement
ICMP Path Echo	Trouble-shooting
ICMP Path Jitter	Trouble-shooting
DLSW+	DLSw peer tunnel performance monitoring

Features and Supported Cisco IOS Version

Feature/Release	11.2	12.0(3)T	12.0(5)T 12.0(8)S	12.1(1)T 12.2	12.2(2) T	12.2(11)T (Eng2)	12.3(4)T	12.3(12) T
ICMP Echo	X	X	X	X	X	X	X	X
ICMP Echo Path	X	X	X	X	X	X	X	X
UDP Echo		X	X	X	X	X	X	X
TCP Connect		X	X	X	X	X	X	X
UDP Jitter			X	X	X	X	X	X
HTTP			X	X	X	X	X	X
DNS			X	X	X	X	X	X
DHCP			X	X	X	X	X	X
DLSw+			X	X	X	X	X	X
SNMP Support			X	X	X	X	X	X
UDP Jitter With One Way Latency				X	X	X	X	X
FTP Get				X	X	X	X	X
MPLS/VPN Aware					X	X	X	X
Frame-Relay (CLI)					X	X	X	X
ICMP Path Jitter					X	X	X	X
APM					X	X	X	X
Voice with MOS/ICPIF Score							X	X
Post Dial Delay H323/SIP								X

Cisco IOS IP SLA Partners

Cisco Network Management Solution	
IP Communications Service Monitor	Telephony Monitoring
Internetworking Performance Monitor	Enterprise performance measurements

THIRD PARTY PRODUCTS

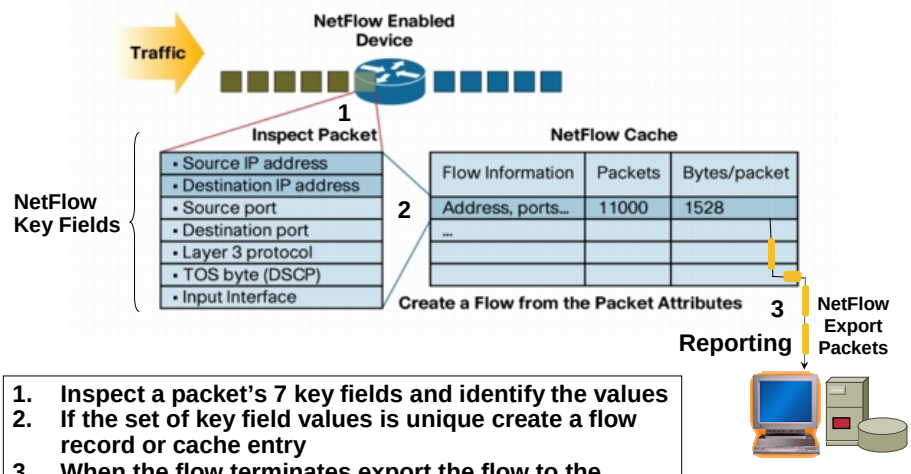
New Partners 2006

Things to Look For

- Provisioning
  - –Does the tool provision IP SLA (easily), or do you have to do it via CLI?
  - –Don't assume: some of the costly products may not do provisioning all that well
  - –How much effort in turning on many IP SLA measurements?
- Reporting
  - –What does the tool do for IP SLA data collection and reports?
  - –Easy to set up and maintain?
- Hierarchy
  - –Does the tool allow aggregate of hierarchical measurements for a more scalable set of measurements?
  - –Not aware of any products that do this yet …

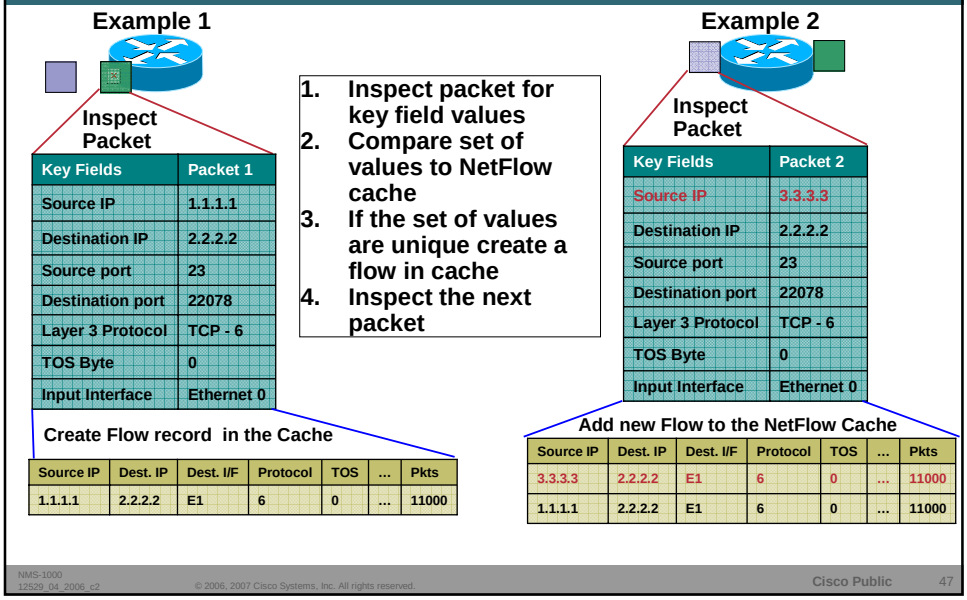
NetFlow

What Is a Traditional IP Flow?



1. Inspect a packet's 7 key fields and identify the values
2. If the set of key field values is unique create a flow record or cache entry
3. When the flow terminates export the flow to the collector

NetFlow Key Fields Creating Flow Records



NetFlow

What Is a Flow?

