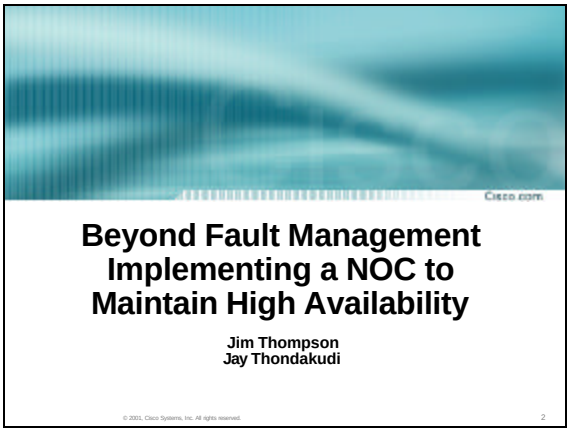
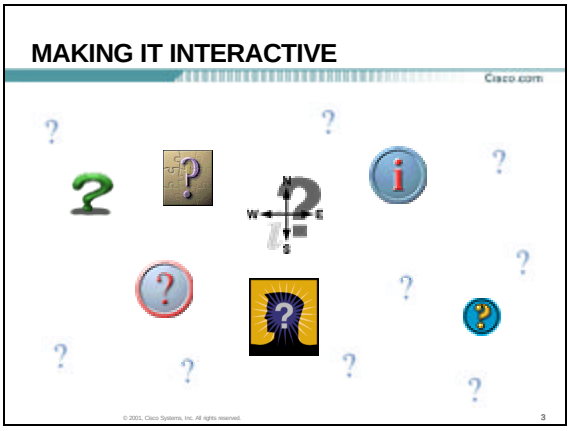




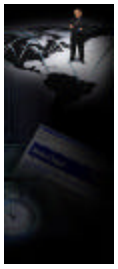
Agenda

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

Method for Attaining a Highly Available Network

or a road to five 9's

- Establish a Standard Measurement Method
- Define Business Goals as Related to Metrics
- Categorize Failures, Root Causes, and Improvements
- Take Action for Root Cause Resolution and Improvement Implementation



Why should we care about network availability?

Recent studies by Sage Research determined that US based Service Providers encountered:

- Percent of downtime that is unscheduled: 44%
- 18% of customers experience over 100 hours of unscheduled downtime or an availability of 98.5%
- Average cost of network downtime per year: $21.6 million or $2,169 per minute!

Downtime - Costs too much!!!

SOURCE: Sage Research, IP Service Provider Downtime Study: Analysis of Downtime Causes,Costs and Containment Strategies, August 17, 2001, Prepared for Cisco SPLO B

Upside has Downside Application Downtime

What are your business goals?

Cisco.com

- **Financial**
  - ROI Economic Value Added Revenue/Employee
- **Productivity**
- **Time to Market**
- **Organizational Mission**
- **Customer Perspective**
  - Satisfaction Retention Market Share

Define your 'end-state'?
What is your goal?

Business Objectives & Availability

Cisco.com

Definition of Network Availability for your company– generalized (i.e.): Network availability management is the optimization of the availability and reliability of networking services and of the supporting network infrastructure, with the objective of ensuring all business requirements are met.

Availability management policy will set a definite course of action for availability measurement, reporting, and procedures. This strategy for availability management will be based on defined and agreed upon business requirements that will help drive policy to determine present and future resource decisions.

The role of network management including availability and performance management functions, is in managing growth and achieving efficiencies of scale as a critical strategic objective for your company

Availability Business Requirements

Cisco.com

- **Yield Control**
  - Yield per customer by volume & mix
  - Maximizing the yield per bandwidth, per router
- **Activity-based accounting**
  - Cost of downtime
  - Cost of waiting for a needed part or tool
  - Cost of reworking or redesign

Availability Business Requirements

Cisco.com

Availability as a Basis for Productivity Data
- Measurement of Total-Factor Productivity
- Benchmarking the Organization
- Overall Organizational Performance Metric

Availability as a Basis for Organizational Competency
- Availability as a Core competency
- Availability Improvement as an Innovation Metric

Resource Allocation Information
- Identify defects
- Identify root cause
- Measure MTTR – tied to process

How does your network enable your business to reach its goals?

Cisco.com

- **User Requirements**
  - Timeliness, Interactivity, Reliability
  - Quality, Adaptability, Security, Affordability
- **Application Requirements**
  - Mission Criticality
  - Controlled-Rate Applications
  - Real-time
- **Performance Requirements**
  - Delay, Reliability, Capacity
- **Network Requirements**
  - Scaling, Services, Interoperability
  - Performance, Monitoring, Troubleshooting

Agenda

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

What is a NOC?

A Helpdesk?

A trouble-ticket logging center?

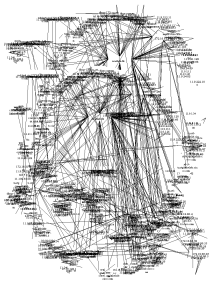
A Break-fix team?

All of the above?

What is a NOC?

Maybe a worst case discussion on

CHAOS Theory!



What is a NOC?

Cisco.com

Are there references?

- **RFC1302 - Building a Network Information Services Infrastructure**
- **Authored February '92 by Merit contributors**

What is a NOC?

Cisco.com

- **From RFC1302**

Definition of a NIC and a NOC

A Network Information Center (NIC) is an organization whose goal is to provide informational, administrative, and procedural support, primarily to users of its network and, secondarily, to users of the greater Internet and to other service agencies.

What is a NOC?

Cisco.com

- **Definition of a NIC and a NOC (cont)**

A Network Operations Center (NOC) is an organization whose goal is to oversee and maintain the daily operations of a network. …

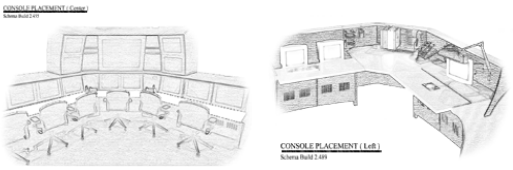
A NIC must work closely with its NOC to ensure users get the best service possible.

Are there other resources?

- North American Network Operator's Group
  - www.nanog.org
  - www.merit.edu/internet/
  - Informative mailing lists
  - Sean "Backhoe King" Donelan
- puck.nether.net/netops/
  - NOC Telephone/Contact List!

Are there other resources?

www.nocbuilder.com



Example of Network Management Goals

- Increase/Maintain Network Availability
- Provide meaningful analysis and correlation of events to assist in FAST fault resolution
- Provide effective use of engineering resources by automating repetitive tasks and de-complexifing network operation

Example of Network Management Goals

- Ensure network configuration information is available for network/device restoration.
- Monitor to ensure that no network outage is caused by a device which has reached its performance limitations.
- Provide regular reports which summarize the network for the various management teams which require them.

What kind of NOC?

Reactive

Proactive

Operational

Develop A Plan

"First comes thought; then organization of that thought, into ideas and plans; then transformation of those plans into reality.

The beginning, as you will observe, is in your imagination."

Napoleon Hill

What are our goals?

- What type of shop are we?

Lights Out & Remote… … or BIC-EOT

Initial Considerations

- What are our Availability/SLA requirements? Maintenance Windows?
- Is the NOC simply identify and escalate… … or also fix?
- How many managed devices are we responsible for?
- Roughly how many events/day (hour, minute) do we currently get or expect?

Initial Considerations (cont'd)

- How much $$ can we allocate?
- What are the skills of the operators?
- What types of devices are we monitoring?
- What are the technologies in use?

Develop A Plan!

Cisco.com

"Given two equally likely solutions to a problem… The simplest one is usually correct."

Occam's Razor

Develop A Plan!

Cisco.com

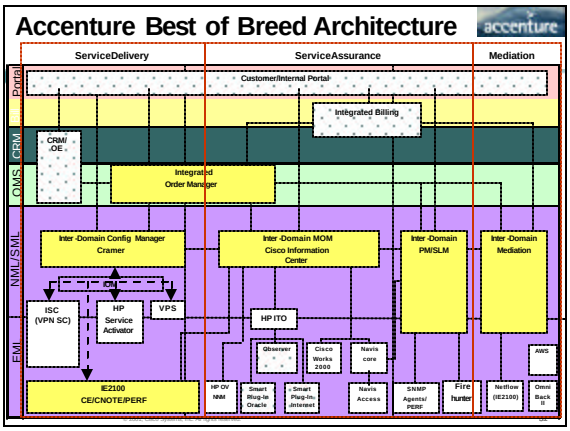
"Given a choice between two methodologies, choose the simplest -- the method which requires the fewest resources. ."

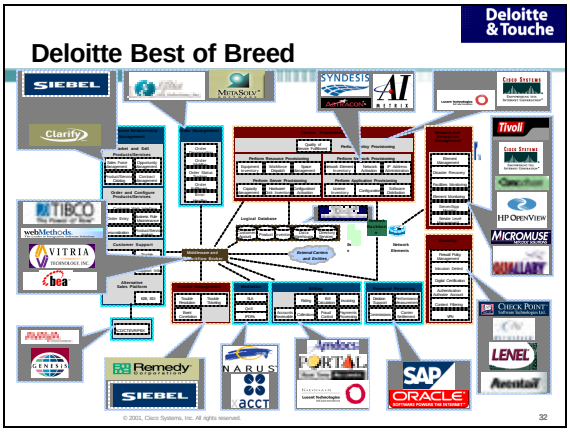
NOC Corollary to Occam's Razor

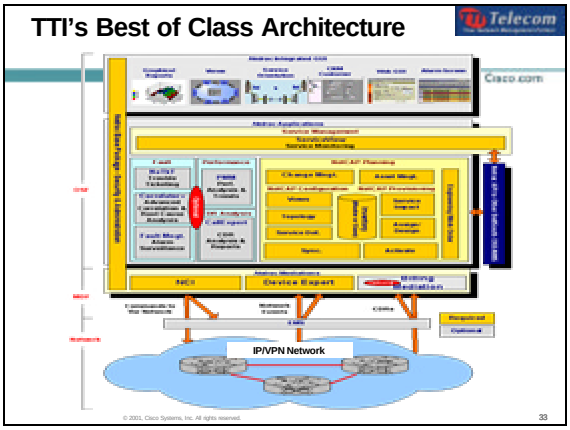
Agenda

Cisco.com

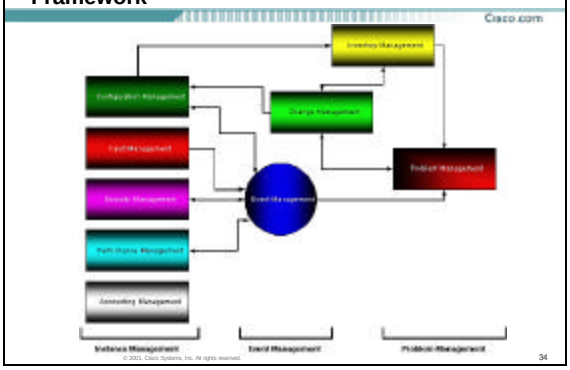
- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC



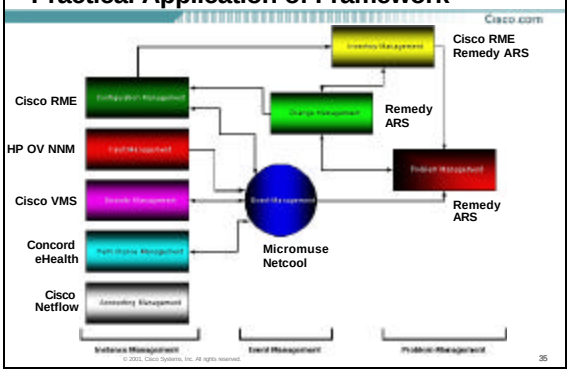




Simplified Network Management Framework



Practical Application of Framework



Agenda

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- **Fault Management**
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

Device Management

- Master Device Inventory
- SNMP
- SYSLOG
- CLI

Master Device Inventory

- Need a complete infrastructure device inventory in order to effectively manage the environment

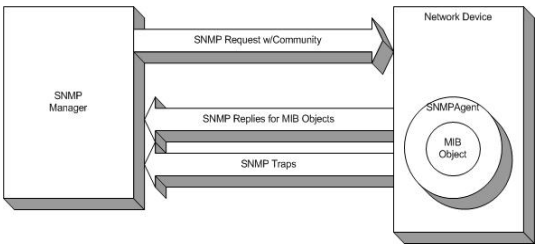
SNMP Protocols

• v1	RFCs 1155, 1157, 1212, 1213, 1215
• v2	RFCs 1441, 1445 – 1447, 1451, 1905 – 1907, 2578 – 2580,
• v2c	RFC1901
• v3	RFC2571 – RFC2576

SNMP

	Level	Auth	Encryption	What Happens
SNMPv1	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv2c	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv3	noAuthNoPriv	Username		Uses Username Match for Authentication
SNMPv3	authNoPriv	MD5 or SHA		Provides Authentication Based on HMAC- MD5 or HMAC-SHA Algorithms
SNMPv3	authPriv	MD5 or SHA	DES	Adds DES 56-Bit Encryption in Addition to Authentication Based on DES-56

SNMP Operations



Basic SNMP Operations

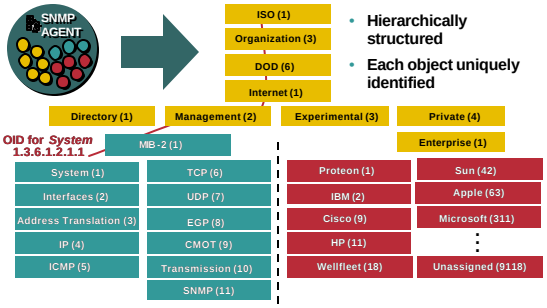
- **get request**
  - Reads a value from a specific variable.
- **getNext request**
  - Traverse information from a table of specific variables.
- **getBulk request (v2)**
- **get response**
  - Replies to a get or a set request.
- **set request**
  - Writes a value into a specific variable.
- **trap or notification**
  - A message initiated by the agent without requiring the management station to send a request.

MIBs: Management Information Bases

- A MIB defines the variables that reside in a managed node
  - Defined according to SMI (Structure of Management Information) rules
  - Each managed object is described using an object identifier defined in the SMI
- MIB I
  - 114 standard objects
  - Objects included are considered essential for either fault or configuration management
- MIB II
  - Extends MIB I
  - 185 objects defined
- Other standard MIBs
  - RMON, host, router, ...
- Proprietary vendor MIBs
  - Extensions to standard MIBs

1000s of Manageable Objects Defined Following Rules Set Out in the SMI Standards

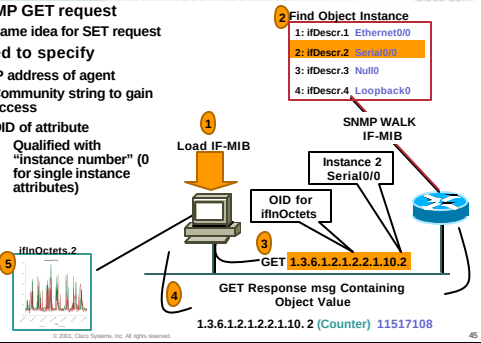
MIBs Object Identifiers



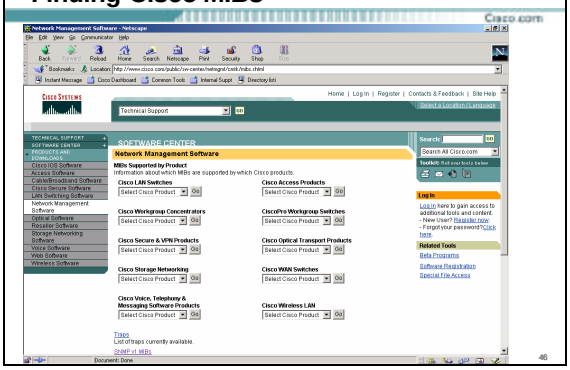
- Hierarchically structured
- Each object uniquely identified

Polling an Object

- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute
    - Qualified with "instance number" (0 for single instance attributes)



Finding Cisco MIBs



46

SNMP Configuration – Cisco Router

snmp-server community string [**view** ***view-name***] [**ro** | **rw**] [***number***]

snmp-server host host [**traps** | **informs**] [**version** {**1**| **2c**}] ***community-string*** [**udp-port** ***port***] [***notification-type***]

snmp-server enable traps [***notification-type***] [***notification-option***]

bgp, config, entity, envmon (voltage, shutdown, supply, fan, temperature), frame-relay, isdn (call-information, isdnu-interface), repeater (health, reset), rtr, snmp (authentication), syslog

Reference: http://www.cisco.com/univercd/cc/td/doc/product/iosfw/ios12.0/products_command_reference_chapter/06106c06000.html

47

SNMP Configuration – Catalyst Switch

set snmp community {**read-only** | **read-write** | **read-write-all**} [*community_string*]

set snmp trap {**enable** | **disable**} [**all** | **auth** | **bridge** | **chassis** | **config** | **entity**| **entityfru** | **envfan** | **envpower** | **envshutdown** | **ippermit** | **module** | **repeater** | **stpx** | **syslog** | **system** | **vmps** | **vtp**]

set snmp trap *rcvr_addr rcvr_community* [**port** *rcvr_port*] [**owner** *rcvr_owner*] [**index** *rcvr_index*]

If the traps aren't enabled, you're not going to get them!

Reference: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_1/cmd_ref/setsn_su.html

48

My Favorite SNMP Traps

Cisco.com

229 Traps defined in RFCs

- coldstart
- warmstart
- linkup
- linkdown
- frDLCIStatusChange
- newRoot
- topologyChange
- ospfIfStateChange
- ospfNbrStateChange

900 Traps defined for Cisco

- chassisAlarmOn
- ciscoEnvMonShutdownNotification
- ciscoEnvMonFanNotification
- ciscoEnvMonRedundantSupplyNotification
- ciscoEnvMonTemperatureNotification
- ciscoEnvMonVoltageNotification
- rttMonThresholdNotification
- rttMonTimeoutNotification
- sysConfigChangeTrap

1. Identify technologies and platforms in your network
2. Identify MIBs defined to manage them
3. Identify TRAPs defined in MIBs to monitor for

Syslog Overview

Cisco.com

- **Origin:** University of California
  Berkeley Software Distribution (BSD)
- Defined in Informational RFC 3164
- Format
  mm/dd/yyy:hh/mm/ss:facility-severity-MNEMONIC:description

  Example:
  Nov 23 12:37:37.713: %SYS-5-CONFIG_I: Configured from console by vty1 (172.18.86.76)

- Ported to various Unix and other operating systems, including Cisco IOS and Cisco Catalyst OS
- More syslog messages than SNMP Traps with a more verbose description of errors
- syslogd listens on UDP port 514

Syslog Error Messages

Cisco.com

syslog messages listed by facility

Syslog Configuration

Cisco.com

Logging severity level		<0-7>
emergencies	System is unusable	(severity=0)
alerts	Immediate action needed	(severity=1)
critical	Critical conditions	(severity=2)
errors	Error conditions	(severity=3)
warnings	Warning conditions	(severity=4)
notifications	Normal but significant conditions	(severity=5)
informational	Informational messages	(severity=6)
debugging	Debugging messages	(severity=7)

Syslog Configuration – Cisco IOS

Cisco.com

service timestamps	# add timestamps to log messages
logging <host>	# log messages to remote system
logging trap	# limit logging of messages sent to remote host based on severity
logging facility facility-type	# default local7
logging buffered [size|level]	# limits messages kept in internal buffer
logging console level	# limits messages logged to the console based on severity
logging monitor level	# limits logging of messages to terminal lines
logging [on|off]	# logging off will stop all logging processes
logging source interface type number	# specifies syslog packets contain IP Address of given interface

Reference: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a00800d9840.html

Syslog Configuration – Cisco CatOS

Cisco.com

set logging server enable|disable

set logging server < IP_Address>

set logging server <facility> <severity>

set logging server severity <severity>

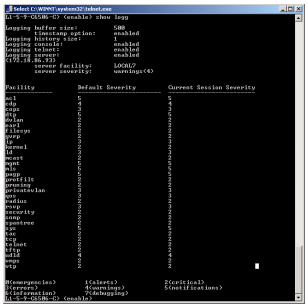
set logging console enable|disable

set logging level <facility> <severity>

set logging session enable|disable

set logging telnet enable|disable

set logging timestamp enable|disable



Reference: http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a008007f8ce.html

Syslog Message Examples

Error Message
%LINK-3-UPDOWN
: Interface [chars], changed state to [chars]
Explanation The interface hardware has gone either up or down.
Recommended Action If the state change was unexpected, confirm the configuration settings for the interface.

Error Message
%SYS-2-GETBUFFFAIL: [chars] buffer allocation ([dec] bytes) failed from [hex]
Explanation An operation could not be accomplished because of a low memory condition. The current system configuration, network environment, or possibly a software error might have exhausted or fragmented the router memory.
Recommended Action If the message recurs, copy the error message exactly as it appears on the console or in the system log, call your Cisco technical support representative, and provide the representative with the gathered information.

Syslog Error Message Decoder

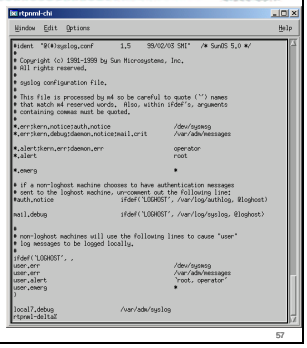
Reference: http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Syslog Server

- **syslog daemon (syslogd)**
- **syslog.conf file**

local7.info /var/log/syslog_info

- **man syslog.conf**



Syslog Analysis

- Need to use an application/script that summarizes syslog message data
- Review summarized message log daily
- Identify syslog messages that indicate action must be taken
- Investigate new messages not previously encountered
- Automate detection and notification of actionable syslog messages

Syslog Imbedded in SNMP

Configuration

logging history	# set level of messages to send to SNMP Manager
logging history size	# set size of syslog table buffer
snmp trap enable syslog	# enable syslog encapsulation in SNMP

- `syslog trap enable all` will enable syslog encapsulation !!
- syslog over SNMP is more processor overhead for the network device
- CISCO-SYSLOG-MIB clogMessageGenerated Trap

Processing clogMessageGenerated

1069607780 1 Sun Nov 23 12:16:20 2003 bxb25-adv-svcs-gw-sw.cisco.com - Received clogMessageGenerated from bxb25-adv-svcs-gw-sw.cisco.com (Enterprise : ciscoSyslogMIBNotificationPrefix , Event forwarded from : rtpnml-delta) at 12:16:20 on 11/23/03 with 5 parameters, Severity : Normal , Parameters : clogHistFacility=SYS, clogHistSeverity=warning, clogHistMsgName=SYS, clogHistMsgText=2003 Nov 23 09:05:33 %SYS-4-P2_WARN: 1/Tag 700 on packet from 00:05:00:96:64:1c port 2/10, but port's native vlan is 182, clogHistTimestamp=330992025;1 .1.3.6.1.4.1.9.9.41.2.0.1 0

- Many SNMP Managers do not process the content of an SNMP Trap but function against the unique trap identified or trap OID
- Therefore, many SNMP Managers will not correctly identify the message as being something other than a default, which in the example above is Normal !

Proactive Fault Management?

Cisco.com

Poll for …

- device cpu
- device memory
- link utilization
- link errors

Using …

- thresholds on SNMP Manager
- RMON Alarm & Events

How do you know what is Normal ??

Agenda

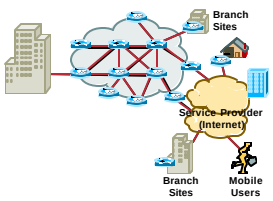
Cisco.com

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

Performance Management

Cisco.com

- Performance Management
  The configuration and measurement of network traffic for the purpose of providing a consistent and predictable level of service
- Why is it important?
  - Ensure network availability
  - Verify network performance
  - Verify QoS/CoS
  - Ensure SLA compliance



Performance Management

Cisco.com

- Understanding the behavior of a network and its elements in response to traffic demands
- Measuring and reporting on network performance so that performance can be maintained at an acceptable level
- Not real-time—near real-time for some applications
- Measurement examples: line utilization, link error rate, network throughput, throughput for QoS and CoS classes, user response times

Steps to performance management

Cisco.com

- Data collection
- Process and analyze data (baseline, report, capacity plan)
- Determining thresholds of acceptable performance

Performance Management Identifies:

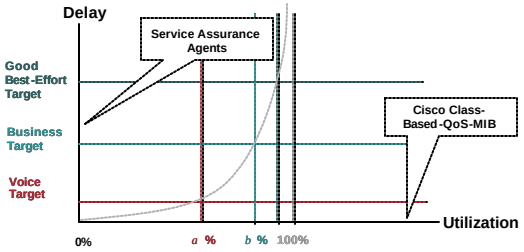
Cisco.com

- Normal baseline network performance
  - For comparing perceived 'bad' network behaviour
- Current or potential utilization problems
- Slow response time
- Application, server, and network availability
- Optimum data transfer times
- Violation of SLAs, QoS policies, or CoS guarantees

Monitoring QoS Networks

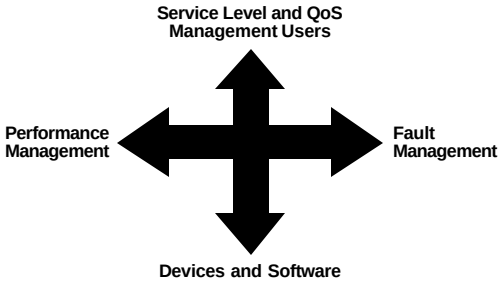
- **Myth**
  - Enabling QoS means that QoS will manage customer traffic so there is no need to monitor/or capacity plan service
  - The network will look after itself
- **Reality**
  - QoS makes networks more complex to manage
  - Requires performance management/capacity planning for each class of service

How to Make it Work in Theory? CoS: Delay/Utilization Trade-Off



If I can keep Voice traffic < *a* % , I will keep Voice delay under *M1* ms
If I can keep Business traffic < *b* % , I will keep Business delay under *M2* ms

Management Domain



Performance, Fault and Accounting Management Relationship

- All could use the same data source
- Processed and presented differently
- Interaction between all three
  - Performance management sends events to fault management, notifying it of performance related faults
  - Performance management can send events to accounting notifying it of SLA violations
  - Collection of performance, fault and accounting data can impact network performance and trigger faults

How Performance and Fault Management Intersect

- Proactive fault analysis is the conceptual area that ties together fault, performance and change management in an ideal network management system
- Processing performance data may uncover network faults
  - This may lead you to add event thresholds to more quickly report these issues
- Excessive or repeated faults may lead you to change what is being monitored for performance
  - Monitor additional objects and modify the thresholds of acceptable performance
- Real-time, as soon as a notification is generated

How Performance and Accounting Management Intersect

- Defining service, monitoring usage, reporting, and charging for services
- Processing performance data may uncover failure to deliver a service
  - This may lead to providing more tightly controlled SLA monitoring
  - Upgrading network, based on accounting and performance monitoring information
- Accounting data provides usage based information and user behaviour
  - Directs performance monitoring to key areas in the network
  - Modify thresholds of acceptable performance

How Performance and Configuration Management Intersect

- The network must be designed to make it manageable
- Dedicated management nets/VLANs
- Enable correct protocols and filter to only allow correct NM stations to use them
- Analysis may lead to changes in configs
- Ensure all protocols needed to manage the network are designed in
  - NTP
    - ensures time is consistent across all devices and management platforms
  - DNS
    - allows consistent use of names for devices instead of addresses

How Performance and Security Management Intersect

- Must consider security for performance management
  - Read -only access to all devices
  - Consider using SNMP views
- Denial of Service
  - Don't make performance data collection a DoS attack against the net…
- Security logs may be used during performance analysis
  - AAA records

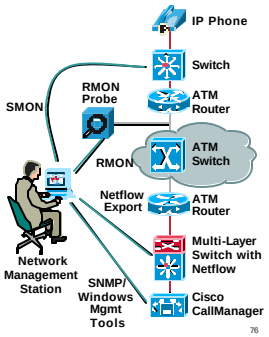
Measurement Strategies

Active	Sampling	Passive
Embedded	Source	External
Device/Link	Scope	End-to-End/Path
User	Perspective	Network

Sampling

Passive

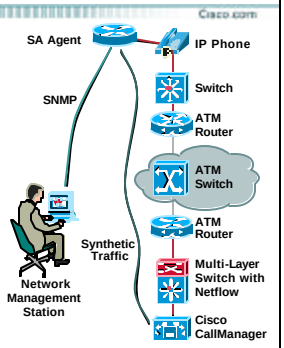
- **Definition**
  - Actual end-user network traffic where performance is measured by timing specific application traffic flows
- **Advantages**
  - Most accurate for live application traffic on a specified link
- **Disadvantages**
  - Limited to measuring:
    - Existing traffic types, which may not be present on the network at all times
    - Existing traffic patterns, which may not reflect patterns for new or future applications



Sampling

Active

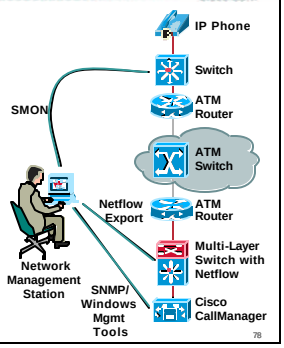
- **Definition**
  - Network traffic generated strictly for the purpose of measuring a network performance characteristic
- **Advantages**
  - Measures performance:
    - Between any two points in the network
    - Controllable, on a continuous basis
    - By traffic class based on IP Precedence marking
- **Disadvantages**
  - Only an approximation for performance of live traffic



Source

Embedded

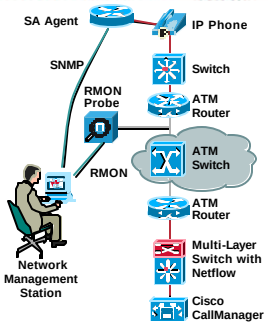
- **Definition**
  - Mechanisms for collection of network statistics are integrated into the network communication device (e.g., router or switch), itself
- **Advantages**
  - Follows network infrastructure
  - Gathers metrics that cannot be observed externally
- **Disadvantages**
  - Performance monitoring has device-level performance implications



Source

External

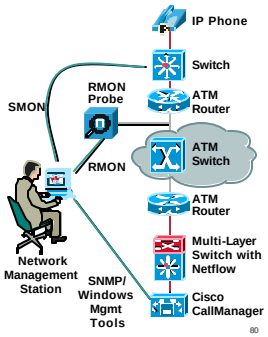
- **Definition**
  - Mechanisms for collection of network statistics are provided by a stand-alone device specifically designed to collect network performance statistics
- **Advantages**
  - Validation of performance performed independent of the devices that transmit network traffic
- **Disadvantages**
  - More hardware to administer
  - Observed statistics limited to points of deployment



Scope

Device or Link Oriented

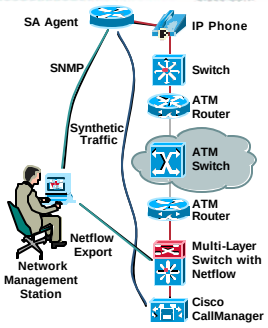
- **Definition**
  - Performance measurement based on analysis of specific device or device interface, and typically based on utilization rates
- **Advantages**
  - Detailed application performance monitoring of critical network links
- **Disadvantages**
  - When network-wide performance problems exist, how does one select which device or link to evaluate?



Scope

End-to-End

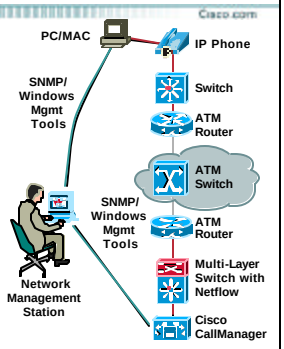
- **Definition**
  - Performance measurement based on analysis of response time across two or more network devices, and typically based on latency
- **Advantages**
  - Starting point performance troubleshooting
  - Reflects end-user experience
- **Disadvantages**
  - Prior knowledge of relevant end-to-end paths is needed



Perspective

User

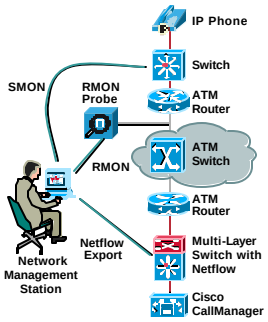
- **Definition**
  - Measurement based on performance statistics measured at the end-user workstation
- **Advantages**
  - Accurate measurement of end-user experience
- **Disadvantages**
  - Scale and distribution issues
  - Intrusive on the desktop



Perspective

Network

- **Definition**
  - Measurement based on performance statistics measured in network devices
- **Advantages**
  - Easy to deploy, and non-intrusive to the desktop
  - Identifies network performance issue
- **Disadvantages**
  - Imperfect understanding of end-user experience



Performance and Fault Management

- **Steps to effective management**
  - Baseline your network
  - Set thresholds
  - Monitor
  - Adjust as necessary

Critical Success Factors for Performance Management

Cisco.com

- Network baseline and application traffic baseline over a relatively long period of time to develop:
  - Network utilization trends, resource trends,
  - High growth, and shrinking utilization areas
- What-if analysis prior to deploying into the network
- Perform exception reporting for capacity issues:
  - CPU, memory, link utilization, etc.
- Analyze the capacity information
- Review baseline, exception, and capacity information on a periodic bases

Baseline Your Network

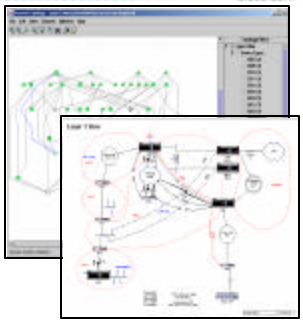
Cisco.com

- Gather device inventory information
  - Show version, show module, show run, show config all
- Gather statistics (device, network and service) at a given time
  - CPU, memory and link utilization, error rate, etc.
- Monitor statistics over time and study traffic flows
  - Show commands, SNMP, Cisco Service Assurance Agent (SAA), RMON, Netflow, NBAR

Baseline Your Network (Cont.)

Cisco.com

- Make a logical map of your network
- Know the protocols and traffic profiles that are running in your network
  - Routing protocols, VoIP, QoS, multicast, MPLS/VPN, ATM, Frame Relay, DLSW, web servers,…



Baseline Your Network—Documentation

- Document the physical and logical network
- Document detailed and measurable Service Level Agreements (SLA's)
- Have a list of the variables collected for the baseline
- Periodic meeting for review the analysis of the baseline
- Have a what-if analysis methodology documented, including modelling and verification
- Change control
  - All network modifications need to be documented and planned in advance whenever possible

Methods of Retrieving Performance Data

- Polling and events
  - SNMP
    - Most established and commonly used today
    - Well defined standards
  - Telnet, command line execution and screen scraping
    - Because data is not available in SNMP
    - No defined standards
- Data streaming
  - Netflow
  - FTP collection of call records

Performance Measurement Technologies

SNMP MIBs

MEASURES: CPU/Memory Utilization, Availability

Sampling:	Passive
Collection:	Embedded
Scope:	Device/Link
Perspective:	User/Network

Service Assurance Agent (SAA)

MEASURES: Latency And Jitter Between Source Router And Specified Target

Sampling:	Active
Collection:	Embedded
Scope:	Link/End-to-End
Perspective:	User/Network

RMON / ART MIB

Remote Monitoring / Application Response Time SNMP MIB s

MEASURES: Response Time Of Live Application Traffic To Server Device

Sampling:	Passive
Collection:	External Probe
Scope:	Link/End-to-End
Perspective:	User/Network

NetFlow

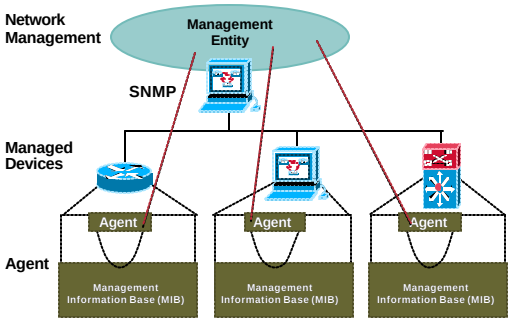
MEASURES: Device Interface Traffic Rate By S/D IP Address, Port Number Or AS

Sampling:	Passive
Collection:	Embedded
Scope:	Link/End-to-End
Perspective:	Network

Why SNMP?