- A flow is a stream of traffic from a source to a destination that moves across a device
- Seven fields identify flows
  - –Source IP address
  - –Destination IP address
  - –Source port number
  - –Destination port number
  - –Layer 3 protocol type
  - –ToS byte
  - –Input logical interface (ifIndex)

Traditional Layer 3 NetFlow Cache

1. Create and update flows in NetFlow cache

Key Fields in Yellow
Non-Key Fields white

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A 2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A 1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- Inactive timer expired (15 sec is default)
- Active timer expired (30 min (1800 sec) is default)
- NetFlow cache is full (oldest flows are expired)

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

4. Export version

Non-Aggregated Flows—Export Version 5 or 9

5. Transport protocol

30 Flows per 1500 byte export packet

Export Packet: Header | Payload (Flows)

NetFlow

What Kind of Information Does a Device Send About a Flow?

- Currently, devices export flow information for ingress traffic only
- Devices export NetFlow Data Export (NDE) in UDP packets
- NDE includes flow information such as
  - Source address, destination address
  - Bytes, packets

NetFlow

NDE Versions

- Static versions

	src addr	dst addr	src port	dst port	nexthop	SNMP input	SNMP output	prot	tos	flags	flows	octets	packets	start time	end time	src as	dst as	src mask	dst mask	router sc	src prefix	dst prefix
Version 1	x	x	x	x	x	x	x	x	x	x		x	x	x	x							
Version 5	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x			
Version 7	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x		
Version 8—AS						x	x				x	x	x	x	x	x	x					
Version 8—ProtoPort			x	x				x			x	x	x	x	x							
Version 8—DstPrefix							x				x	x	x	x	x		x		x			x
Version 8—SrcPrefix						x					x	x	x	x	x	x		x			x	
Version 8—Prefix						x	x				x	x	x	x	x	x	x	x	x		x	x

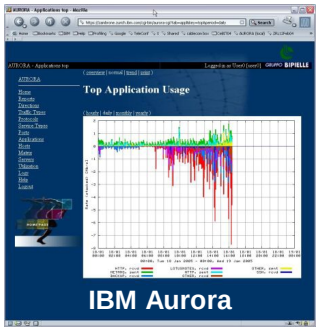
- Version 9 Templates define NDE fields and lengths
  - –NetFlow version 9 is the IETF standard mechanism for information export: IPFIX

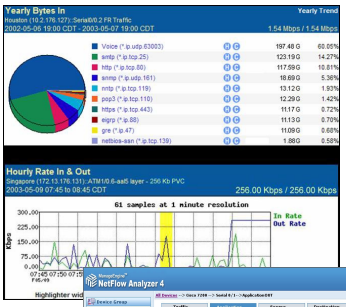
NetFlow

What Do Customers Do with NetFlow?

- Network traffic analysis
- Billing and accounting
- Anomaly detection
- Capacity planning

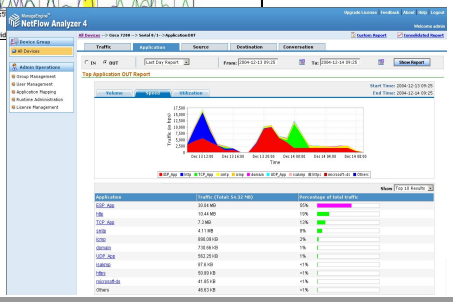
NetFlow Reporting Application Examples





NetQos

AdventNet



Partner Links:
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/

http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/

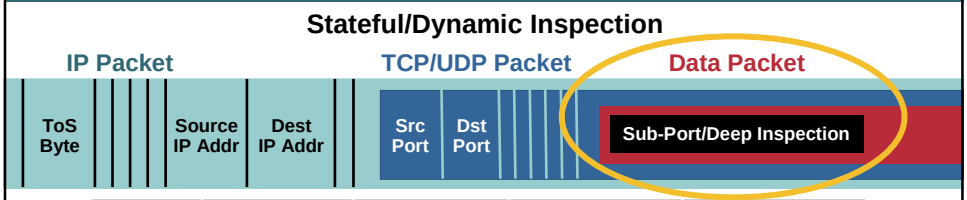
NBAR

NBAR Principles

- Network-Based Application Recognition classifies traffic by protocol (layer 4–7)
- NBAR supports the following QoS features:
  - Guaranteed bandwidth with Class-Based Weighted Fair Queuing (CBWFQ)
  - Policing and limiting bandwidth
  - Marking (ToS or IP DSCP)
  - Drop policy with weighted random early detection (WRED)
- Accounting functionality is enabled via NBAR feature "protocol discovery"
- Protocol discovery analyzes Application Traffic patterns in real time and discovers which traffic is running on the network
- Per interface, per application, bidirectional (input and output) Statistics: bit rate (bps), packet counts, byte counts

Information: http://www.cisco.com/go/nbar

NBAR Details



Egp	Exchange	Kerberos	Secure-nntp	Smtp
Gre	Finger	L2tp	Notes	Snmp
Icmp	Ftp	Ldap	Novadigm	Socks
Ipinip	Secure-ftp	Secure-ldap	Ntp	Sqlnet
Ipsec	Gopher	Netshow	Pcanywhere	Ssh
Eigrp	Http	Pptp	Pop3	Streamwork
Bgp	Secure-http	Sqlserver	Secure-pop3	Syslog
Cuseeme	Imap	Netbios	Printer	Telnet
Dhcp	Irc	Nfs	Realaudio	Secure-Telnet
Dns	Secure-irc	Nntp	Rcmd	Tftp
		Citrix	Napster	Vdolive
				Xwindows

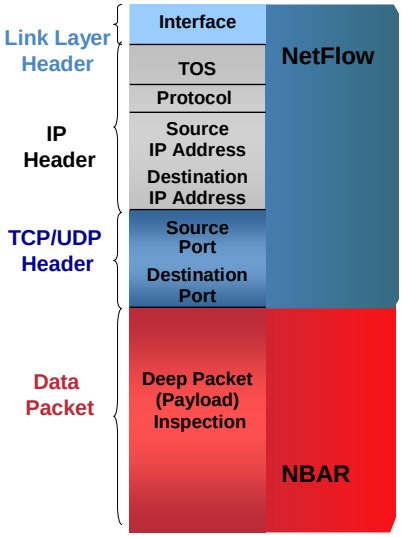
NBAR Currently Supports > 90 Protocols/Applications

NBAR show Command

```
router# show ip nbar protocol-discovery interface FastEthernet 6/0

FastEthernet6/0
                              Input                                     Output
Protocol                      Packet Count                              Packet Count
                              Byte Count                                Byte Count
                              5 minute bit rate (bps)                   5 minute bit rate (bps)
------------------------      ------------------------                  ------------------------
http                          316773                                    0
                              26340105                                  0
                              3000                                      0
pop3                          4437                                      7367
                              2301891                                   339213
                              3000                                      0
snmp                          279538                                    14644
                              319106191                                 673624
                              0                                         0
ftp                           8979                                      7714
                              906550                                    694260
                              0                                         0
…
Total                         17203819                                  151684936
                              19161397327                               50967034611
                              4179000                                   6620000
```


NetFlow and NBAR Differentiation



NetFlow

- ✓ Monitors data in Layers 2 thru 4
- ✓ Determines applications by port
- ✓ Utilizes a 7-tuple for flow
- ✓ Flow information who, what, when, where

NBAR

- ✓ Examines data from Layers 3 thru 7
- ✓ Utilizes Layers 3 & 4 plus packet inspection for classification
- ✓ Stateful inspection of dynamic-port traffic
- ✓ Packet and byte counts

NBAR and AutoQoS

- Cisco IOS AutoQos feature has two flavors
  1. AutoQoS for VoIP: one stage mechanism, creates pre-defined policy maps for voice traffic
  2. AutoQoS Enterprise
     - I) Turn on the discovery mode and gather traffic statistics *(config-if)# "auto discovery qos"*
     - II) A policy map is created based on the detected traffic with suggested bandwidth settings per class
     - Two modes
     - "Trusted mode" in case DSCP has been set correct
     - "Untrusted mode" discovers applications by leveraging NBAR
- Introduced in 12.3 T

Cisco AutoQoS for Enterprise

Procedure

1. Invoke "auto discovery qos" on the applicable link

   Use "show auto discovery qos" to view data collection in progress
2. Automatically configure the link with "auto qos" command

   Use "show auto qos" to display the QoS policy settings deployed
3. Use "auto discovery trust" in the core if DSCP values are already assigned at the edge

Traffic Class	DSCP
IP Routing	CS6
Interactive Voice	EF
Interactive Video	AF41
Streaming Video	CS4
Telephony Signaling	CS3
Transaction/Interactive	AF21
Network Management	CS2
Bulk Data	AF11
Best Effort	0
Scavenger	CS1

Cisco AutoQoS: Discovery in Progress

```
router# show auto discovery qos

AutoQoS Discovery enabled for applications
 Discovery up time: 2 days, 55 minutes
 AutoQoS Class information:
 Class VoIP:
 Recommended Minimum Bandwidth: 517 Kbps/50% (PeakRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol       (kbps/%)       (kbps/%)   (bytes)
 rtp audio      76/7           517/50     703104
 Class Interactive Video:
 Recommended Minimum Bandwidth: 24 Kbps/2% (AverageRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol       (kbps/%)       (kbps/%)   (bytes)
 rtp video      24/2           5337/52    704574
 Class Transactional:
 Recommended Minimum Bandwidth: 0 Kbps/0% (AverageRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol       (kbps/%)       (kbps/%)   (bytes)
 citrix         36/3           74/7       30212
 sqlnet         12/1           7/<1       1540
```

Note: Review Recommendations

Cisco AutoQoS: Suggested Policy

```
Suggested AutoQoS Policy for the current uptime:
 !
 class-map match-any AutoQoS-Voice-Et3/1
 match protocol rtp audio
 !
 class-map match-any AutoQoS-Inter-Video-Et3/1
 match protocol rtp video
 !
 class-map match-any AutoQoS-Signaling-Et3/1
 match protocol sip
 match protocol rtcp
 !
 class-map match-any AutoQoS-Transactional-Et3/1
 match protocol citrix
 !
 class-map match-any AutoQoS-Bulk-Et3/1
 match protocol exchange

policy-map AutoQoS-Policy-Et3/1
 class AutoQoS-Voice-Et3/1
 priority percent 1
 set dscp ef
 class AutoQoS-Inter-Video-Et3/1
 bandwidth remaining percent 1
 set dscp af41
 class AutoQoS-Signaling-Et3/1
 bandwidth remaining percent 1
 set dscp cs3
```

Recommended Policy Is Based on AutoDiscovery Statistics

Options

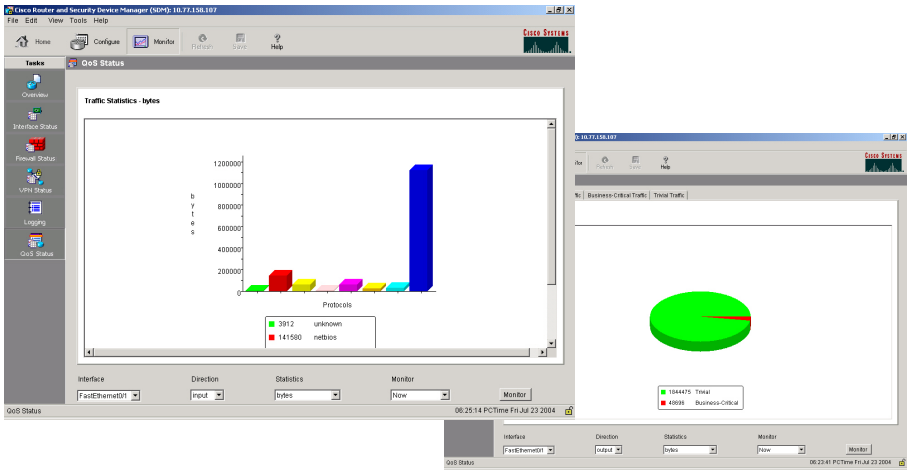
- Continue AutoDiscovery (policy may change)
- Copy and change the policy (offline)

```
. . .
 class AutoQoS-Transactional-Et3/1
 bandwidth remaining percent 1
 random-detect dscp-based
 set dscp af21
 class AutoQoS-Bulk-Et3/1
 bandwidth remaining percent 1
 random-detect dscp-based
 set dscp af11
 class class-default
 fair-queue
```