- Most established and commonly used today
- Well defined method for extracting data from a device
- Almost all vendors support SNMP
  - Collect consistent data across the network from different platforms and vendors, by polling common objects
  - Example ifInOctets, ifOutOctets

SNMP Basic Components

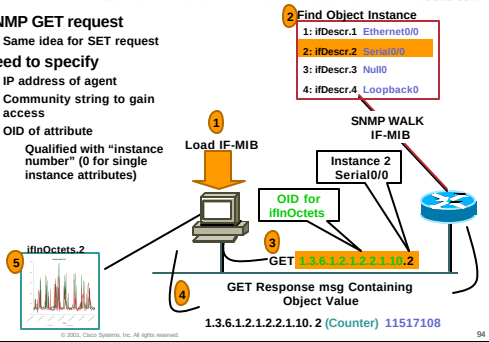


How to Poll

- Identify what objects need to be polled
  - Examples, Interface bytes, Interface packets, CPU utilization
- Load MIBs into the management station
  - So Management system knows how to poll the device
  - To provide human form
- Identify the object instance number
  - Example, for a device with multiple interfaces, each interface will have a unique index number
- Identify the object type
  - Counters require delta calculations to be meaningful
  - Gauges provide an absolute value

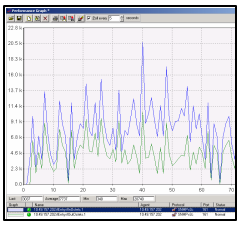
Polling an Object

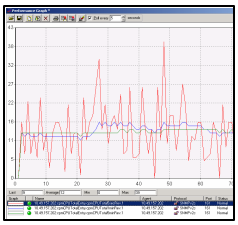
- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute
    - Qualified with "instance number" (0 for single instance attributes)



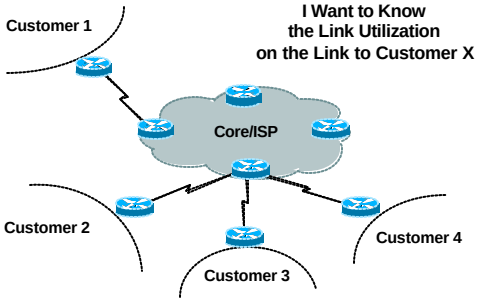
SNMP Basic Reporting

- Ethernet 0/0 5s polling interval
- ifInOctets.1 and ifOutOctets.1
- Counter32, plots are delta calculations
- CPU Utilization 5s Polling interval
- cpmCPUTotal5secRev.1
  cpmCPUTotal1minRev.1
  cpmCPUTotal5minRev.1
- Gauge32, plots are of CPU values





Case Study: Link Statistics



SNMP Interface Counters: Principles

- On all (sub)interfaces
- Both incoming and outgoing counters
- For every packet/byte per interface
  - Layer 3 traffic, layer 2 encapsulation, all layers retransmission and control traffic
- The counters will wrap up after some time; must choose an adequate polling interval
- Per RFC, the counters don't start necessarily at 0; a single value has no meaning, need the delta; per RFC, the SNMP counters can't be cleared
- On all the routers and switches
- Independent of the switching path

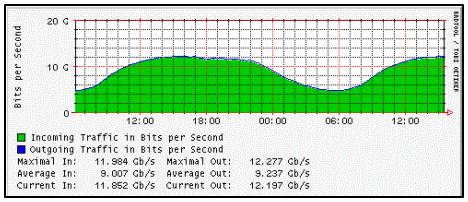
SNMP Interface Counters

- RFC2863, "Evolution of the Interfaces Group of MIB-II"
  - ifSpeed <= 20 Mbps
    - 32-bit byte and packet counters
  - ifSpeed > 20 Mbps and ifSpeed < 650 Mbps
    - 32-bit packet counters and 64-bit byte counters
  - ifSpeed >= 650 Mbps
    - 64-bit byte and packet counters
  - Implementations may provide additional counters, i.e. 64-bit byte counters for 10M interfaces

Example

..ifTable.ifEntry.ifInOctets

..ifTable.ifEntry.ifOutOctets

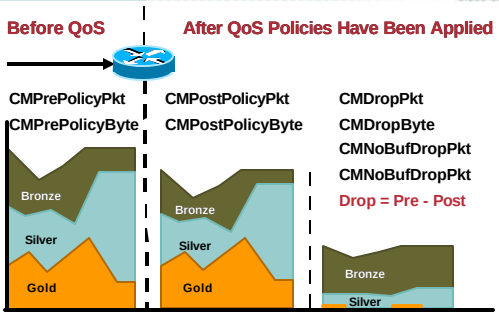


Some Specific Feature / Technology MIBs

- CISCO-CLASS-BASED-QOS MIB
- CISCO-CAR MIB
- CISCO-TCP MIB
- MPLS-TE MIB
- DOCSIS MIB
- Counters for Frame-Relay circuit (RFC1315)
- Counters for ATM connection
- Counters for DLSW circuit
- Etc…

CISCO-CLASS-BASED-QOS MIB

Class Map Stats Table (cbQosCMstats)



DOCSIS 1.1 MIBs

DOCSIS 1.1 SNMP Support in Cisco IOS® 12.1(7)CX:

- DOCS-QOS-MIB—Describes the quality of service (QoS) attributes
- DOCS-SUBMGT-MIB—Describes the subscriber management attributes
- DOCS-CABLE-DEVICE-MIB—Describes the operation of the CM and CMTS; Only the syslog and event tables are supported by this MIB, which was released as RFC2669
- DOCS-CABLE-DEVICE-TRAP-MIB—Defines the traps supported by CMs and the CMTS and is the extension of the RFC2669 (DOCS-CABLE-DEVICE-MIB)
- DOCS-IF-EXT-MIB—Extends the RFC2670 (DOCS-IF-MIB) to provide information about whether CMs and CMTS support DOCSIS 1.0 or DOCSIS 1.1

CMTS: Cable Spectrum Management for MCNS compliant Cable Modem Termination Systems

MPLS MIB Overview

- MPLS-LSR MIB
  - Mirrors the Label Forwarding Information Base (LFIB) for incoming and outgoing labels at an LSR, their associated parameters, accounting, and cross-connect table entries
- MPLS-TE MIB
  - Provides information about the traffic flows on MPLS traffic engineering tunnels
- MPLS-LDP MIB
  - Provides details about LDP (entities, peers, and sessions)
- MPLS-FTN MIB
  - Associate FEC with LSP (FEC-To-NHLFE, Next Hop Label Forwarding Entry)
- MPLS-VPN MIB
  - Supports monitoring and configuring BGP/MPLS VPNs

How to Find Out about a MIB Variable?

- Support list
  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- List of MIBS
  ftp://ftp.cisco.com/pub/mibs
- MIB locator
  http://tools.cisco.com/ITDIT/MIBS/servlet/index
- Object navigator
  http://www.cisco.com/cgi-bin/Support/Mibbrowser/unity.pl
- Non-Cisco tools
  http://www.mibdepot.com
  http://jaguar.ir.miami.edu/%7Emarcus/snmptrans.html

Other Useful MIB Links:

- IETF Operations and Management Area
  - http://www.ietf.org
  - http://www.rfc-editor.org
  - http://www.ops.ietf.org
  - Specific web site for O&M Index
- Bill Fenner's site
  - http://www.aciri.org/fenner/mibs/
- Cisco
  - http://www.cisco.com/go/mibs/
  - Cisco's MIBs
  - MIB locator: lists MIBs in image, or Platform+ release+feature set
  - SNMP Object Navigator: Search for MIB containing OID

SNMP Possible Applications

	SNMP
Network Monitoring	X
Network Planning	X
Security Analysis	
Application Monitoring	
User Monitoring	
Traffic Engineering	(X)
Peering Agreement	
Usage-Based Billing	(X)
Destination Sensitive Billing	

Performance Measurement Technologies

SNMP MIBs

MEASURES: CPU/Memory Utilization, Availability

Sampling: Passive
Collection: Embedded
Scope: Device/Link
Perspective: User/Network

Service Assurance Agent (SAA)

MEASURES: Latency And Jitter Between Source Router And Specified Target

Sampling: Active
Collection: Embedded
Scope: Link End-to-End
Perspective: User/Network

NetFlow

MEASURES: Device Interface Traffic Rate By S/D IP Address, Port Number Or AS

Sampling: Passive
Collection: Embedded
Scope: Link End-to-End
Perspective: Network

RMON/ART MIB

Remote Monitoring/Application Response Time SNMP MIBs

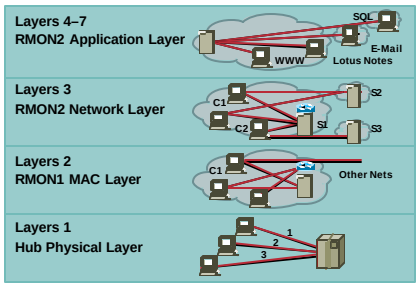
MEASURES: Response Time Of Live Application Traffic To Server Device

Sampling: Passive
Collection: External Probe
Scope: Link/End-to-End
Perspective: User/Network

Remote MONitoring (RMON) Background

- RMON is a set of standard MIBs
- RMON is based on IETF RFCs
- Analyzes every frame on a segment
- RMON1 is for data link layer
- RMON2 is for the network layer to application layer
- RMON2 supported on Network Analysis Module (NAM) for Catalyst 6000 and 5000

How does RMON Work?



RMON1 Groups (RFC 2819 and 1513)

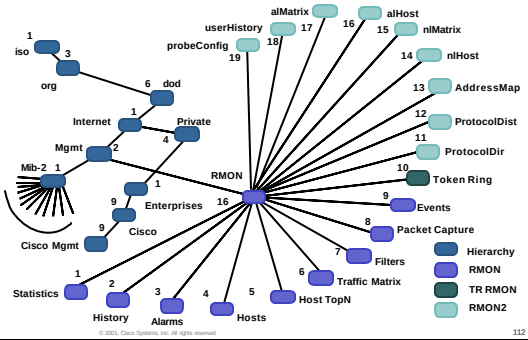
statistics	Real-Time—Current Statistics
history	Statistics over Time
alarm	Predetermined Threshold Watch
host	Tracks Individual Host Statistics
hostTopN	"N" Statistically Most Active Hosts
matrix	A < > B—Conversation Statistics
filters	Packet Structure and Content Matching
capture	Collection for Subsequent Analysis
event	Reaction to Predetermined Conditions
tokenRing	Token Ring—RMON Extensions

mini-RMON Groups

RMON2 Groups (RFC 2021)

protocolDir	Probe's Master List of Protocols
protocolDist	Segment Protocol Statistics
addressMap	Host-to-MAC Address Matching List
nlhost	Host In/Out—Network Layer Statistics
nlMatrix	A < > B3—Network Layer Statistics
alHost	Host In/Out—Application Layer Statistics
alMatrix	A < > B—Application Layer Statistics
usrHistory	Data Logging—User-Specified Variables
probeConfig	Probe Configuration Standards

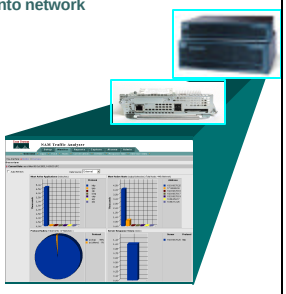
RMON Objects



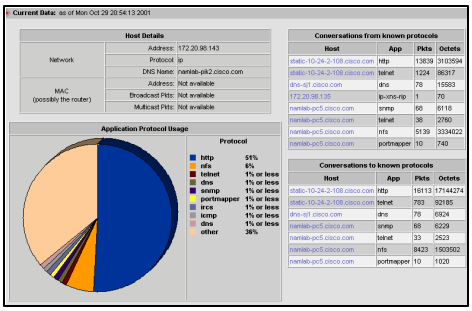
Cisco 2600/3660/3700 Series Network Analysis Module (NM-NAM)

Integrated traffic monitoring solution in branch routers to build application level visibility into network infrastructure

- **Leverages application SW from Cat6K NAM and Network Module HW used for CE, CIDS, etc. on 26/36/3700 Series Routers**
- **Extends standards based RMON2 and extended RMON traffic monitoring to edges of the network**
- **Embedded web based Traffic Analyzer similar to Cat6K NAM**
- **Much lower performance than Cat6K NAM and some impact on router performance**



Report Examples



Current Data: as of Mon Oct 29 20:54:13 2001

Host Details

Network	Address:	172.20.98.143
	Protocol:	ip
	DNS Name:	namlab-pix2.cisco.com
MAC (possibly the router)	Address:	Not available
	Broadcast Pkts:	Not available
	Multicast Pkts:	Not available

Application Protocol Usage

Protocol	
http	51%
nfs	6%
telnet	1% or less
dns	1% or less
snmp	1% or less
portmapper	1% or less
irc6	1% or less
icmp	1% or less
dns	1% or less
other	36%

Conversations from known protocols

Host	App	Pkts	Octets
static-10-24-2-108.cisco.com	http	13839	3103594
static-10-24-2-108.cisco.com	telnet	1224	86317
dns-sj1.cisco.com	dns	78	15583
172.20.98.135	ip-icmp-icmp	1	70
namlab-pc5.cisco.com	snmp	68	6118
namlab-pc5.cisco.com	telnet	38	2760
namlab-pc5.cisco.com	nfs	5139	3334022
namlab-pc5.cisco.com	portmapper	10	740

Conversations to known protocols

Host	App	Pkts	Octets
static-10-24-2-108.cisco.com	http	16113	17144274
static-10-24-2-108.cisco.com	telnet	783	92185
dns-sj1.cisco.com	dns	78	6924
namlab-pc5.cisco.com	snmp	68	6229
namlab-pc5.cisco.com	telnet	33	2523
namlab-pc5.cisco.com	nfs	8423	1503502
namlab-pc5.cisco.com	portmapper	10	1020

RMON Possible Applications

	RMON
Network Monitoring	X
Network Planning	X
Security Analysis	X
Application Monitoring	X
User Monitoring	X
Traffic Engineering	
Peering Agreement	
Usage-Based Billing	(X)
Destination Sensitive Billing	

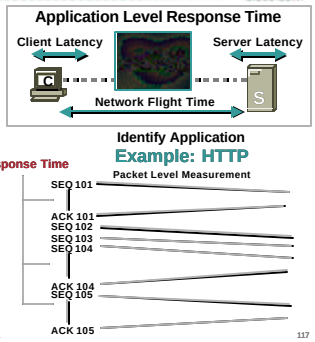
ART MIB Background

- Application Response Time (ART) MIB extends RMON2 standards
- Measures delays between request/response sequences in application flows e.g. http and ftp
- Supports any application that uses well-known TCP ports
- Probe is needed at both client and server ends with the ART software option enabled

How Does ART MIB Work?

- TCP protocols only
- Supported protocols include:

COMPUSRV	NNTP
DLSW_RD	NOTESTCP
DLSW_WR	ORACLSQL
DNS_TCP	REALAUD
FTP-CTRL	SMTP
FTP-DATA	SNA_TCP
HTTP	SOCKET
HTTPS	SQLNET_N
NB_DGM_T	SUNRPC_T
NB_NS_T	TELNET
NB_SSN_T	XWINDOW
NEWS_TCP	SCCP



Case Study 1.1
CPU Utilization—CLI Commands

- Routers running constantly at high utilization level can affect the overall performance of forwarding and processing packets

```
Router#sh proc cpu
CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Mgr
   2         368    274108          1  0.00%  0.00%  0.00%   0 Load Meter
   3       32940    716632         45  0.00%  0.00%  0.00%   0 OSPF Hello
Router#sh proc cpu sorted ?
  1min  Sort based on 1 minute utilization
  5min  Sort based on 5 minutes utilization
  5sec  Sort based on 5 seconds utilization
  |     Output modifiers
```


Case Study 1.2
CPU Utilization—SNMP

- CPU utilization using OLD-CISCO-CPU MIB
- Supported since 10.2
- As of 12.0 all OLD-CISCO-*-MIBs are "deprecated"

busyPer avgBusy1 avgBusy5

```
Router#sh proc cpu
CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Mgr
   2         368    274108          1  0.00%  0.00%  0.00%   0 Load Meter
   3       32940    716632         45  0.00%  0.00%  0.00%   0 OSPF Hello
```

- OLD-CISCO-CPU MIB only applies to RP CPU
- OLD-CISCO-CPU MIB doesn't apply to CPU utilization for VIP cards (7500) or LC (GSR)

Case Study 1.2
CPU Utilization—SNMP

- CISCO-PROCESS-MIB: New MIB introduced in 12.0T train; Provides information on CPU utilization and running processes

cpmCPUTotal5sec cpmCPUTotal1min cpmCPUTotal5min

```
Router#sh proc cpu
CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Mgr
   2         368    274108          1  0.00%  0.00%  0.00%   0 Load Meter
   3       32940    716632         45  0.00%  0.00%  0.00%   0 OSPF Hello
```

- Solution for VIP cards(7500) and LC(GSR):

  CISCO-PROCESS-MIB + ENTITY-MIB

- ENTITY-MIB is not supported in 12.0(T) train: Compatibility issue with the PROCESS MIB!

Case Study 1.3
CPU Utilization—SNMP for VIP and LC

- The ENTITY-MIB provides an inventory of the chassis, cpu card(s), line cards, fans, power supplies etc.; This MIB is the industry-standard replacement to the OLD-CISCO-CHASSIS-MIB
- Which MIB variables to use for VIP and LC?

```
cpmCPUTotalTable
    cpmCPUTotalIndex Unsigned32,
    cpmCPUTotalPhysicalIndex EntPhysicalIndexOrZero,
    cpmCPUTotal5sec Gauge32,
    cpmCPUTotal1min Gauge32,
    cpmCPUTotal5min Gauge32,
  INDEX { cpmCPUTotalIndex }
```

Assigned Arbitrarily And Is Not Saved Over Reboots

CISCO-PROCESS MIB

Defined In Another Variable entPhysicalEntry In the ENTITY-MIB

Case Study 1.3: CPU Utilization in VIP and LC ENTITY and CISCO-PROCESS MIBs Together

CISCO-PROCESS-MIB:

```
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotalPhysicalIndex.1 : INTEGER: 0
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotalPhysicalIndex.2 : INTEGER: 28
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5sec.1 : Gauge32: 12
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5sec.2 : Gauge32: 9
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal1min.1 : Gauge32: 10
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal1min.2 : Gauge32: 5
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5min.1 : Gauge32: 8
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5min.2 : Gauge32: 4
```

There are 2 CPUs displayed.

The second CPU is a VIP identified by an index number of 2.

Case Study 1.4
CPU Utilization—RMON

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

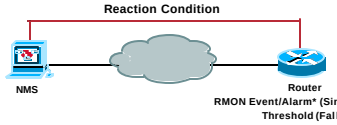
Rising Condition

Falling Condition

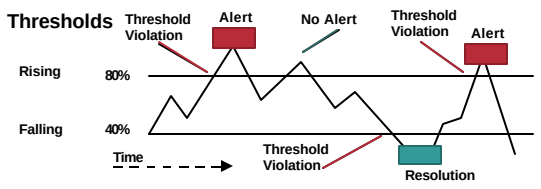
```
Router(config)#rmon alarm 1 cpmCPUTotalEntry.3.0 20 absolute
rising-threshold 80 1 falling-threshold 40 2 owner me

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

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



Case Study 1.4
CPU Utilization—RMON Reaction Condition



Performance Measurement Technologies

Service Assurance Agent (SA Agent)

MEASURES: Latency, Connectivity, Packet Loss, and Jitter Between Source Router And Specified Target

Sampling:	Active
Collection:	Embedded
Scope:	Link/End-to-End
Perspective:	User/Network

SNMP MIBs

MEASURES: CPU/MemoryUtilization, Availability

Sampling:	Passive
Collection:	Embedded
Scope:	Device/Link
Perspective:	User/Network

RMON / ART MIB

Remote Monitoring / Application Response Time SNMP MIB s

MEASURES: Response Time Of Live Application Traffic To Server Device

Sampling:	Passive
Collection:	External Probe
Scope:	Link/End-to-End
Perspective:	User/Network

NetFlow

MEASURES: Device Interface Traffic Rate By S/D IP Address, Port Number Or AS

Sampling:	Passive
Collection:	Embedded
Scope:	LinkEnd-to-End
Perspective:	Network

Historical Components of a Service Level Agreement

- Delay
- Jitter
- Bandwidth
- Availability/connectivity
- Packet loss
- Out of Sequence (OoS)
- [Add your favourite here]

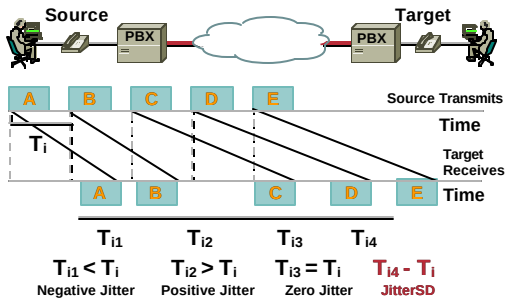
Latency (Delay)

- Propagation delay: the time it takes to the physical signal to traverse the path; (add 6 ns per meter for fibre, ie 36 ms for a transatlantic 6000 km link)
- Serialization delay is the time it takes to actually transmit the packet; depends on the bit-rate
- Queuing delay is the time a packet spends in router queues; depends on queue length and type
- Comfortable human-to-human audio is only possible for round-trip delays not greater than 100ms

Jitter

- This is the variation of the delay, a.k.a the 'latency variance,' can happen because:
- Variable queue length generates variable latencies
- Load balancing with unequal latency
- Harmless for many applications but real-time voice and video

Performance Measurements Network Delay Variation (Jitter)



Packet Loss

- Loss of one of more packets, can happen because…
- CRC error
- Full queue (tail drop) or out of contract
- Route change (temporary drop) or blackhole route (persistent drop)
- Interface or router down
- Misconfigured access-list
- …

Misordering [1/2]

- This is not a rare situation…
- According to a study, roughly 25% of the hosts monitored on the Internet exhibit reordering
- For the hosts that exhibited reordering on average 8 of the 50 packets were identified as being out of order

(Results Are Based on "Packet Reordering Is Not Pathological Network Behavior, Jon C. R. Bennett, Craig Partridge and Nicholas Shectman, IEEE/ACM Transactions on Networking, Vol. 7, No. 6, December 1999, p789")

Misordering [2/2]

- Out-of-order packet delivery, can happen because…
- Load balancing through multiple paths having different latencies
- Typically happening on parallel architectures (equivalent to multiple parallel routers)
- …

But Also…

- Packet alteration—the content is randomly modified
- Packet duplication—the same packet arrives multiple times (generally combined with misordering)

Current Solutions to Measure SLAs?

- Wait for problem to happen, and customer to complain
  - Reactive approach
- Manually
  - Monkey approach
- Custom, home-made application
  - The geeky approach
- Special hardware probes
  - The expensive approach

Current Solutions Drawbacks

- Requires additional hardware
- New software, protocols
- Additional configuration skills
- Eventually adding a new vendor, support contract…

The Idea behind SAA

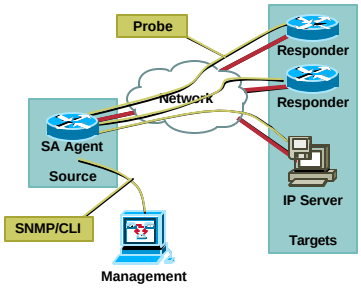
- If you have a running Cisco IOS router, turn it into a probing device
  - The smart approach
- Reuse your current equipment and enhance existing network management applications
  - (ex: CiscoWorks, VPNSC, Infovista, Concord eHealth, Agilent Firehunter…)

SA Agent Background on Cisco Routers

- Response Time Reporter (RTR):
  - Introduced in Cisco IOS 11.2
  - Uses the Response Time Monitoring (RTTMON) MIB
  - Monitor Round Trip Response Time (RTT)
- Service Assurance Agent (SA Agent):
  - New name since 12.0(5)T
  - Enhancement (notion of services)

Note: There Is No License Fee for the use of SAA

Global Architecture Overview



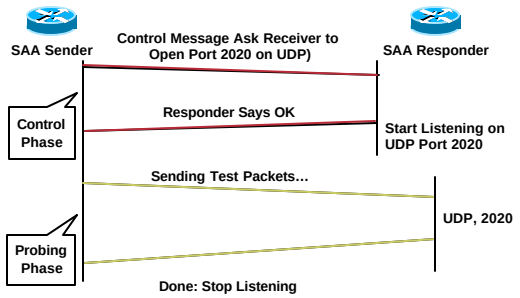
SAA Sender

- Cisco router a box that sends probes
- Where the probes are configured
- Where all the results are calculated and stored
- Target might be another Cisco device or another system like a server

SAA Responder

- Runs on Cisco router
- To activate, add `'rtr responder'` to the config, or set rttMonApplResponder.0=1 with SNMP
- Sender uses the SAA control protocol to communicate with responder before sending the test packets
- Responder knows the type of operation, the port used, the duration
- Communication on UDP 1967 and can be authenticated with MD5, not encrypted

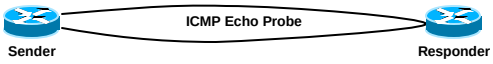
SAA Operation with Responder [1/2]



SAA Operation with Responder [2/2]

- The responder, based on the type of operation, may insert in/out timestamps in the packet's payload
- Processing time spend on the responder can therefore be calculated and deduced
- The response time is always calculated by the sender

SAA Accuracy…ICMP Echo Probe



(90% Process Load)

- With unloaded receiver, SAA measures 1.5 ms
- With high CPU load on the receiver: 45 ms!!

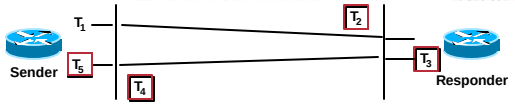
Any System Will Report Wrong Results when Too Much CPU Time Is Spent on the Receiver between the ICMP Echo Request and Echo Reply

Fortunately, We Have a Solution…

Processing Time Measurement

- When running the responder, we have a clear advantage, because…
- There is a mechanism to evaluate the processing time spend on the receiving router
- Insert a timestamp when the responder receives the packet, and when it replies
- Receive timestamp done at interrupt level, as soon as the packet is dequeued from the interface driver; absolute priority over everything else
- With SA Agent, this mechanism is implemented for both UDP Echo and UDP Jitter probes

UDP Echo Operation (w/SAA Responder)



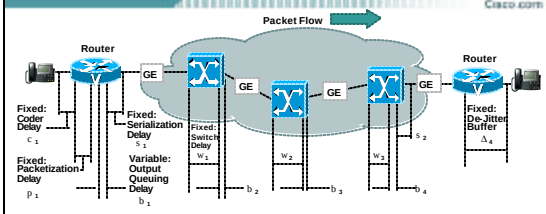
Processing Delay on the Source: Tps = T_5-T_4

Processing Delay on the Destination: Tpd = T_3-T_2

Round Trip Time Delay: T = [...] = T_2 - T_1 + T_4 - T_3

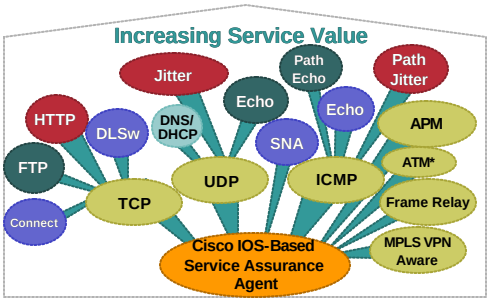
- We have no control on the queuing delay on the source and destination, but this is experienced by real traffic too, and must be accounted as such

Network Delay Variation
UDP Jitter SAA Operation Example



- Select the proper operation
- Select the proper test pair
- Select the proper payload, sampling interval, threshold

SA Agent Operations



*With Cisco IOS 12.2(11)T

SA Agent Highlights

- Provides real-time performance metrics
- Cisco feature available on most Cisco router platforms
- Proactive notification
- Integrates with many management applications

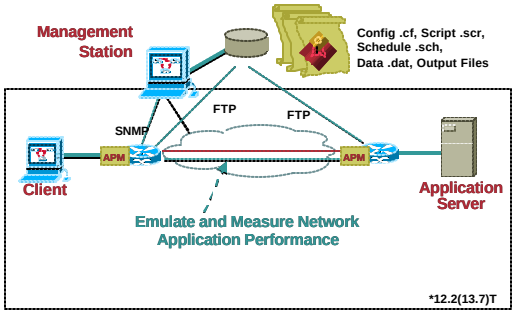
To Summarize…

- The network is like a live ecosystem
- There are harmless and harmful species living together
- They cannot always be under control
- But at least we can vigilantly observe what's going on

SA Agent Application Performance Monitor (APM)

- Emulates and measures performance of network applications
- TCL scripting language management interface
- Emulation scripts currently supported:
  - SMTP, POP3, IP/TV, LDAP, LotusSend, NNTP, PATTERN, and SAP
- Initially supporting measurements between two APM nodes
- Goal is to extend the measurements between APM node(s) into the real application server(s)

How APM Works?



Case Study 2.1— Device Availability PING from NMS

- Ping gives you availability details from your network management station

```
NMS% ping 1.1.1.1
1.1.1.1 is alive
```

Note: Only Target Device Is Involved

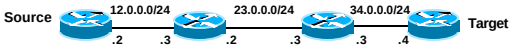
Case Study 2.1— Device Availability PING from NMS

- Ping gives you availability details from your network management station

```
NMS% ping 1.1.1.1
1.1.1.1 is alive
```

Note: Only Target Device Is Involved

Case Study 2.1—Device Availability Ping within the Network



- **Ping command successful only if:**

  The echo request gets to the destination, and the destination is able to get an echo reply back to the source

```
Source# debug ip packet IP packet debugging is on
Source# ping 34.0.0.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 34.0.0.4, timeout is 2 seconds:
5d21h: IP: s=12.0.0.1 (local), d=34.0.0.4, Len 100, unroutable. 5d21h:
IP: s=12.0.0.1 (local), d=34.0.0.4, Len 100, unroutable. 5d21h: IP:
s=12.0.0.1 (local), d=34.0.0.4, Len 100, unroutable. 5d21h: IP:
s=12.0.0.1 (local), d=34.0.0.4, Len 100, unroutable. 5d21h: IP:
s=12.0.0.1 (local), d=34.0.0.4, Len 100, unroutable. Success rate is 0
percent (0/5)
```


Case Study 2.1—Device Availability Ping within the Network—SNMP

ftp://ftp.cisco.com/pub/mibs/v2/CISCO-PING-MIB.my

destroy(6), creatAndWait(5), active(1)

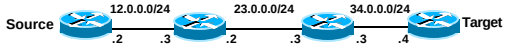
```
snmpset -c public Source ciscoPingEntryStatus.333 integer 6
snmpset -c public Source ciscoPingEntryStatus.333 integer 5
snmpset -c public Source ciscoPingEntryOwner.333 octetstring
  Owner_Name
snmpset -c public Source ciscoPingProtocol.333 integer 1
snmpset -c public Source ciscoPingAddress.333 octetstringhex ab447667
snmpset -c public Source ciscoPingPacketCount.333 integer 20
snmpset -c public Source ciscoPingEntryStatus.333 integer 1
snmpwalk -c public Source ciscoPingEntry
```

ip(1)

HEX

Row Created in Table

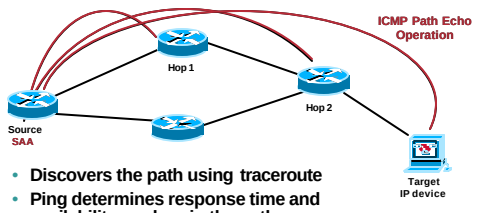
Case Study 2.2—Network Availability Traceroute Command




```
Source# traceroute 34.0.0.4
Type escape sequence to abort.
Tracing the route to 34.0.0.4
1 12.0.0.2 4 msec 4 msec 4 msec
2 23.0.0.3 20 msec 16 msec 16 msec
3 34.0.0.4 16 msec * 16 msec
5d01h: IP: s=12.0.0.1 (local), d=34.0.0.4 (Serial0/0), Len 28, sending
5d01h: UDP src=33976, DST=33434
5d01h: IP: s=12.0.0.2 (Serial0/0), d=12.0.0.1 (Serial0/0), Len 56, rcvd 3
5d01h: ICMP type=11, code=0
…
```

This is the first sequence of packets we send with a TTL=1. The first router, in this case Router2 (12.0.0.2), drops the packet and sends back to the source (12.0.0.1) a type=11 ICMP message. This corresponds to the Time Exceeded Message.

Case Study 2.2—Network Availability ICMP Path Echo SAA Operation



- Discovers the path using traceroute
- Ping determines response time and availability per hop in the path
- Options in IP packets: Loose Source Routing (LSR) and QoS (ToSbits)
- Isolates hop that causes the SLA violation

Case Study 2.2—Network Availability ICMP Path Echo SAA Operation Example

```
Source#
   rtr 1
     type pathEcho protocol ipIcmpEcho 10.0.0.1
     frequency 10
   rtr schedule 1 start-time now
```

IP address of the target device

Frequency in sec (default is 60)

Case Study 2.3 Service Availability

Two Levels of Availability:

- IP Connectivity
  - If the user can reach the IP end-point the service is available
  - Can be calculated using basic availability equation

$$\text{Availability} = 1 - \frac{\text{Probes with no Response}}{\text{Total Probes Sent}}$$

- Bounded IP Connectivity
  - The user can reach the IP end-point within some bounded criteria agreed upon between the Service Provider and customer
  - IP Connectivity is a requirement for Bounded IP Connectivity

Case Study 2.3
Service Availability Example

- SLA states response time must be within 200ms
- Network probe is an ICMP ping
- 10000 probes are sent between management system and managed device
- 1 probe fails to respond
- 9 probes have a response time >200ms

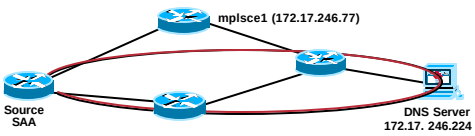
$$\text{IP Connectivity} = 1 - \frac{1}{10000} = 0.9999$$

$$\text{SLA Availability} = 1 - \frac{1+9}{10000} = 0.999$$

Case Study 2.3.1—Service Availability ART MIB

- Find out 'where' the application delays are occurring
  - Detailed data on request-response exchanges between clients and servers
- Server visibility
  - Monitor servers for protocols, application usage and top talkers

Case Study 2.3.2—Service Availability DNS Operation




```
Source#
      rtr 8
       type dns target-addr 172.17.246.77 name-server 172.17.246.224
      rtr schedule 8 start-time now
```

Source# RTR 8: Starting An Echo Operation - IP RTR Probe 8
2d03h: DNS Query return code: no error
2d03h: hostname = mplsce1.cisco.com
2d03h: responseTime = 5 (ms)

Performance Measurement Technologies

Cisco.com

SNMP MIBs

MEASURES: CPU/MemoryUtilization, Availability

Sampling:	Passive
Collection:	Embedded
Scope:	Device/Link
Perspective:	User/Network

Service Assurance Agent (SAA)

MEASURES: Latency And Jitter Between Source Router And Specified Target

Sampling:	Active
Collection:	Embedded
Scope:	LinkEnd-to-End
Perspective:	User/Network

RMON / ART MIB

Remote Monitoring / Application Response Time SNMP MIB s

MEASURES: Response Time Of Live Application Traffic To Server Device

Sampling:	Passive
Collection:	External Probe
Scope:	Link/End-to-End
Perspective:	User/Network

NetFlow

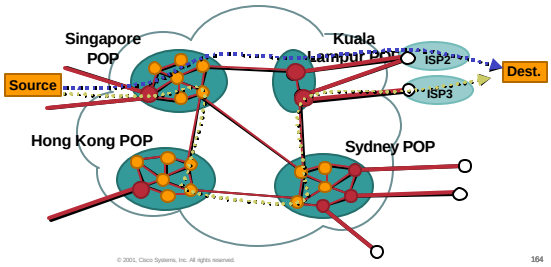
MEASURES: Device Interface Traffic Rate by S/D IP Address, Port Number or AS

Sampling:	Passive
Collection:	Embedded
Scope:	Link/End-to-End
Perspective:	Network

NetFlow Accounting—Why?
Network Design

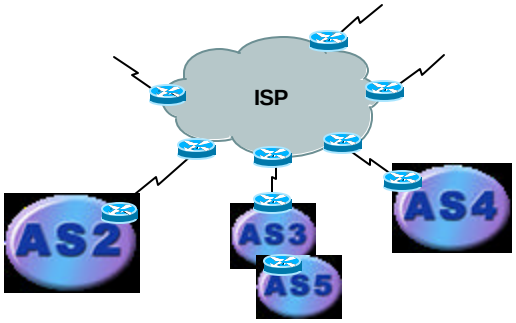
Cisco.com

- Capacity planning
- Traffic engineering



NetFlow Accounting—Why?
Peering Agreements

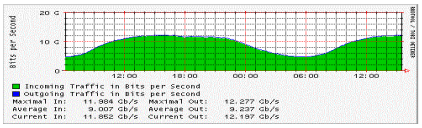
Cisco.com



What to Collect:
The Two Extremes...

Cisco.com

SNMP



NetFlow

- Usage — Packet count, Byte count
- Time of Day — Start sysUpTime, End sysUpTime
- Port Utilization — Input ifIndex, Output ifIndex
- QoS — Type of service, TCP flags, Protocol
- From/To — Source IP address, Destination IP address
- Application — Source TCP/UDP port, Destination TCP/UDP port
- Routing and Peering — Next hop address, Source AS number, Dest. AS number, Source prefix mask, Dest. prefix mask

NetFlow Background

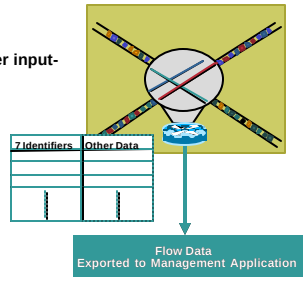
Cisco.com

- Who are my top N talkers? Which percentage?
- How many users are on the network at any given time? When will upgrades effect the least number of users?
- How long do my users surf?
- Are users staying within an acceptable usage policy?
- DOS/DDOS attack detections!
- NetFlow was originally started as a network accounting technology
- Traffic Engineering is now one of more popular NetFlow applications

How Does NetFlow Work?

Cisco.com

- Flows are unidirectional
- Flows are enabled on a per input-interface basis
- Flows are defined by 7 keys:
  - Source address
  - Destination address
  - Source port
  - Destination port
  - Layer 3 protocol
  - TOS byte (DSCP)
  - Input interface (ifIndex)



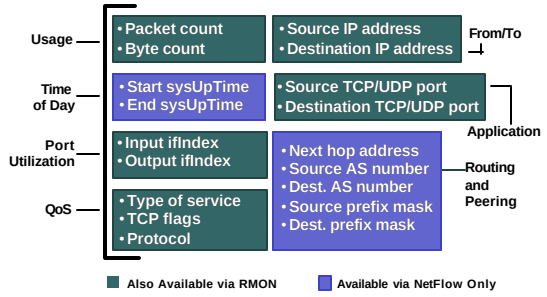
NetFlow: Principles

- Only for inbound traffic
- Unidirectional flow
- IP unicast only
- Transit traffic and traffic destined for the router is also accounted
- Work with CEF or fast switching; this is not a switching path
- On all interfaces
- Can only be enabled on the main interface; but returns the sub-interface in the flow record

NetFlow Versions

- Version 1—initial one
- Version 5—enhanced version 1
- Version 7—in connection with MultiLayer Switching (MLS)
- Version 8—router-based aggregation
- Version 9—flexible, extensible, and recently chosen as basis for IETF standard. Enables VPN-Aware Netflow.

Version 5: Flow Format



Version 5: Configuration