Note: Review Recommendations

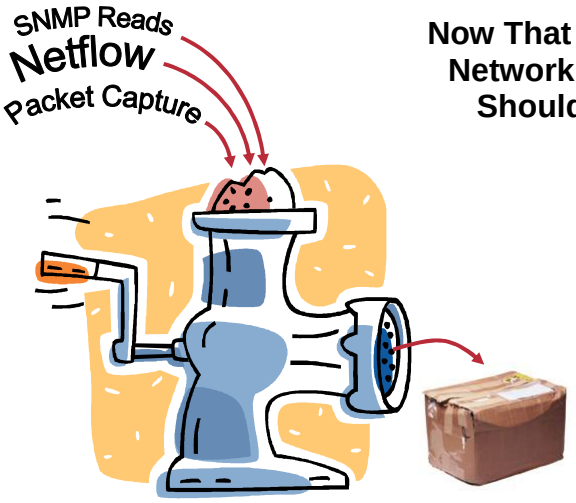
Cisco Router and Security Device Manager (SDM)

GUI for Device Configuration and Monitoring



Net Mgmt Stories

Applying a Management Model



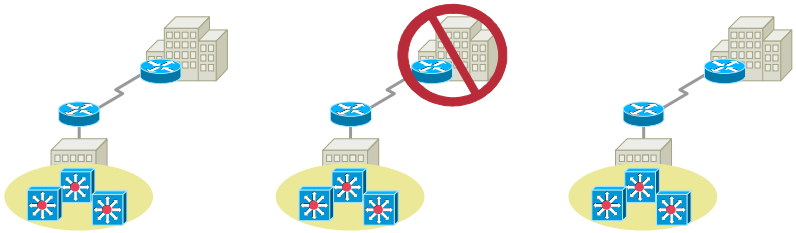
Now That You Have Gathered Network Information, What Should You Do with It?

Fault: Production Example

The Problem

- **Network administrator was receiving fault notifications of a recurring problem; each evening between 8:00 and 8:30 connectivity is lost to a branch office; connectivity is restored at approximately 9:00pm**

7:50pm **8:30pm** **9:00pm**



Fault: Production Example

- **Considerations**
  - –Is an entire device failing? If so, what device?
  - –Is a link failing? If so, which link?
  - –How can this be prevented in the future?
- **Management processes in place**
  - –Actively polling critical devices for availability
  - –Notification tool to alert administrator

The Remedy →

Fault: Production Example

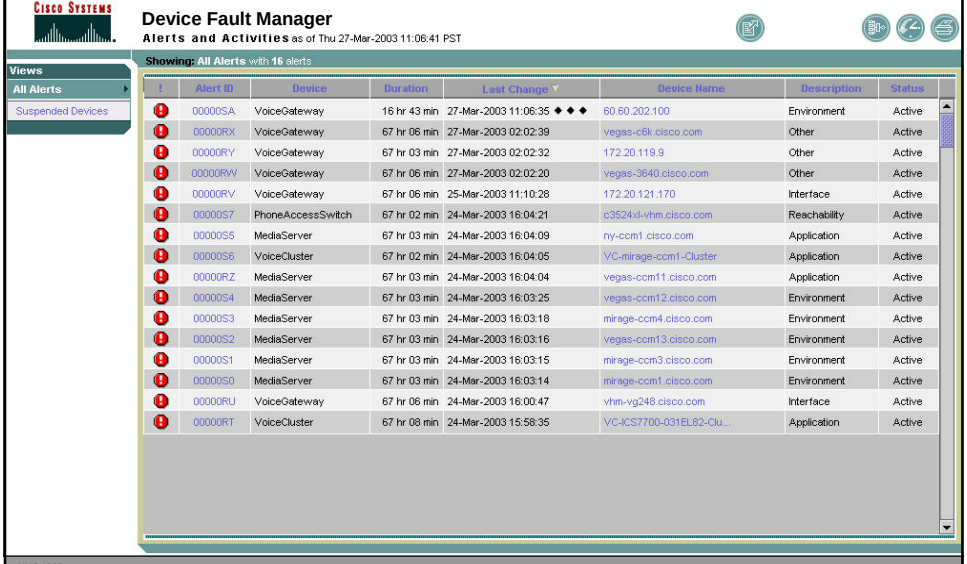
The Remedy

- The loss of connectivity was linked to the late night janitor unplugging the WAN router to plug in his vacuum cleaner
- The fix was to provide the late night janitor with his own power outlet

Fault Management
Device Fault Manager

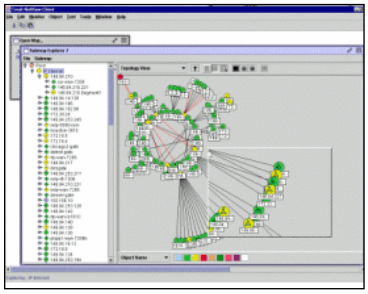
- **Administrator was notified of failure via a notification tool (email, page, etc.)**
- **Notification shows up on the console as an unresponsive router**
- **Device level fault and root cause analysis for Cisco products**
- **Monitor for high availability**
- **MIBs, polling intervals and thresholds set by default out of the box**

Fault Management
Device Fault Manager



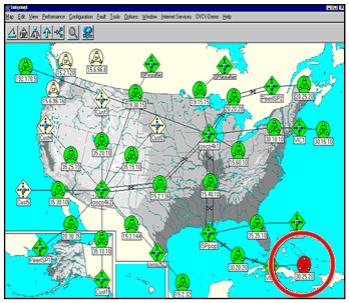
Fault Management Tools
HP and Tivoli

Tivoli



Correlate and Manage
Events and SNMP Traps

HEWLETT® PACKARD



Perform Fault Isolation
and Root Cause Analysis

Configuration: Practical Example

The Problem

- Network administrator notices night time configuration changes in the production network followed by immediate configuration rollbacks to disguise any tampering