```
router (config-if)#ip route-cache flow
router (config)#ip flow-export destination
  172.17.246.225 9996
router (config)#ip flow-export version 5 <peer-as |
  origin-as>

Optional configuration
router (config)#ip flow-export source loopback 0
router (config)#ip flow-cache entries <1024-524288>
router (config)#ip flow-cache timeout …
```


NetFlow Performance Impact:

- CPU impact:
  - 10,000 active flows: < 4% of additional CPU utilization
  - 45,000 active flows: <12% of additional CPU utilization
  - 65,000 active flows: <16% of additional CPU utilization
- NetFlow data export (single/dual): No real impact
- NetFlow v5 vs. v8: Minimal to no impact at all
- NetFlow feature acceleration: >200 lines of ACLs
- NetFlow sampled NetFlow on the Cisco 12000: 23% vs. 3% (65,000 flows, 1:100)

What to Collect:
Full Collection vs. Sampling

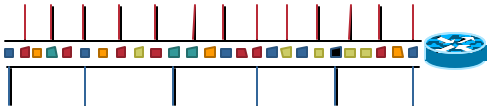
- Processing every packet might not scale up to very high-speed interfaces
- Amount of collected data might be huge
- It might take longer to process the data than to generate it ☹
- Network Management traffic might fully utilize the available bandwidth ☹ ☹
- Packet sampling can help to overcome those issues ☺

What to Collect:
1 in „n“ Sampling

Cisco.com

Sampling Interval: 1 in 2 Packets

Missed Flows: 1 out of 5 (15 %)



Sampling Interval: 1 in 5 Packets

Missed Flows: 2 out of 5 (35%)

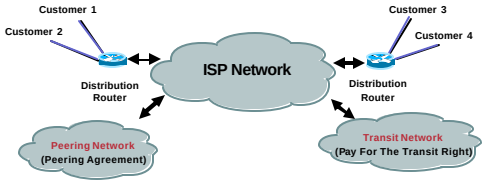
What to Collect:
Sampling Best Practices

Cisco.com

- Sampling for monitoring is fine
- Continuously sampling might be OK even for billing purposes
- Carefully determine the sampling rate
- Sampling algorithms:
  - 1 in n (deterministic, random, hash -based)
  - Filter, expressions
  - Time based
  - Trajectory sampling
- Sampling White Paper: work in progress

A Typical Service Provider Scenario

Cisco.com



Usage-Based Billing (Different Pricing for 6 Categories of Traffic):

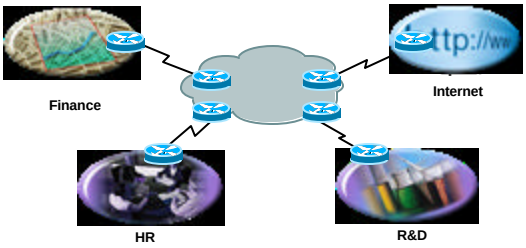
• Inbound on- net:	e.g. Customer1 receiving traffic from Customer3
• Inbound off-net (peering):	Customer1 receiving traffic from someone in peering network
• Inbound off-net (transit):	Customer1 receiving traffic from someone in transit network
• Outbound on-net:	Customer1 sending traffic to Customer3
• Outbound off-net (peering):	Customer1 sending traffic to someone in peering network
• Outbound off-net (transit):	Customer1 sending traffic to someone in transit network

A Typical Enterprise Scenario

Cisco.com

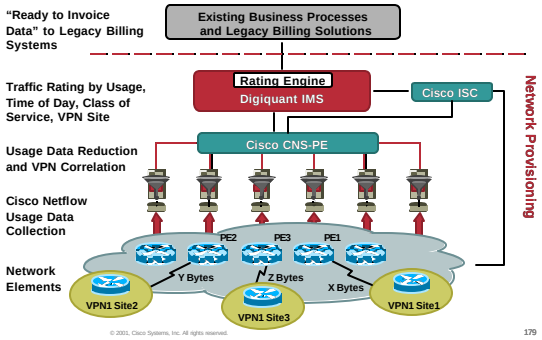
Account per Network (Rather than per IP Addresses)

Example: Charge the Department for the Cost of the Internet Link



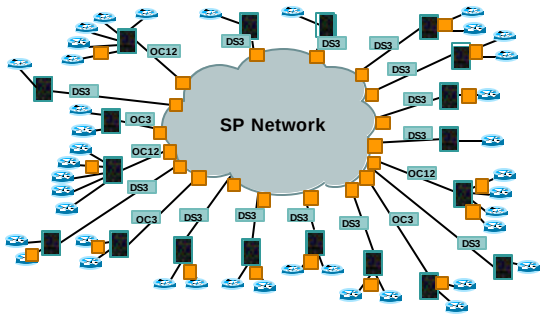
Per VPN Usage-Based Accounting Using CNS Performance Engine

Cisco.com



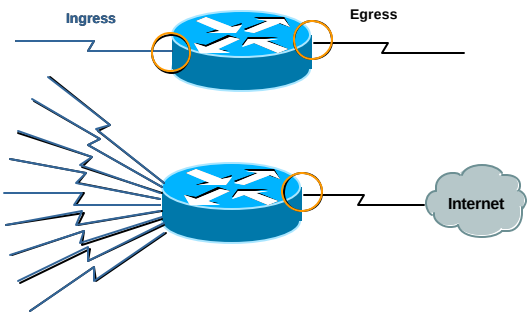
Where to Collect the Traffic: Integrated Functionality vs. External Devices

Cisco.com



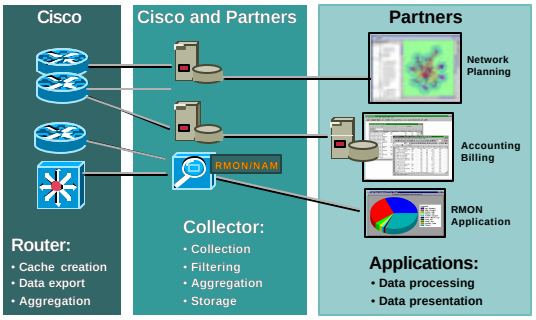
Presentation_ID.scr

Where to Collect the Traffic: Ingress vs. Egress



181

NetFlow Infrastructure



182

NetFlow Partners

183

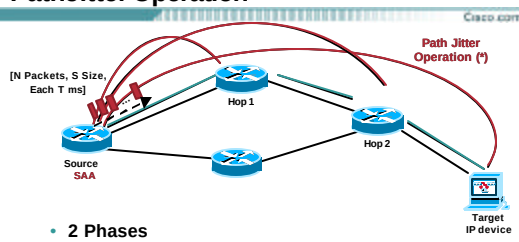
NetFlow Possible Applications

	NetFlow
Network Monitoring	X
Network Planning	X
Security Analysis	X
Application Monitoring	X
User Monitoring	X
Traffic Engineering	X
Peering Agreement	X
Usage-Based Billing	X
Destination Sensitive Billing	X

NetFlow Highlights

- Run on top of CEF or fast switching
- 7 flow identifiers
- For ingress traffic only
  (also traffic terminated on the router)
- IP only
- Previously only unicast, now with v9
  multicast traffic is also tracked

Case Study 3.1—Device Packet Loss PathJitter Operation



- 2 Phases
  - Discovers the path to target device using traceroute
  - Evaluates each hop one by one

(*) Requires Cisco IOS Version 12.2(2)T or Later

Case Study 3.1—Device Packet Loss PathJitter Operation (Cont.)

- Sends a specified number of packets to each hop along the traced path
  - Default values for all jitter operations:
    - N(number of packets) = 10, T(inter-packet delay) = 20ms, S(size) = 10 Bytes/packet
- Measures:
  - Per hop average response time delay
  - Per hop packet loss
  - Per hop cumulated jitter with noise reduction (RFC 1889)
- Use ICMP packet to measure jitter
- Specific to VoIP environment

(*) Requires Cisco IOS Version 12.2(2)T or Later

Case Study 3.1—Device Packet Loss PathJitter Operation Example

```
Source# sh rtr operational-state 2
---- Path Jitter Statistics ----

Source IP               - 172.17.246.5
Destination IP          - 172.17.246.20
Number of Echos         - 50
Interval between Echos  - 30 ms
Target Only             - Enabled (default)

Hop IP 172.17.246.2:
        RTT:1                PacketLoss:0          Jitter:0
        MinRTT:1             MaxRTT:2              SumRTT:19     Sum2RTT:37
        MinPosJitter:1       MaxPosJitter:1        SumPos:1      Sum2Pos:1
        MinNegJitter:0       MaxNegJitter:0        SumNeg:0      Sum2Neg:0
        OutOfSequence:0      DiscardedSamples:0
Hop IP 172.17.246.20:
        RTT:1                PacketLoss:0          Jitter:0
        MinRTT:1             MaxRTT:3              SumRTT:14     Sum2RTT:24
        MinPosJitter:2       MaxPosJitter:2        SumPos:2      Sum2Pos:4
        MinNegJitter:1       MaxNegJitter:1        SumNeg:2      Sum2Neg:2
        OutOfSequence:0      DiscardedSamples:0
```

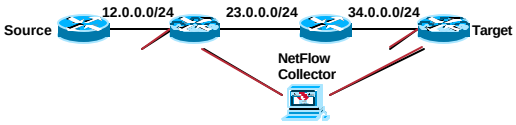
Σ Device PacketLoss = Network PacketLoss

For Hop 1

For Target

Case Study 3.2—Packet Loss NetFlow

- NetFlow will need external intelligence from NMS to calculate packet loss
- Enable NetFlow in input interfaces on strategic points in our network for a particular traffic flow
- Compare the exported flows in the NMS



Case Study 3.3
Service Packet Loss—NetFlow

```
Router2# sh ip cache verbose flow
IP packet size distribution (94452 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .199 .342 .300 .094 .028 .012 .005 .013 .000 .001 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 25322 added
  525430 ager polls, 0 flow alloc failures
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP              7       0.0         2    41      0.0       1.6       7.5
UDP-TFTP             1       0.0         1    67      0.0       0.0      15.1
UDP-other        19884       0.0         3   111      0.1       5.6      15.4
ICMP              5429       0.0         3    41      0.0       0.9      15.5
Total:           25321       0.0         3    97      0.2       4.6      15.4

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr ToS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Se0/1          12.0.0.1        Se0/0          34.0.0.2        11 00  10    5
00A1 /24 193                   C628 /0  0     0.0.0.0                84    39.7
```


Case Study 3.3
Device and Network Packet Loss—NetFlow

```
Router2# sh ip cache flow
IP packet size distribution (94442 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .199 .342 .300 .094 .028 .012 .005 .013 .000 .001 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  3 active, 65533 inactive, 25320 added
  525312 ager polls, 0 flow alloc failures
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP              7       0.0         2    41      0.0       1.6       7.5
UDP-TFTP             1       0.0         1    67      0.0       0.0      15.1
UDP-other        19880       0.0         3   111      0.1       5.6      15.4
ICMP              5429       0.0         3    41      0.0       0.9      15.5
Total:           25317       0.0         3    97      0.2       4.6      15.4