10:55pm

```
logging 192.168.76.228
logging 192.168.76.229
!
snmp-server community public RO
snmp-server community forks RW
snmp-server system-shutdown
```

11:05pm

```
logging 192.168.76.228
logging 192.168.76.229
logging 192.168.76.4
!
snmp-server community public RO
snmp-server community spoons RW
snmp-server system-shutdown
```

11:23pm

```
logging 192.168.76.228
logging 192.168.76.229
!
snmp-server community public RO
snmp-server community forks RW
snmp-server system-shutdown
```

Configuration: Practical Example

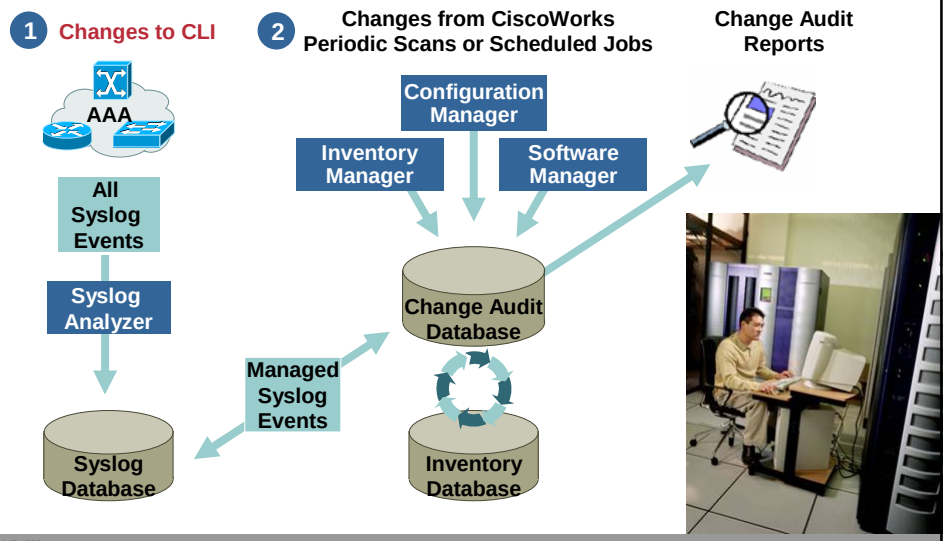
- **Considerations**
  - –**What changes were made?**
  - –**When were the changes made?**
  - –**Who made them?**
  - –**How can this be prevented in the future?**
- **Management processes in place**
  - –**Devices configured to send config change syslog messages to NMS**
  - –**User authentication tool**
  - –**Configuration archiving**

The Remedy →

Configuration: Practical Example

- **The Diagnosis**
  - –**The network configuration changes were being made by a colleague "upgrading their skills" after hours using the production network**
- **The Remedy**
  - –**The remedy was to provide the culprit with an unused 1841 router to be used in their home**

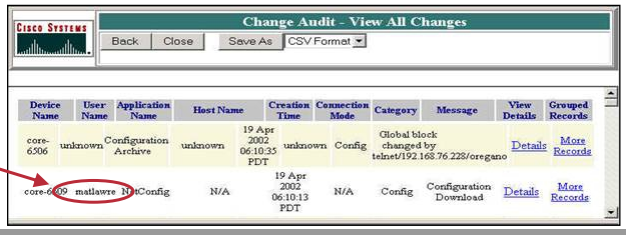
Configuration Management
Resource Manager Essentials Change Audit Service



Configuration Management
RME Change Audit Setup

- **Change audit relies on syslog messages to operate**
  - **Point syslogs from all managed devices (except Pix firewalls) to the RME server**
- **Collection of usernames occurs in three ways**
  1. **Using usernames on devices themselves**
  2. **Using a RADIUS or TACACS server**
  3. **Using a configurations change tool in RME (NetConfig, Config Editor)**

That User Name Field Is Important to Most Customers



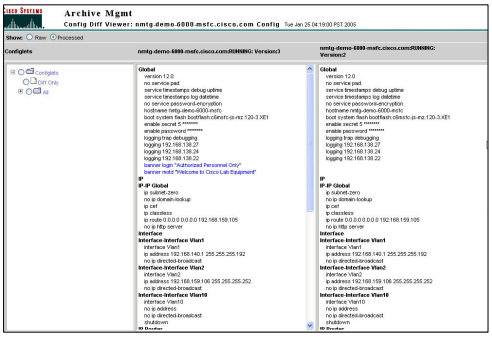
Configuration Management
Cisco IOS and Catalyst OS Upgrades

- Use a **dedicated** TFTP server to store and distribute software images

```
core-6506-msfc#copy tftp flash
Address or name of remote host []? 19.16.76.175
Source filename []? 12.1.8a
Destination filename []? 12.1.8a
```

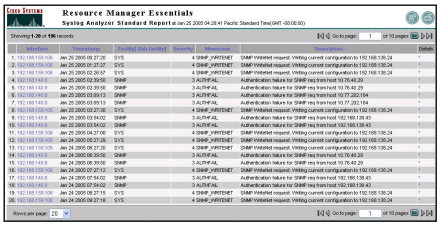
Or

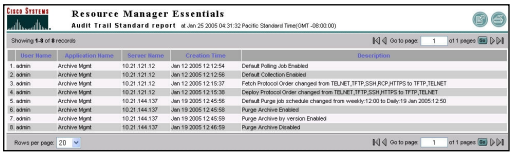
- Resource Manager Essentials includes **Softw**are **I**mage **M**anager to automate the upgrade process



Resource Manager Essentials

- **Syslog Analyzer**
  - –Distributed collection, flexible reporting, and action scripts to pinpoint network incidents
- **Diagnostics and Tools**
  - –Troubleshoot device connectivity
  - –Desktop integration of partner and customer applications
  - –User customizable Network-wide show command tool





Resource Manager Essentials

Cisco Systems

Resource Manager Essentials

Syslog Analyzer Standard Report at Jan 25 2005 04:28:41 Pacific Standard Time(GMT -08:00:00)

Showing **1-20** of **196** records — Go to page: 1 of 10 pages Go

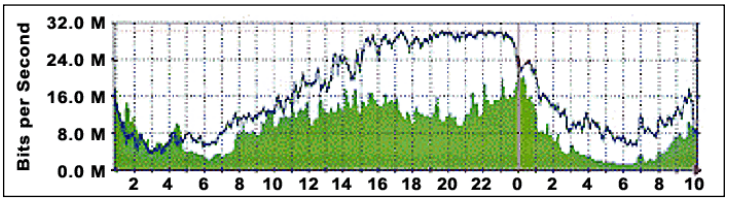
	Interface	Timestamp	Facility[-Sub-facility]	Severity	Mnemonic	Description	Details
1.	192.168.159.106	Jan 25 2005 00:27:20	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
2.	192.168.159.106	Jan 25 2005 01:27:27	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
3.	192.168.159.106	Jan 25 2005 02:26:57	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
4.	192.168.140.8	Jan 25 2005 02:39:50	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.76.40.29	*
5.	192.168.140.8	Jan 25 2005 02:39:50	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.76.40.29	*
6.	192.168.140.8	Jan 25 2005 03:09:13	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.77.202.184	*
7.	192.168.140.8	Jan 25 2005 03:09:13	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.77.202.184	*
8.	192.168.159.106	Jan 25 2005 03:27:30	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
9.	192.168.140.8	Jan 25 2005 03:54:02	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 192.168.138.43	*
10.	192.168.140.8	Jan 25 2005 03:54:02	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 192.168.138.43	*
11.	192.168.159.106	Jan 25 2005 04:27:00	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
12.	192.168.159.106	Jan 24 2005 05:27:29	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
13.	192.168.159.106	Jan 24 2005 06:27:20	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
14.	192.168.140.8	Jan 24 2005 06:39:50	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.76.40.29	*
15.	192.168.140.8	Jan 24 2005 06:39:50	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 10.76.40.29	*
16.	192.168.159.106	Jan 24 2005 07:27:12	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
17.	192.168.140.8	Jan 24 2005 07:54:02	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 192.168.138.43	*
18.	192.168.140.8	Jan 24 2005 07:54:02	SNMP	3	AUTHFAIL	Authentication failure for SNMP req from host 192.168.138.43	*
19.	192.168.159.106	Jan 24 2005 08:27:15	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*
20.	192.168.159.106	Jan 24 2005 09:27:18	SYS	4	SNMP_WRITENET	SNMP WriteNet request. Writing current configuration to 192.168.138.24	*

Rows per page: 20 — Go to page: 1 of 10 pages Go

Performance Management Real World Example

The Problem

- **A university network administrator observes dramatic increase in outgoing WAN traffic resulting in increased costs and decreased response times**



Solid Green **Represents Incoming Traffic**

Blue Line **Represents Outgoing Traffic**

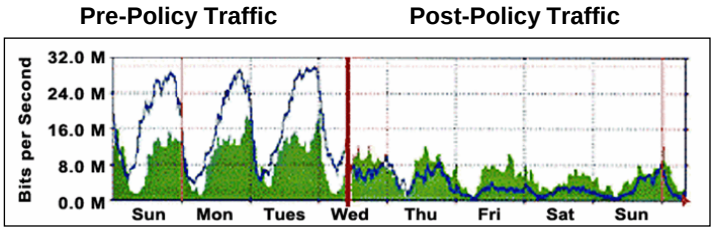
Performance Management Real World Example

- **Considerations**
  - –**What** traffic type is leaving the university?
  - –**Why** is the traffic being generated?
  - –**Who** is generating the traffic?
  - –**How** can this be prevented in the future?
- **Management processes in place**
  - –Link usage trending software
  - –**Traffic capture and analysis** capability
  - –Scalable **QoS policy** deployment software

The Remedy →

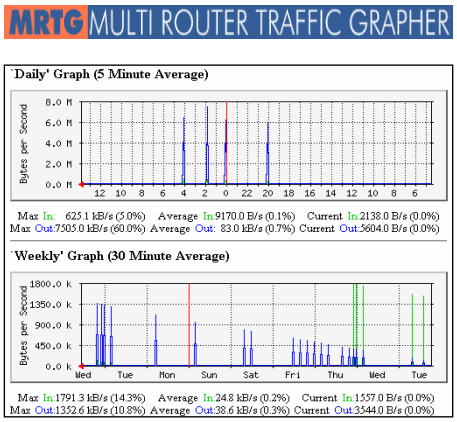
Performance Management Real World Example

- **The network congestion was being caused by file sharing applications**
- **The remedy was to deploy quality of service policies to edge devices**



Performance Management
Link Usage Trending

- University was logging incoming and outgoing usage over time with MRTG
- Monitors traffic load on network links based on SNMP statistics
- Generates real-time HTML traffic reports
- Can be used to monitor any SNMP variable you choose
- It's FREE! www.mrtg.org
- See also Cacti: www.cacti.net



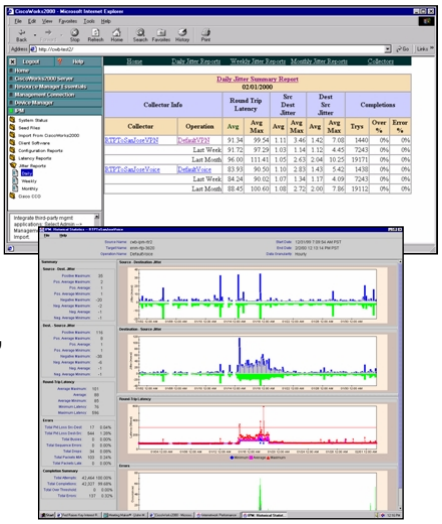
Performance Management
Traffic Analysis

Network Analysis Module

- Enables full traffic monitoring
  - –Real-time traffic analysis
  - –Performance monitoring
  - –Troubleshooting
- Web-based embedded traffic analyzer
  - –VoIP, QoS(DSMON), ART, VLAN(SMON), RMON 1 and 2 monitoring
  - –Data capture and decode, alarms
- Supported by other applications
  - –nGenius Real-Time Monitor, CiscoView, Concord eHealth