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Se0/0          12.0.0.1        Se0/1          34.0.0.2        11 C2E5 00A1    13
Se0/1          193.1.1.3       Se0/0          172.17.246.225  11 0 0A1 C2E5    13
Se0/1          193.1.1.3       Se0/0          172.17.246.228  11 0 0A1 C628     2
```


Agenda

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

Tools Issues

Cisco.com

What niches need to be filled?

Before we can talk about tools we have to understand a commonly used methodology called FCAPS

- **Fault**
- **Configuration**
- **Accounting**
- **Performance**
- **Security**

Tools Issues

Cisco.com

Fault Management

- **Fault Monitoring**
- **Fault Identification**
- **Fault Notification**
- **Fault Logging**
- **Fault Correlation**
- **Fault Diagnosis**
- **Fault Escalation**
- **Fault Resolution**

Tools Issues

Cisco.com

Configuration Management

- **Device Configuration Backup**
- **Configuration Comparison**
- **Global Configuration Changes**
- **Change Control - Moves, Adds, Changes**
- **Hardware Inventory**
- **Software Inventory (Image Management)**
- **Configuration Information**

Tools Issues

Cisco.com

Configuration Management

- Device Configuration Backup
- Configuration Comparison
- Global Configuration Changes
- Change Control - Moves, Adds, Changes
- Hardware Inventory
- Software Inventory (Image Management)
- Configuration Information

Tools Issues

Cisco.com

Accounting Management

- Some cross-over with performance
- Cost Control
- Charge Back – who is using the network

Tools Issues

Cisco.com

Performance Management

- Capacity Planning
- Availability / Response time
- Accuracy
- Throughput / Utilization
- Statistics trending
- Proactive alerts
- Statistics thresholding
- Device Health
- Link Health

Tools Issues

Cisco.com

Security Management

- Policy
- Authority
- Authentication
- Accountability
- Access Level
- Exceptions
- Logging

Network Management Tool Components

Cisco.com

Platform	The basic Network Management Tool -- performs auto-discovery, topology, basic configuration and information gathering.
Proactive Managers	Watches network devices for indications that the device or link is suspect.
Element Managers	Has detailed information about the network and the network elements.
Event Managers	Accepts, correlates and summarizes events from diverse systems. (Manager of Managers -- MoM)
Information	Provides general information about the network elements.

Network Management Components

Cisco.com

Software	Function	Type
IBM Tivoli NetView, HP OpenView, Aprisma Spectrum, CA Unicenter TNG, etc.	Reactive	Platform
Cisco Info Center / Micromuse Netcool	Reactive	Event Manager
CiscoWorks2000 RWAN – Routed WAN CiscoWorks2000 LMS – LAN Mgmt Solution	Operational Reactive	Element Manager Configuration Manager Information Event Manager (basic)
CiscoWorks2000 DFM – Device Fault Manager	Proactive	Element Manager
CiscoWorks2000 QPM - Quality of Service Policy Manager	Operational	Element Manager Configuration Manager
CiscoWorks 2000 CVM – Cisco Voice Manager	Operational	Element Manager Configuration Manager Event Manager (basic)

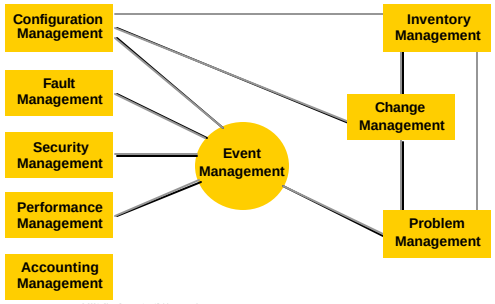
Network Management Components (cont'd)

Network Management Components

Software	Function	Type
Cisco Secure ACS – Access Control Server	Operational	Security/AAA Manager
Netflow Collector/ Analyzer	Proactive	Accounting/Performance Information
Concord eHealth Suite	Proactive Reactive	Performance
Visionael	Operational	Information

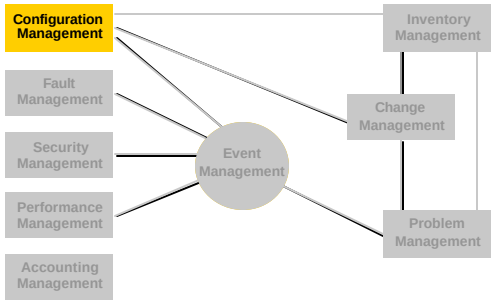
Tools Issues

What Tools To Use? Where Do They Fit?



Tools Issues

What Tools To Use? Where Do They Fit?



Configuration Management

Know the current configuration of all Cisco network devices.

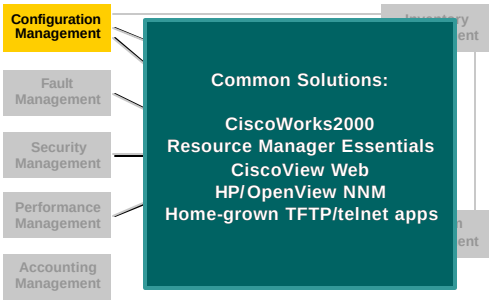
Identify, plan, and implement configuration changes as necessary.

Track all changes to device configurations.

Maintain history of device configurations.

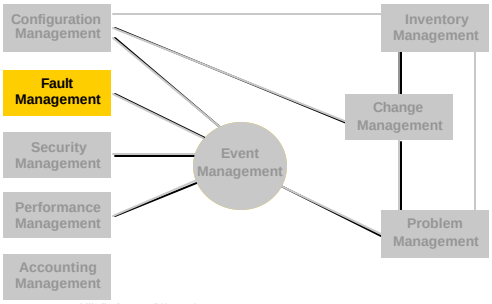
Tools Issues

What Tools To Use? Where Do They Fit?

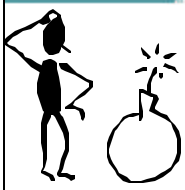


Tools Issues

What Tools To Use? Where Do They Fit?



Fault Management



Track errors and notifications sent from network devices.

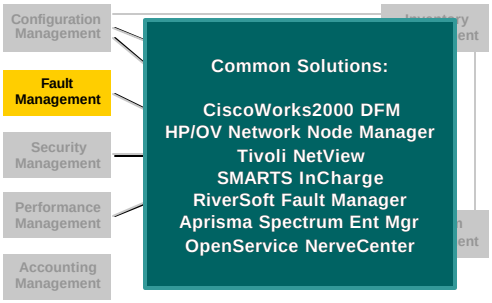
Know when the operation of a device changes or has reloaded.

Identify and resolve problems quickly.

Initiate action in response to critical errors.

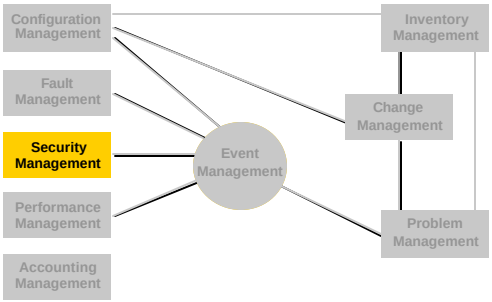
Tools Issues

What Tools To Use? Where Do They Fit?



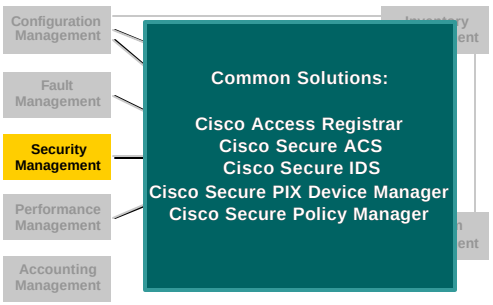
Tools Issues

What Tools To Use? Where Do They Fit?



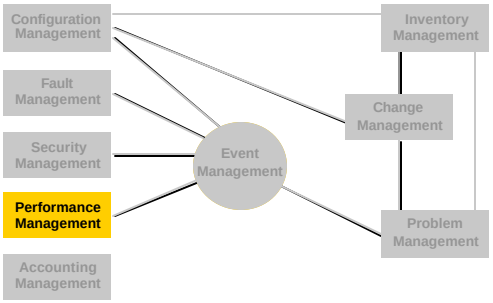
Tools Issues

What Tools To Use? Where Do They Fit?



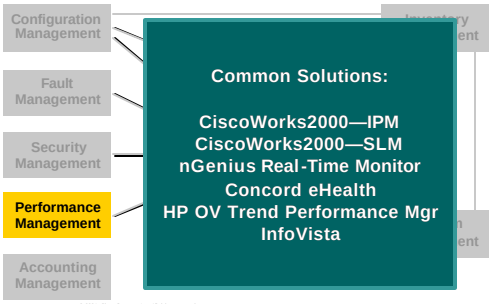
Tools Issues

What Tools To Use? Where Do They Fit?



Tools Issues

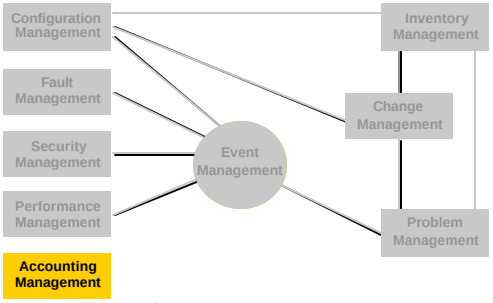
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

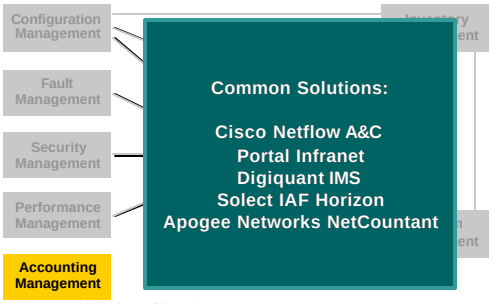
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

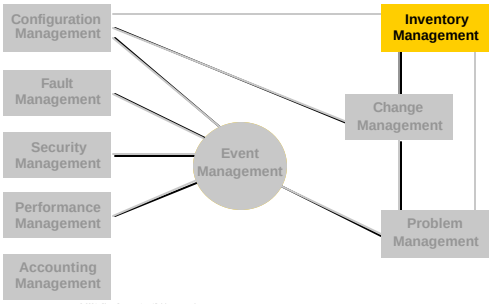
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

What Tools To Use? Where Do They Fit?



Inventory Management

Cisco.com

Know the number, type, and capacity of all devices running on the network.

Keep track of additions, deletions, and changes to network devices.

Maintain detailed device information, such as name, address, and interface settings.

Tools Issues

Cisco.com

What Tools To Use? Where Do They Fit?

Common Solutions:

CW2k Resource Mgr Essentials
Peregrine's Remedy Asset Management
Peregrine ServiceCenter
Peregrine AssetCenter
Cisco Network Designer (Netformx)
Visionael Studio

Inventory Management

Change Management

Problem Management

Management

Tools Issues

Cisco.com

What Tools To Use? Where Do They Fit?

Configuration Management

Fault Management

Security Management

Performance Management

Accounting Management

Event Management

Inventory Management

Change Management

Problem Management

Change Management

Cisco.com

Maintain history of all inventory, software, and device configuration changes.

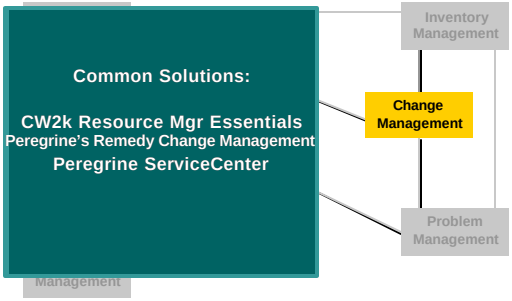
Know when a change is made, and who made it.

Identify source of problems quickly.

Tools Issues

Cisco.com

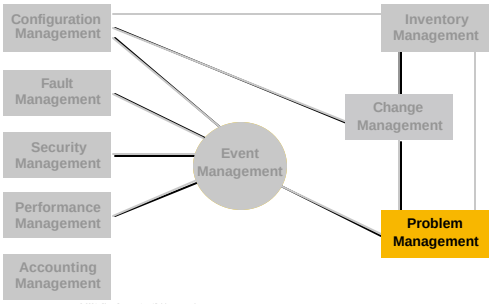
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

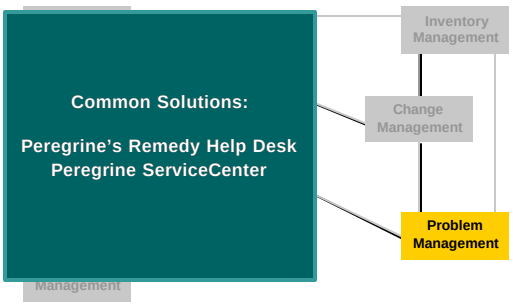
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

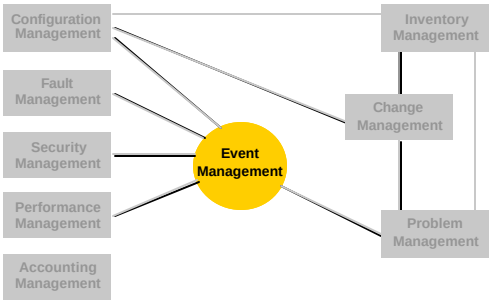
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

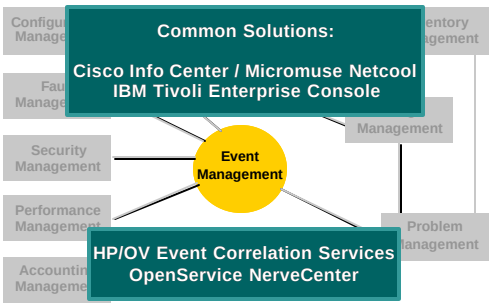
What Tools To Use? Where Do They Fit?



Tools Issues

Cisco.com

What Tools To Use? Where Do They Fit?



Tools Issues

- If I had to prioritize…
  - Availability - Device
  - Fault
  - Configuration
  - Availability – Path/Service (Problem)
  - Inventory
  - Performance
  - Security
  - Accounting

Tools Issues – Ease of Use

- An unfortunate reality of growing businesses is the lack of "Grade-A" operators
- Tools need to be easy to use or customizable to the extent that average users can be proficient—web interfaces seem to be popular and easy to use

Tools Issues – Ease of Use

- An unfortunate reality of growing businesses is the difficulty of KEEPING "Grade-A" operators
- Tools need to be easy to use or customizable to the extent that average users can be proficient—web interfaces seem to be popular and easy to use

Challenges of Large Network Management Environments

Cisco.com

Sharing Data/Integration

- Look for applications that share data via CIM/XML exchange
- At a minimum applications should export data in CSV format for import into other application
- Integrate menu picks to reduce "load-n-launch" syndrome
- Encourage vendors to integrate launch capabilities between apps—especially web-enabled ones

Tools Issues - Scaling

Cisco.com

- Separating by job function, network boundary, geographical area
- Some applications suites, like CiscoWorks 2000, are modular—separate the functions, if necessary

Tools Issues

Cisco.com

What Tools to Use?

	Application	Quantity
F C A P S	CiscoWorks2000 RWAN/LMS	1 per 2500 devices
F C A P S	CiscoWorks2000 DFM	1 per 30k ports
F C A P S	nGenius Real-Time Monitor	1 per 50 probes / 10k ports
F C A P S	CiscoSecure ACS NT: AAA/TACACS+	2
F C A P S	SNMP Platform: CIC, HP/OV NNM, Tivoli NetView, Aprisma Spectrum	Varies

Tools Issues

Cisco.com

What Tools to Use?

	Application	Quantity
F C A P S	Concord eHealth Suite	
F C A P S	Trouble-ticketing: Peregrine Remedy	1
F C A P S	Cisco Network Registrar (DNS)	2
F C A P S	NTP Server (C2500 or GPS)	2
F C A P S	SA Agent Source Router decommissioned C2500/C1601R	1
F C A P S	Network Doco: Visionael	1

Tools Issues

Cisco.com

What Tools to Use?

	Application	Quantity
F C A P S	Team Web Server: Apache	2
F C A P S	Team Disk Storage w/ Tape Backup	1
F C A P S	Portable Sniffers/RMON probes	2

Tools Issues - Applications

Cisco.com

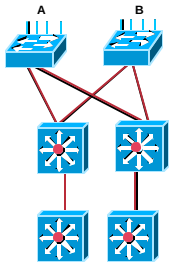
- Consider how your application scales when supporting large networks
- Distributed/Hierarchical?

Tools Issues – Inputs & Outputs

- Telnet/SSH (CLI)
- SNMP Gets/Sets
- SNMP responses
- SNMP notifications
- Syslog messages

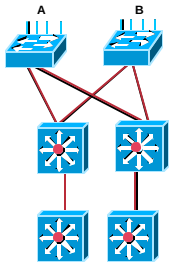
Sample NOC Net

- Dual DNS servers
- Dual NTP servers
- NM Servers
- Consoles
- Firewall/VPN connectivity
- Disk Storage
- Backup Services



Sample NOC Net

- Modems (OOB)
- Vendor Connectivity
- Security - AAA

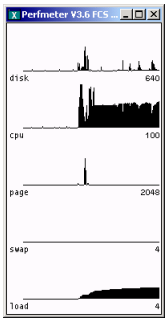


NM Hardware Platforms

Cisco.com

Effective Systems Monitoring

- AKA—How to know when you are running out of gas
  - CPU load
  - Memory utilization
  - Disk utilization
  - Interface utilization
  - SWAP utilization



Tools Issues – Distributed Architectures

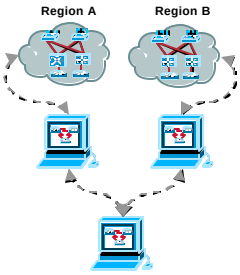
Cisco.com

- Not all applications are inherently hierarchical functional, i.e current generation of CW2000 suite:
- Cisco Info Center / Micromuse Netcool MUST be deployed hierarchically in most cases (I.e. Visionary!)

Tools Issues – Distributed Arch (cont'd)

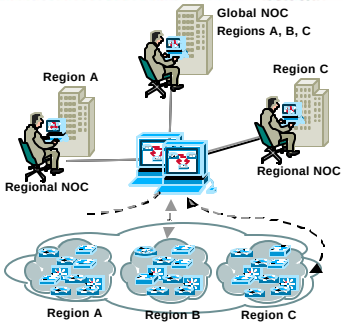
Cisco.com

- Great for scaling a truly large network architecture
- Be sure to periodically review the masks/rules that propagate regional events to the MoM
- Distributed NM Apps that can understand topology (esp L2) are unique
- Distributed event (textual exchange) seems more common



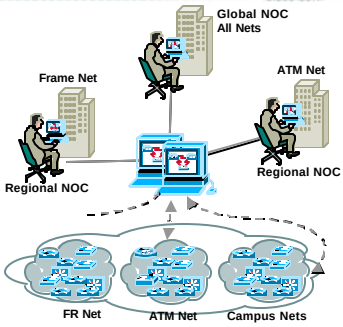
Tools Issues – Distributed Arch (cont'd)

- Partitioning across geographic administrative boundaries



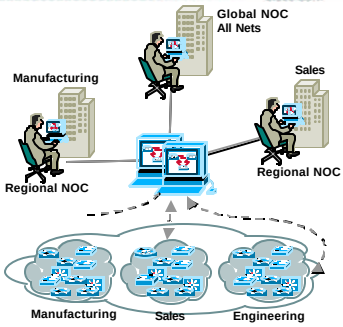
Tools Issues – Distributed Arch (cont'd)

- Partitioning across service boundaries



Tools Issues – Distributed Arch (cont'd)

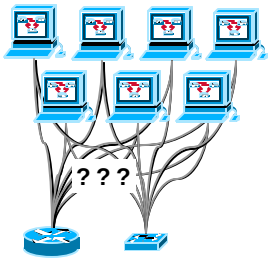
- Partitioning across functional boundaries



Tools Issues – Distributed Arch (cont'd)

Cisco.com

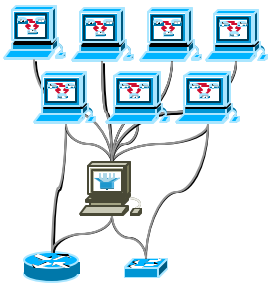
- What do we do with multiple trap and Syslog receivers??
- Example - Each event generates 1 x (# of trap/syslog receiver) messages (i.e. with 7 trap/syslog receiver— would generate 7|14 messages for one event
- We recommend no more than 4 trap and 4 syslog receivers defined in each device
- What do I do if I need more?



Tools Issues - Distributed Arch (cont'd)

Cisco.com

- Consider trap/Syslog repeaters and "switchboards"
- Excellent economies of scale and reduction in traffic if repeater is put close to NMS cluster
- Remember: eggs and baskets!



Tools are great…

But it's really about,

PEOPLE!

Challenges

Empowering

Teamwork

Agenda

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tools Issues
  - Applications
  - Servers
- People, Processes and Procedures
- Back to the Concept of the NOC

People Issues

- Organizational Alignments
- Staffing
- Shifts
- Training
- Career Progression
- Communication

Organizational Alignment

Cisco.com

- Engineering
- Operations
- Field Support (Remote Techs)
- Change Control
- Security
- Management/Supervisors

Organizational Models

Cisco.com

- How do we organize?
  - Geography
  - Business Function

Organizational Models – What Works

Cisco.com

- Keeping teams in close proximity
- Cross-training
- Open communication

Organizational Models – What Doesn't

Cisco.com

- Putting teams in different geographies with limited communication capabilities
- Allowing people to feel "silo'd" or "pigeon-holed" in a certain function
- Organizing by HR reporting structure

People Issues - Staffing

Cisco.com

Too few people =

staff burn-out =

fewer people =

ineffective staff

People Issues - Staffing

Cisco.com

- On-the-job-training is nice, but make sure the skills/capabilities fit the job
- Staffing levels are dictated by shift coverage
- Esprit de Corps

People Issues - Staffing

Cisco.com

- Can staffing be based on # of managed devices?
  - 1 Helpdesk - Level-1 operator per __X__ devices
  - 1 NOC / Level-2 operator per __Y__ devices
  - 1 Engineering / Level-3 per __Z__ devices
- Yes, but highly variable, possibly inefficient
- Determine the ratio for your situation and use that for future growth

People Issues - Staffing

Cisco.com

- Factors used to determine staffing for each support tier:
  - Devices per support engineer
  - Overall number of end-users supported
  - Number of company locations

People Issues - Staffing

Cisco.com

- Standardization of network environment
- Reduction of Network Environment Complexity
- Amount of automation deployed in the environment
- Number of systems and applications being used

People Issues - Shifts

Cisco.com

- Maintain knowledgeable people each shift
- Have someone authorized to make emergency changes on each shift
- Popular (effective?) to put less skilled operators on later shifts
  (i.e. run the low-impact batch updates)

People Issues - Shifts

Cisco.com

- Consider rotating Engineering/Ops folks for a week-long stint every quarter
  - Let Engineering see how manageable their designs are first hand!
  - Let Ops see the challenges of designing

Too bad we can't rotate management in!

People Issues - Shifts

Cisco.com

- Coverage periods? 5x9, 4x10, ????
- Su-Wed & Wed-Sat 10-hour shifts
- M-F 9-hour shifts, Sa-Su 2x12-hour shifts
  - Downside is the Sa-Su people are just "extras".
- Overlap shifts by an hour to do turn-over/hand-off processes
- To do 7x24 comfortably, you'll need 12 people and a supervisor at a minimum.

People Issues – Shifts & Tier Structure

Position	Responsibilities	Goal
Tier 1 / Helpdesk	• Full-Time Help Desk support • Answer support calls, open reactive trouble tickets and capture all pertinent info • Troubleshoot/triage problem for up to 15 minutes • Document ticket and escalate to appropriate tier 2 support	Resolve 30% of reported calls

People Issues – Shifts & Tier Structure

Position	Responsibilities	Goals
Tier 2 / NOC	• Network management station monitoring • Daily trouble-ticket review • Open proactive trouble-tickets for problems • Hands-on troubleshooting • Take calls from tier 1, vendor and tier 3 escalation • Retain overall ownership of issue until resolved • Ensure all network documentation up to date	Resolve 60% of reported calls

People Issues – Shifts & Tier Structure

Position	Responsibilities	Goals
Tier 3 / Engineering	• Provide immediate support to tier 2 for all priority 1 issues • Vendor escalation • Review performance data to proactively identify network faults and capacity planning • Agree to help with all problems unresolved by tier 2 within defined resolution periods • Chronic issue troubleshooting • Network design and planning • Root Cause analysis	Resolve all escalated and priority 1 issues

People Issues - Training

Cisco.com

- Balance training budget with employee longevity, commitment and responsibility
- Strive to make the training used ASAP
- Provide a training lab – don't use the production net for training!
- Engineering AND Operations need facilities for familiarization

People Issues – Career Progression

Cisco.com

- (Why is engineering considered "more prestigious?")
- Both Engineering and Operations require special skills
- Encourage certification
- Define a career path for your people!

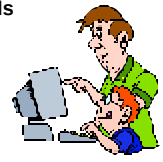
People Issues – Communication!

Cisco.com

- How do we keep the teams informed?

  Use Corporate Instant Messaging / Internal Internet Relay Chat (IRC)

  Interesting observation:
  IRC 'Bots used to answer FAQs or provide troubleshooting commands



People Issues – Communication!

Cisco.com

- How do we keep the teams informed?
  - Team Status Web-page
    - (In / Out, Vacation, TDA, training, etc)
  - Team Directories
    - (electronic, web-enabled & updated!)
  - Email Team Aliases
  - Epage Team Aliases

People Issues – Communication!

Cisco.com

- Video Monitors with Streaming Status Ticker
  - Pros: Effective and "cool demo" factor
  - Cons: Linear; have to wait for info that I care about to scroll
- Dynamic Network Status Page / Dashboard
  - Pros: Awesome "One View" to all status
    Nice executive overview
  - Cons: Few Commercial tools pull all the components together that you may want (Network Status, DHCP, DNS, Core Servers, etc, etc.)
    Usually requires customization
    (i.e. "The W word")

People Issues – Communication!

Cisco.com

- Network Status Dial-In Recording
  - Pros: Convenient
    Anyone can use
  - Cons: Tends to be updated less frequently than most people want
    Requires a speaker with excellent speaking skills
- Critical Events Phone Bridge
  - Run two bridges? One for management and one for troubleshooters
  - Keep both informed
  - Allow troubleshooters to work
  - Allow managers to manage/authorize

Agenda

Cisco.com

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tools Issues
  - Applications
  - Servers
- People, Processes and Procedures
- Back to the Concept of the NOC

Processes and Procedures

Cisco.com

Remember this?

> "First comes thought; then organization of that thought, into ideas and plans; then transformation of those plans into reality.
>
> The beginning, as you will observe, is in your imagination."

Napoleon Hill

Processes and Procedures

Cisco.com

Build a Priority/Severity Definition

Severity 1	Severity 2	Severity 3	Severity 4
Severe business impact	High business impact through loss or degradation, possible workaround exists	Some specific network functionality is lost or degraded such as loss of redundancy	A functional query or fault that has no business impact for the organization
• Major LAN or server segment down • Critical WAN site down • Critical Campus Site down	• Campus LAN down, notable number of users affected • Standard non-critical WAN site down • Critical performance impact	• Campus LAN performance impacted • LAN redundancy lost • Single user outage or service-affecting problem	• N/A

Processes and Procedures

Cisco.com

Priority/Severity – Tools perspective

Critical	An event which causes a major outage to most parts of the network
Alert	An event which causes a minor outage to certain parts of the network
Warning	An event which could potentially cause faults to the network if attention is not given
Error	An event which is erroneous, attention should be paid to ensure no further action is required
Informational	Purely informational

Processes and Procedures

Cisco.com

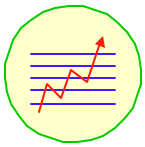
- Proactive Management is Problem Avoidance

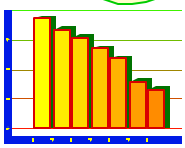
Link Congestion
Frame Relay Faults
Memory Utilization
CPU Utilization
Network congestion
Network overload
Broadcast storms
Buffering problems
Disk Utilization

Processes and Procedures

Cisco.com

Reporting – What's Needed?





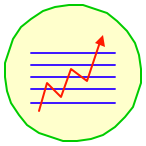
Daily/Weekly/Monthly:

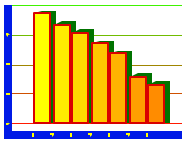
Top Issues List by Priority
Top Devices by CPU Utilization
Top Devices by Memory Utilization
Top Links by Utilization
Top Devices/Paths by Availability
Top Devices/Paths by Latency
Top Devices by Notifications/Syslog Priority
Top Devices by Notifications/Syslog Count
…

Processes and Procedures

Cisco.com

Reporting – What's Needed?





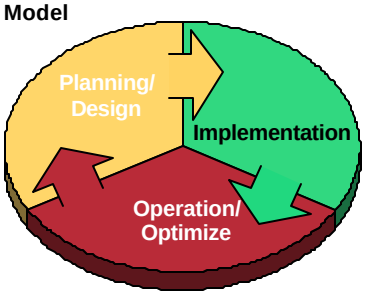
Daily/Weekly/Monthly:

Changes Per Device (historical)
Changes Per Device Type
Changes Per Software Image
Trouble-ticket volume
SNMP notification volume
Syslog event volume
Successful vs. Failed Changes
…

Processes and Procedures

Cisco.com

PDIO Model



Processes and Procedures

Cisco.com

- **Automate or drown!**
- **Manage by exception.**
- **If you don't use it don't install it.**

Processes and Procedures

Cisco.com

Develop Business Strategies and Policies

- Naming Standards
- Network Development Strategy
- Network Design Strategy
- Network Management Strategy
- Routing Strategy
- Testing Strategy

Processes and Procedures

Cisco.com

Develop Business Strategies and Policies

- Product Selection Strategy
- Internet Connection Strategy
- Network Software Strategy
- Disaster Recovery Strategy
- Change Management Policy
- Quality of Service Policy
- Security Policy
- Service Level Agreements

Processes and Procedures

Cisco.com

Sample Organizational Structure

DISA Information Systems Center (DISC)

www.disa.mil/disc/disc.html

Processes and Procedures

Cisco.com

Examples of Business Processes

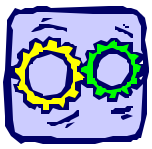
- New device process
- Escalation process
- Configuration change process
- Scheduled outage process

Processes and Procedures

Cisco.com

Business Policy Defines Requirements

Network management applications automate the control of business policies. The customization of any network management system requires the decision on a base set of policies and requirements.



Processes and Procedures

Cisco.com

Sample Security Management Policy

- Control the access to network devices to two levels of access for operators and engineers. The operational access will provide read only access while engineer access will provide change level access.
- SNMP access to the network devices should be limited with the use of access-lists on the community string and the use of non-standard SNMP community strings.

Processes and Procedures

Cisco.com

Sample Fault Management Policy

- The business requires the ability to be warned of an outage by collecting SNMP notifications and Syslog events.
- Fault summary reports will be collected daily to allow for systemic fault analysis.

Processes and Procedures

Cisco.com

Sample Performance Management Policy

- Monitor devices for utilization of internal resources including CPU, Memory, Interfaces and other device-specific performance indicators.
- Measure the application end-to-end performance by having the network management systems perform transactions across the network and provide reports on results.

Processes and Procedures

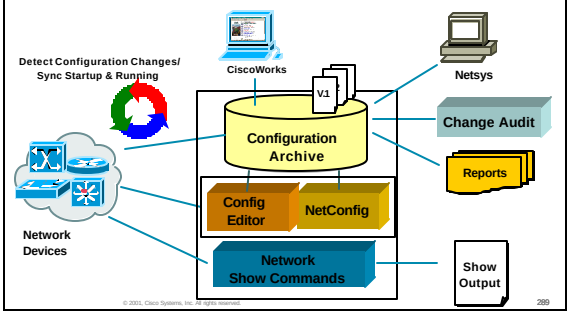
Cisco.com

Sample Configuration Management Policy

- Store details about device inventory, including serial numbers, part numbers, maintenance contracts, etc.
- Backup device configurations for fault restoration, offline viewing and network configuration rollback.
- Standardize device configurations for consistency and ease of maintenance.
- New devices will be loaded with an Engineering-certified image.

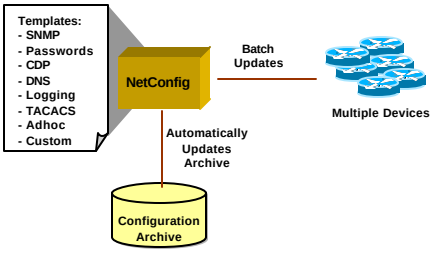
Processes and Procedures

RME Configuration Management work-flow



Processes and Procedures

RME NetConfig work-flow



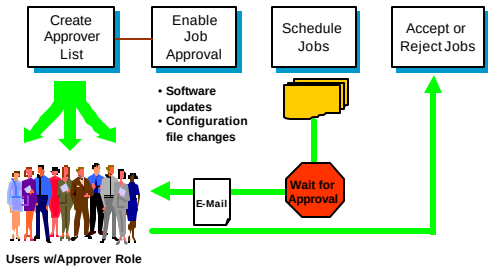
Processes and Procedures

Sample Change Management Policy

- Track and monitor changes to device and network configuration.
- Changes will be compared against Change Control documentation to validate authorized changes
- Maintenance windows will be…

Processes and Procedures

RME Job Approval work-flow

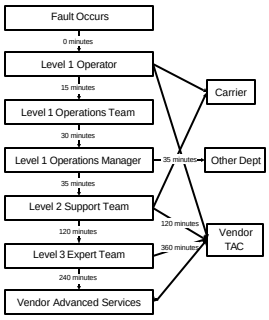


Processes and Procedures

Sample Accounting Management Policy

- Determine which users and business groups are using network resources by establishing application usage on the network.
- Ports are disabled until assigned to a business group.

Processes and Procedures



- Sample Escalation Policy
  - Event Arrives
  - Handled by Operator
  - Escalated to Team
  - Then Manager
  - Up to Level 2 support
  - Then to Experts
- Process should result in analysis of the root cause of the problem.

Processes and Procedures

Cisco.com

Document, Document, Document…

- Change Control
  - Move/Add/Change/Delete Documentation
  - Authorization flow
  - Maintenance Windows
  - Follow-up / Reporting
- Network documentation
  - L2/L3, physical/geographical, functional area/customer

Processes and Procedures

Cisco.com

- Escalation
  - Internal contacts / vendor contacts
- Vendor support documentation
  - Contact numbers
  - Contract / Entitlement Information

Processes and Procedures

Cisco.com

Working With the TAC

- Gather device hardware and software details
- Gather device configurations
- Gather device serial number and contract info
- Have someone knowledgeable with the device and the network involved in the case
- Make sure a remote access solution is in place for TAC or development to do more “hands-on” troubleshooting

Processes and Procedures

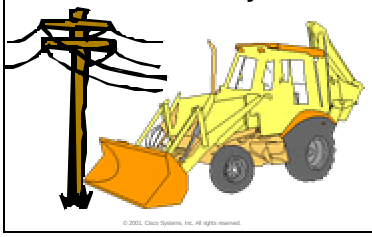
Cisco.com

- **Build Knowledge Databases**
  - Reuse existing knowledge
  - Reduce research on well-known issues
  - Some trouble-ticketing systems do this well
  - Document common troubleshooting techniques

Processes and Procedures

Cisco.com

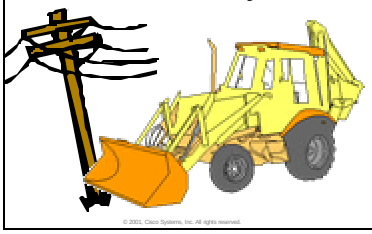
- **Employee Termination Procedures**
- **Disaster Recovery / "Business Continuity"**



Processes and Procedures

Cisco.com

- **Employee Termination Procedures**
- **Disaster Recovery / "Business Continuity"**



Processes and Procedures

Cisco.com

- Employee Termination Procedures
- Disaster Recovery / "Business Continuity"

Processes and Procedures

Cisco.com

- Redundancy/Back-up Verification
  - Dial-up Modems/ISDN work?
  - UPSes/Generators kicking in?
  - Batteries need replacing?
  - Tape Backups Valid?
  - Scheduled Network Redundancy Tests

Agenda

Cisco.com

- Availability Measurement and your business
- Overview of a NOC
- Network Management Framework
- Fault Management
- Performance Management
- Tool Issues
- People, Processes and Procedures
- Back to the Concept of the NOC

Scenarios

- Now that we have staff, processes and procedures, applications and servers let's brain-storm some scenarios – figure what might happen – how to use our tools and document the process for the NOC (think P&Ps!)

Scenario 1

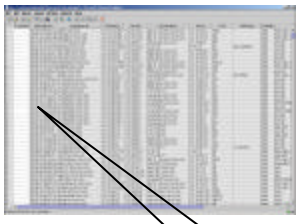
- Someone calls into the NOC:

"I just got a pop-up window on my screen saying 'MAC Address (so & so) has duplicated my IP Address'."

User

Scenario 1

- Trouble-ticket is logged
- Operator pulls up the CW2000 LMS application: Campus Manager User Tracking
- Initiates a search on the MAC Address

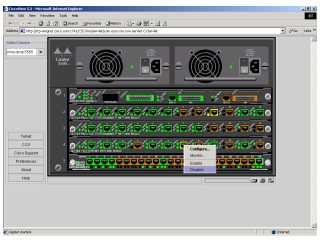


There's the Offender!!

Scenario 1

Cisco.com

- Time to use CiscoView Web or CLI to shut the port down!



Scenario 2

Cisco.com

- Someone calls into the NOC:

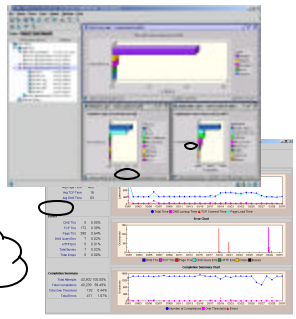
"I'm experiencing performance problems to the mail server."

User

Scenario 2

Cisco.com

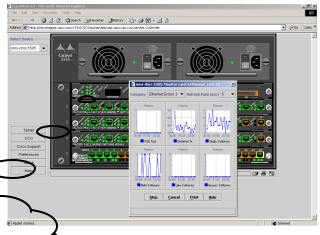
- Trouble-ticket is logged
- Operator pulls up Real-time stats with nGenius Real-Time Monitor, Concord eHealth or IPM



Hmm, network path seems OK – let's look closer at the user port

Scenario 2

- Used User Tracking to determine user port and switch
- Used CiscoView Web (or CLI) to look at port counters



Looks like an NIC issue…Reassign ticket to PC Support

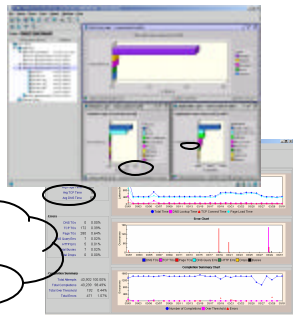
Scenario 3

- A NOC operator notices an event in Cisco Info Center:

> "A Cisco Info Center Internet Service Module says the web server latency is rising. We also got a notification from a router running Service Assurance Agent."
>
> NOC Operator

Scenario 3

- Proactive Time!
- IPM Hop-by-hop latency report is used to determine where the problem might be

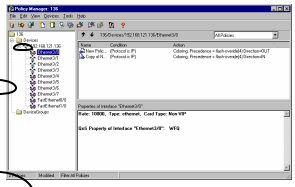


Hmm, IPM is telling me there is some latency. RTM is telling me there's a BUNCH of FTP traffic.

Scenario 3

Cisco.com

- Proactive Time!



Let's assign ticket to Engineering – they can use QPM to build a new QoS rule.

In Summary!

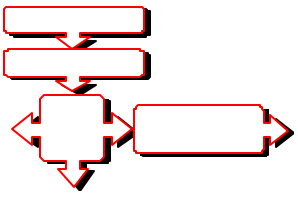
Cisco.com

- It's Mostly About PEOPLE!

In Summary!

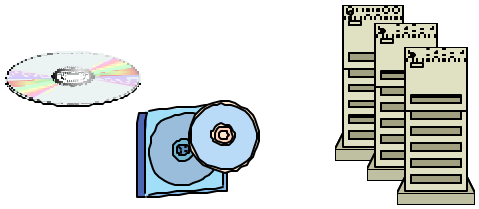
Cisco.com

- Complement with Processes and Procedures



In Summary!

- Follow-up with carefully selected tools



Recommended Reading

Performance and Fault Management
ISBN: 1-57870-180-5

The Art of Testing Network Systems
ISBN: 0-471-13223-3

Network Performance Baselining
ISBN: 1-57870-240-2

The Practical Performance Analyst
ISBN: 0-07-912946-3

Recommended Reading – cont'd

- The Visual Display of Quantitative Information by Edward Tufte (ISBN: 0-9613921-0)
- Practical Planning for Network Growth by John Blommers (ISBN: 0-13-206111-2)
- The Art of Computer Systems Performance Analysis by Raj Jain (ISBN: 0-421-50336-3)
- High Availability Network Fundamentals by Chris Oggerino (ISBN: 1-58713-017-3)
- Implementing Global Networked Systems Management: Stategies and Solutions by Raj Ananthanpillai (ISBN: 0-07-001601-1)
- Information Systems in Organizations: Improving Business Processes by Richard Maddison and Geoffrey Darnton (ISBN: 0-412-62530-X)
- Integrated Management of Networked Systems – Concepts, Architectures, and Their Operational Application by Hegering, Abeck, Neumair (ISBN: 1558605711)

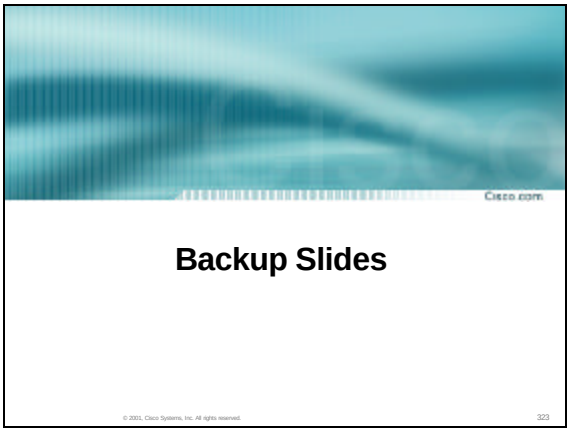
Appendix A: Acronyms - 1

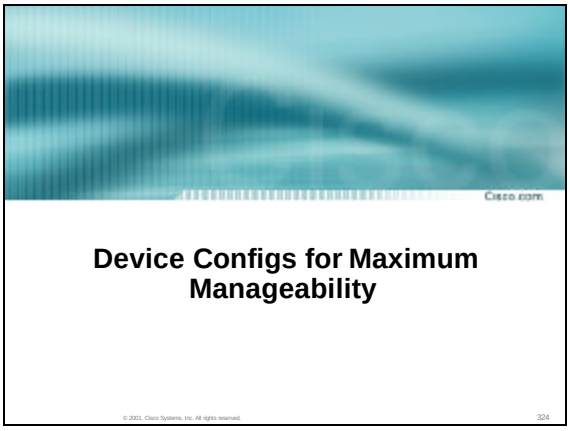
- AVG – Active Virtual Gateway (in GLBP)
- AVF – Active Virtual Forwarder (in GLBP)
- ADM – Add/ Drop Multiplexer
- APS – Automatic Protection Switching
- ATM – Asynchronous Transfer Mode
- CSM – Content Switching Module
- CSS – Content Services Switch
- DPM – Defects Per Million
- DPT – Dynamic Packet Transport
- DWDM – Dense Wave Division Multiplexing
- FCAPS – Fault, Config, Acct, Perf, Security
- FIB – Forwarding Information Base
- FRR – Fast Re-Route
- GE – Gigabit Ethernet
- GLBP – Gateway Load Balancing Protocol
- GR – Graceful Restart
- GSS – Global Site Selector
- HA – High Availability
- HDLC – High Level Data Link Control
- HSRP – Hot Standby Routing Protocol
- IKE – Internet Key Exchange
- IPM – Internet Performance Monitor
- IUM – Impacted User Minutes
- LC – Line Card
- LSP – Link State Path
- MAC – Media Access Control
- MARP – Multi-Access Reachability Protocol
- MIB – Management Information Base
- MLPPP – Multi-Link PPP
- MPLS – Multi-Protocol Label Switching
- MTBF – Mean Time Between Failure

Appendix A: Acronyms - 2

- MTTR – Mean Time to Repair
- NAT – Network Address Translation
- NIC – Network Interface Card
- NSF – Non Stop Forwarding
- PAT – Port Address Translation
- PAgP – Port Aggregation Protocol
- PPP – Point to Point Protocol
- PVF – Primary Virtual Forwarder (in GLBP)
- RFC – Request For Comments
- RME – Resource Manager Essentials
- RMON – Remote Monitor
- RPR – Resilient Packet Ring (L1/L2 resiliency technology)
- RPR, RPR+ - Cisco's Route Processor Redundancy (Device resiliency)
- RP – Route Processor
- RRI – Reverse Route Injection
- RU – Rack Unit
- SA Agent – Service Assurance Agent
- SLB – Server Load Balancing
- sNAT – Stateful Network Address Translation
- SNMP – Simple Network Management Protocol
- SPF – Single Point of Failure
  – Shortest Path First (in routing protocols)
- SSO – Stateful Switch Over
- SSP – State Synchronization Protocol
- SVF – Secondary Virtual Forwarder (in GLBP)
- TCP – Transmission Control Protocol
- UDLD – Uni-directional link detection Protocol
- VF – Virtual Forwarder (in GLBP)
- vIP – Virtual IP Address
- VPN – Virtual Private Network
- VRRP – Virtual Router Redundancy Protocol

Questions





Device Configs for Maximum Manageability

IOS 12.0 SNMP configuration example

Setting SNMP read-only and read-write community strings

Syntax:

snmp-server community *string* [view *view-name*] [ro | rw] [*number*]