Performance Management
Internetwork Performance Monitor

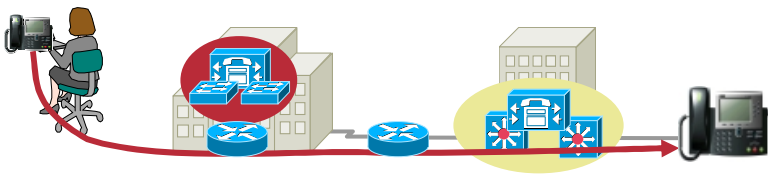
- **WAN troubleshooting**
  - –**Measures hop-by-hop response time, availability, jitter, and drops**
  - –**Provides real-time and historical reports**
- **Utilizes IP-SLA Agent embedded in Cisco IOS**
  - –**Validates and measures TCP, UDP, HTTP, VoIP, DNS, ICMP with QoS awareness**



Voice Management
Pulling It All Together

The Issue

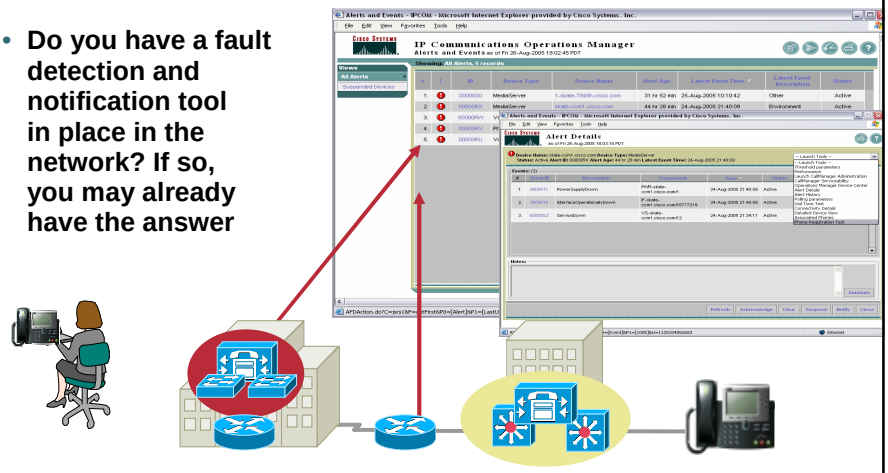
- **Branch office user complains of inability to make or poor quality on a VoIP telephony call to corporate headquarters**



Regional Office **Corporate Headquarters**

Fault

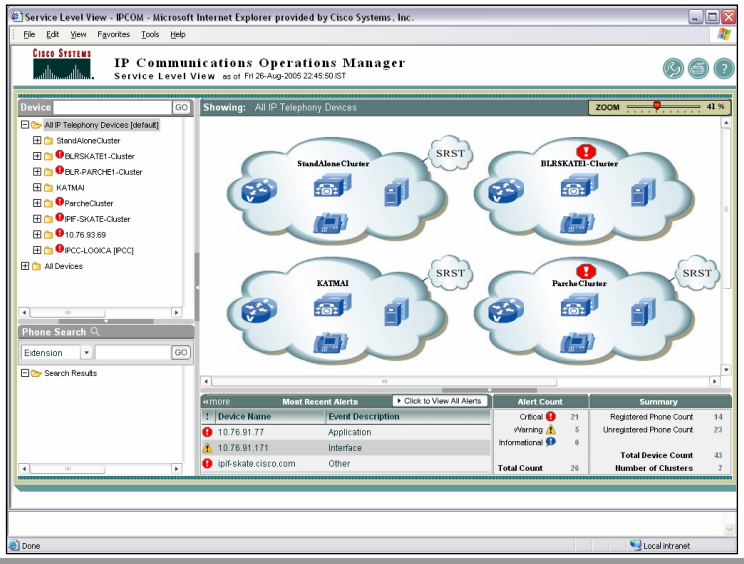
- Do you have a fault detection and notification tool in place in the network? If so, you may already have the answer



Regional Office

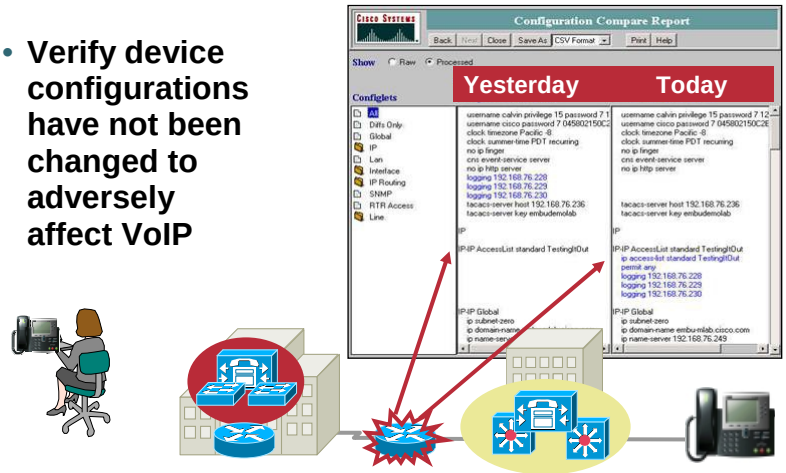
Corporate Headquarters

Fault

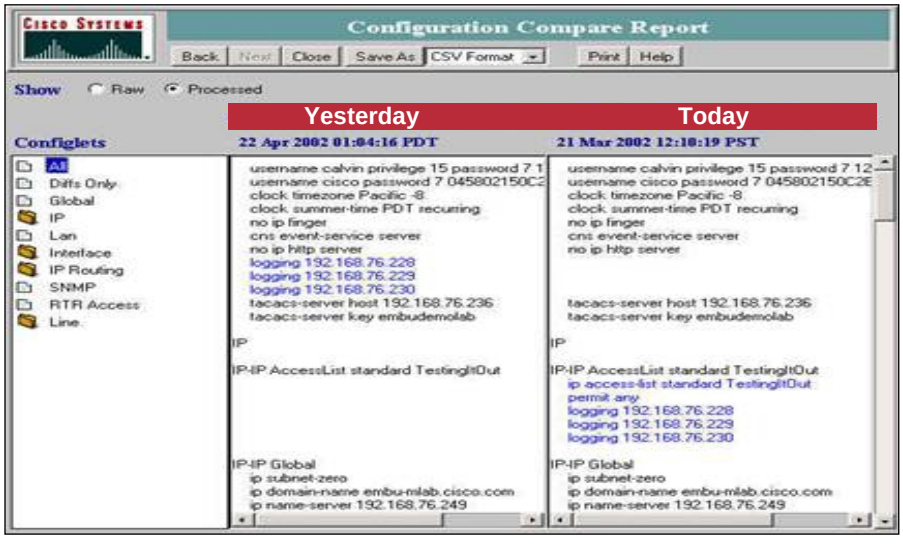


Configuration

- Verify device configurations have not been changed to adversely affect VoIP



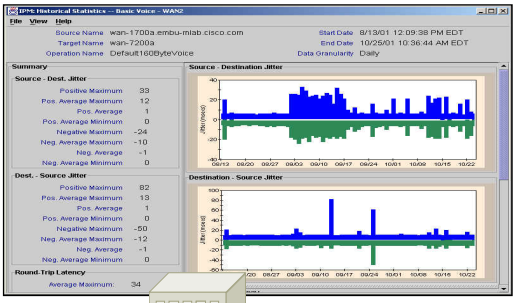
Configuration

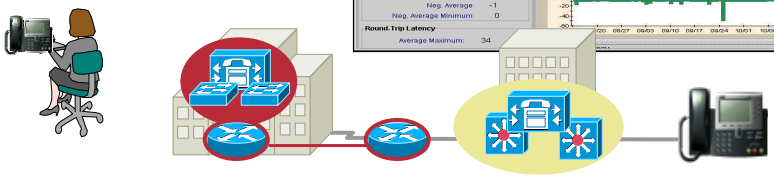


Performance Management

- **Compare current network performance against established baseline**

VoIP Jitter Test Between Offices

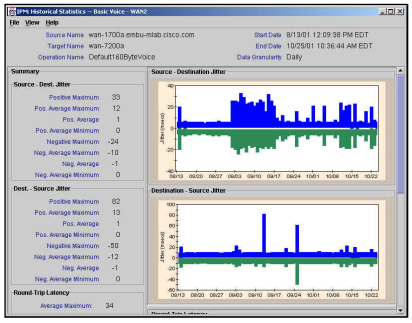




Regional Office **Corporate Headquarters**

Performance Management
A Note on IPM Jitter Reports

If You Want These…



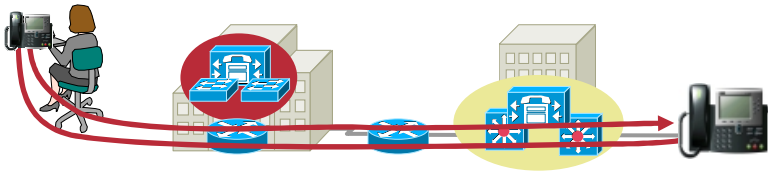
You Have To Do This…

- **Your "source" and "target" must be an SA Agent capable router**
- **You must issue the global configuration to turn on the RTR (Response Time Reporter) responder on the target**

```
core-6506-msfc(config)#rtr responder
```

Voice Management Pulling It All Together

- When faced with a network problem regarding downtime or significant degradation, many different components of proper management must be in place to simplify the troubleshooting process



Regional Office

Corporate Headquarters

Summary

Summary

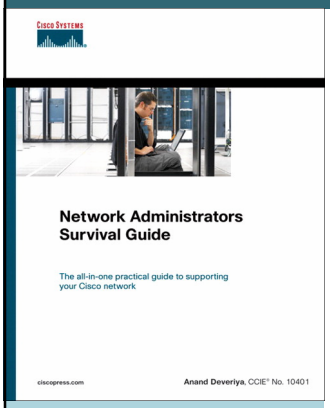
- Stop driving with your eyes closed!
- Find good network management software
  - –Easy to install and use, doesn't keep breaking
  - –Don't want to have to set up data collection one interface or router at a time
- Use the management capabilities in Cisco IOS software!
- Don't just manage the WAN
  - –The Data Center has become just as or more critical
  - –Application / Service measurements are useful
  - –SLA verification is useful

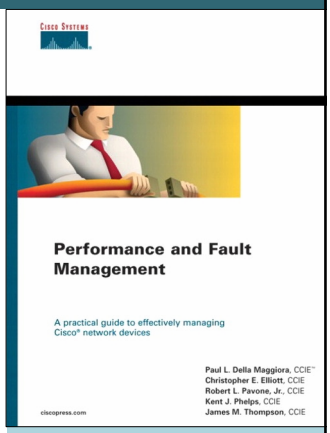
Q and A

Getting More Information

- For more about IP SLA, see Networkers 2006 presentation NMS-1204
  - See also http://www.cisco.com/go/ipsla
- For more about IP Accounting and NetFlow, see NMS-1532
  - See also http://www.cisco.com/go/netflow
- For NBAR, see NMS-3361
  - See also http://www.cisco.com/go/nbar
  - See also AutoQoS for the Enterprise (via the search tool at Cisco)

Recommended Reading





Applause-O-Meter: Net Management Products

- HPOV NNM
- Tivoli Netview
- Tivoli TEC
- MRTG or Cacti
- SolarWinds Orion
- CiscoWorks LMS
- Concord
- InfoVista
- NetQoS ReporterAnalyzer
- NetQoS SuperAgent
- NetQoS NetVoyant
- Network General
- NAM
- NetMRI
- Audience suggestions?
  - –NetFlow reporting
  - –IP SLA provisioning/reporting
  - –Voice / IPT management