```
RouterA(config)# snmp-server
community public ro
RouterA(config)# snmp-server
community private rw
```


Device Configs for Maximum Manageability

IOS 12.0 example

Use ACLs against SNMP community strings:

RO for NOC nets

RW for NMSs

Only devices on 192.168.1.0/24 can do snmpgets. Individual NM server are allowed snmpsets with the correct community string

Log violations

```
RouterA(config)# access-list 10 permit
192.168.1.0 0.0.0.255
RouterA(config)# access-list 10 deny any
log
RouterA(config)# access-list 11 permit
192.168.1.25
RouterA(config)# access-list 11 permit
192.168.1.26
RouterA(config)# access-list 11 deny any
log
RouterA(config)# snmp-server community
public RO 10
RouterA(config)# snmp-server community
private RW 11
```


Device Configs for Maximum Manageability

CatOS v5.5 SNMP configuration example

Setting SNMP read-only, read-write and read-write-all community strings

Syntax:

set snmp community {read-only | read-write | read-write-all} [*community_string*]

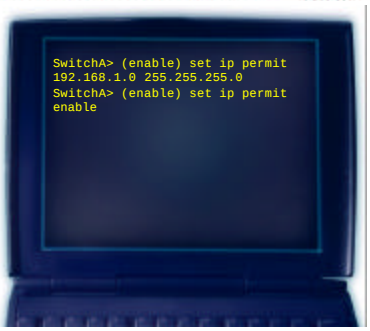
```
SwitchA> (enable) set snmp
community read-only public
SwitchA> (enable) set snmp
community read-write private
SwitchA> (enable) set snmp
community read-write-all secret
```

Device Configs for Maximum Manageability

CatOS v5.5

IP Permit list configured

Only devices on 192.168.1.0/24 can do snmpgets/sets with the correct community string and telnet to the switch



Device Configs for Maximum Manageability

SNMP Access

- An SNMP authenticationFailure trap can be generated and sent to the NMS console
- A Syslog event can be generated when logging level is set to “informational”

Device Configs for Maximum Manageability

SNMP Access

- Sometime we need to restrict access to certain MIBs
- Some NM apps poll IP route tables and ARP caches—this can cause high CPU load on low-end routers with many route entries
- Use “snmp-server view” statements

Device Configs for Maximum Manageability

'snmp-server view' example

If the router doesn't take the ipRouteTable MIB tree descriptor use 'ip.21'—for ipNetToMediaTable use 'ip.22'

```
RouterA(config)# snmp-server view
nopoll internet included
RouterA(config)# snmp-server view
nopoll ipRouteTable excluded
RouterA(config)# snmp-server view
nopoll at excluded
RouterA(config)# snmp-server view
nopoll ipNetToMediaTable excluded
RouterA(config)# snmp-server
community public view nopoll ro
```


Device Configs for Maximum Manageability

Cisco 2621 w/ 64MB RAM and 4000 routes (EIGRP)
snmpwalk would have run for 25 ½ minutes unrestricted

Device Configs for Maximum Manageability

IOS 12.0 SNMP Trap receiver configuration example

Syntax:

snmp-server enable traps [*notification-type*] [*notification-option*]

snmp-server host *host* [traps | informs] [version {1 | 2c}] *community-string* [udp-port *port*] [*notification-type*]

```
RouterA(config)# snmp-server enable
traps
RouterA(config)# snmp-server host
192.168.1.25 public
```

Device Configs for Maximum Manageability

Cisco.com

CatOS v5.5
SNMP Trap receiver configuration example

Syntax:

set snmp trap {enable | disable} [all | auth | bridge | chassis | config | entity | ippermit | module | repeater | stpx | syslog | vmps | vtp]

set snmp trap
rcvr_addr
rcvr_community

```
SwitchA> (enable) set snmp trap
enable all
SwitchA> (enable) set snmp trap
192.168.1.25 public
```


Device Configs for Maximum Manageability

Cisco.com

SNMP trap example from the NMS point of reference

```
988743703 1 Tue May 01 15:01:43
2001 172.18.87.125      -
Authentication Failure trap
received from enterprise
cisco.1.264 with 1 arguments:
authAddr=rtp-nsa-apps2;2
.1.3.6.1.6.3.1.1.5.5.1.3.6.1.4.1.9.
1.264 0
```


Device Configs for Maximum Manageability

Cisco.com

SNMP trap example

Without MIB loaded into NMS

```
988747160 2 Tue May 01 15:59:20 2001
192.168.100.5      - Received event
.1.3.6.1.4.1.9.9.43.2.0.1
(enterprise:.1.3.6.1.4.1.9.9.43.2
generic:6 specific:1), no format in
trapd.conf.   3 args:
 [1] private.enterprises.cisco.ciscoMgmt.
43.1.1.6.1.3.60 (Integer): 1
 [2] private.enterprises.cisco.ciscoMgmt.
43.1.1.6.1.4.60 (Integer): 2
 [3] private.enterprises.cisco.ciscoMgmt.
43.1.1.6.1.5.60 (Integer): 3;
1 .1.3.6.1.4.1.9.9.43.2.0.1 0
```

Device Configs for Maximum Manageability

Cisco.com

SNMP trap example

With MIB loaded into NMS

A little more clearer!

```
988754041 1 Tue May 01 17:54:01 2001
192.168.100.5      - ciscoConfigManEvent
received from enterprise
ciscoConfigManMIBNotificationPrefix  with
 3 arguments:
ccmHistoryEventCommandSource=commandLine;
ccmHistoryEventConfigSource=commandSource;
ccmHistoryEventConfigDestination=running;
1 .1.3.6.1.4.1.9.9.43.2.0.1 0
```


Device Configs for Maximum Manageability

Cisco.com

Syslog Messaging

(timestamps removed)

Format
%FACILITY[-SUBFACILITY]-SEVERITY-MNEMONIC: Message-text

Examples
%GSR_ENV-2-WARNING: Slot 7 MBUS_5V supply at 4984 mv < 5000 mv
%SYS-5-MOD_INSERT:Module 5 has been inserted

Device Configs for Maximum Manageability

Cisco.com

Syslog example

Some formats may vary

```
Apr 26 10:05:15 routera.cisco.com
150905: 14w6d: %GSR_ENV-2-WARNING:
Slot 7 MBUS_5V supply at 4984 mv <
5000 mv
Apr 26 10:07:04 routerb.cisco.com
106052: 12w0d: %BGP-3-NOTIFICATION:
sent to neighbor 10.10.128.200 4/0
(hold time expired) 0 bytes
Apr 26 10:07:10
[10.10.128.129.210.79] 994: 003921:
5d17h: %LINK-3-UPDOWN: Interface
GigabitEthernet1/1, changed state
to down
```

Device Configs for Maximum Manageability

IOS 12.0 Syslog configuration example

Syntax:

logging *host*

logging trap *level*

```
RouterA(config)# logging
192.168.1.25
RouterA(config)# logging trap
notifications
RouterA(config)# logging on
```


Device Configs for Maximum Manageability

CatOS v5.5 Syslog configuration example

Syntax:

set logging server *ip_addr*

set logging server {enable | disable}

```
SwitchA> (enable) set logging
server 192.168.1.25
SwitchA> (enable) set logging
server enable
```


Device Configs for Maximum Manageability

Setting logging history level to "notifications" is a good start

Set lower, to "informational" if you aren't getting the messages you need

Catalyst switches allow different levels for different categories —you can be very granular/specific about the categories that concern you

```
RouterA(config)# logging history
notifications
RouterA(config)# service timestamps
log datetime
```

Device Configs for Maximum Manageability

Cisco.com

Syslog Messaging

- Syslog messages go to a Syslog receiver
  - UNIX server —/var/adm/messages file
  - CiscoWorks 2000 Server (RME app)
- Notifications go to a trap receiver
  - HP/OV NNM, Tivoli Netview, CA Unicenter
  - CiscoWorks 2000 DFM
- Ideally we integrate these into a common Event monitor

Device Configs for Maximum Manageability

Cisco.com

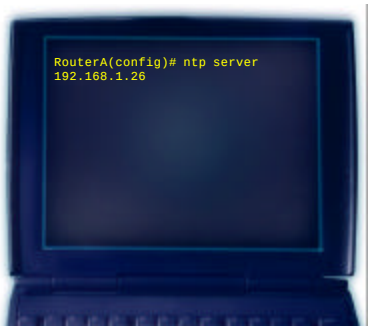
Optionally, we can encapsulate SYSLOG messages in traps

Device Configs for Maximum Manageability

Cisco.com

IOS 12.0 NTP configuration example

Syntax:
ntp server *ip-address* [version *number*] [key *keyid*] [*source interface*] [prefer]



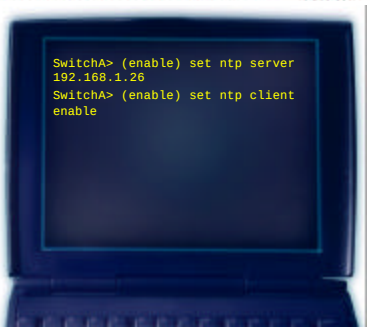
Device Configs for Maximum Manageability

Cisco.com

CatOS v5.5
NTP configuration example

Syntax:
set ntp server *ip_addr*

set ntp client {enable | disable}



Device Configs for Maximum Manageability

Cisco.com

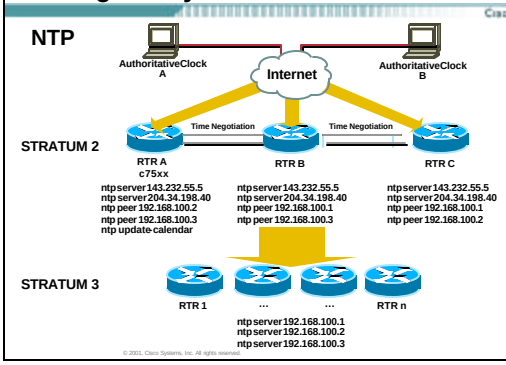
NTP

- **Use a minimum of two reference clocks (GPS and Internet derived are popular)—three recommended**
- **"Peer" time between the reference clocks**
- **If you have subnets of multiple NMSs and/or routers and switches consider using NTP in multicast mode**

Device Configs for Maximum Manageability

Cisco.com

NTP



Device Configs for Maximum Manageability

Cisco.com

AAA/TACACS+

- Authentication, Authorization, and Accounting
- TACACS+ available in routers and switches—allows for centralized username/password/priv administration
- Removes the requirement of having to config hundreds of routers/switches when a user leaves
- Allows for accountability when each user has their own login ID
- AAA implementation case study

www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/aaaisg/index.htm

Device Configs for Maximum Manageability

Cisco.com

IOS 12.0 AAA/TACACS+ configuration example

CiscoSecure ACS used to provide the service—user and TACACS+ key defined in its database

```
RouterA(config)# aaa authentication
login default group tacacs+
RouterA(config)# tacacs-server host
192.168.1.25 key cisconmcons
```


Device Configs for Maximum Manageability

Cisco.com

CatOS v5.5 AAA/TACAS+ configuration example

CiscoSecure ACS used to provide the service—user and TACACS+ key defined in its database

```
SwitchA> (enable) set tacacs server
192.168.1.25 primary
SwitchA> (enable) set tacacs key
cisconmcons
SwitchA> (enable) set
authentication login tacacs enable
all primary
SwitchA> (enable) set
authentication login local enable
all
SwitchA> (enable) set
authentication enable local enable
all
```

Device Configs for Maximum Manageability

IOS 12.0 example

AAA/TACACS+

Build in fallback accounts in case AAA is down

```
RouterA(config)# aaa new-model
RouterA(config)# aaa authentication
login default group tacacs+ local
RouterA(config)# username fallback
password 0 aaa-is-down
RouterA(config)# ip tacacs source-
interface Loopback0
RouterA(config)# tacacs-server host
172.18.86.69
RouterA(config)# tacacs-server key
cisconmcons
```


Device Configs for Maximum Manageability

- Fallback to local user accounts or local enable password??
- Local

  Be aware that "password 7" entries are not highly secure. If the configuration file is compromised someone could use a password cracking utility to derive the password. Additionally, when AAA is down the login prompt is still "Username: / Password:"—you can't tell if AAA/TACACS+ service is down
- Enable

  You know when AAA/TACACS+ is down because the login prompt will be "Password:". Enable secret passwords are more secure. However, you probably won't tell all your NOC personnel the enable secret password in the off-chance that AAA/TACACS+ is down

Device Configs for Maximum Manageability

Other NM config statements

IOS 12.0 example

Interface and controller descriptions

Syntax:
description *string*

```
RouterA(config)# interface serial 0
RouterA(config-if)# description
128k FR : BobNet : CktID 123456
RouterA(config)# controller t1 4/0
RouterA(config-controller)#
description 3174 controller for
test lab
```

Device Configs for Maximum Manageability

Other NM config statements

IOS 12.0 example

SNMP MIB2 settings

Syntax:

snmp-server contact *string*

snmp-server location *string*

snmp-server chassis-id *string*

```
RouterA(config)# snmp-server
contact Cisco NOC : 888-555-1234
RouterA(config)# snmp-server
location Site 10 : Bldg 5 : Rack 5c
RouterA(config)# snmp-server
chassis-id 123F456G
```


Device Configs for Maximum Manageability

Other NM config statements

CatOS v5.5 example

SNMP MIB2 settings

Syntax:

set system contact [*contact_string*]

set system location [*location_string*]

```
SwitchA (enable) set system contact
Cisco NOC 888-555-1234
SwitchA (enable) set system
location Site 10 : Bldg 5 : Rack 5c
```


Device Configs for Maximum Manageability

Other NM config statements

Use timestamps in buffered logs and syslog messages

IOS v12.0 example:

service timestamps [type] datetime [msec] [localtime] [show-timezone]

```
RouterA(config)# service timestamps
log datetime
RouterA(config)# service timestamps
debug uptime
```

Device Configs for Maximum Manageability

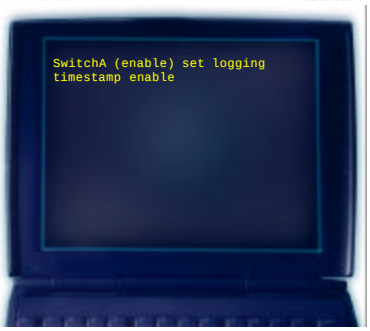
Cisco.com

Other NM config statements

Use timestamps in buffered logs

CatOS v5.5 example:

set logging timestamp [enable | disable]



Cisco.com

Example Configs

Example Configs

Cisco.com

Complete Router and Switch Configuration Examples of Best Practices

- What are we trying to achieve?
  - Document the configuration
  - Maximize authorized network manageability
  - Restrict unauthorized access to the greatest extent possible
    - »(Router Config)
    - »(Switch Config)

Example Configs

IOS 12.0 Router config example

Timestamp to know when messages happened

Using service password-encryption helps, but it's not foolproof – password cracking tools exist!

```
RouterA# show running-config
Current configuration:
!
version 12.0
no service single-slot-reload-enable
service timestamps debug datetime msec
localtime show-timezone
service timestamps log datetime msec localtime
show-timezone
service password-encryption
!
hostname RouterA
!
boot system flash:c2600-is-mz.120-9.bin
logging buffered 4096 debugging
 --More--
```


Example Configs

IOS 12.0 Router config example

Use AAA/TACACS+ with fall-back to local if AAA is down

AAA Accounting is turned on (if desired)

```
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default group tacacs+
local
aaa accounting update newinfo periodic 4
aaa accounting exec default start-stop group
tacacs+
aaa accounting commands 15 default start-stop
group tacacs+
aaa accounting network default start-stop group
tacacs+
aaa accounting connection default start-stop
group tacacs+
aaa accounting system default start-stop group
tacacs+
 --More--
```


Example Configs

IOS 12.0 Router config example

Set your timezone accordingly – if network is truly large, assess if using UTC net-wide is prudent; setting to NOC timezone is helpful

```
enable secret REMOVED
!
clock timezone Eastern -5
clock summer-time EDT recurring
ip subnet-zero
ip cef
!
!
no ip finger
no ip domain-lookup
ip domain-name cisco.com
ip name-server 192.168.1.30
ip name-server 192.168.2.30
!
no ip dhcp-client network-discovery
call rsvp-sync
!
 --More--
```

Example Configs

IOS 12.0 Router config example

Put descriptions on your interfaces ("to locations", circuit Ids, patch panel locations, etc.)

```
interface Loopback0
 description Management interface
 ip address 192.168.100.5 255.255.255.255
!
interface FastEthernet0/0
 description to 6500 port3/5 vlan2
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 --More--
```


Example Configs

IOS 12.0 Router config example

```
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 description to hr7-2621-2 s0/0 : BobCom CID
ABC123
 bandwidth 64
 ip address 192.168.6.1 255.255.255.0
 clockrate 64000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 --More--
```


Example Configs

IOS 12.0 Router config example

Setting up Syslog

Redundant Syslog receivers

Syslog messages stamped as coming from Loopback to easily ID the device (optional)

```
router eigrp 100
 network 192.168.5.0
 network 192.168.6.0
 network 192.168.100.0
 no auto-summary
 eigrp log-neighbor-changes
!
ip classless
no ip http server
!
logging history notifications
logging trap notifications
logging 192.168.1.25
logging 192.168.1.25
logging source-interface Loopback0
!
 --More--
```

Example Configs

IOS 12.0 Router config example

ACL to restrict SNMP usage

RO for NOC net

RW for NMS (users have to login to NMS to do writes – think audit trail)

Other SNMP MIB-2 type data config'd

```
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any log
access-list 11 permit 192.168.1.25
access-list 11 permit 192.168.1.26
access-list 11 deny any log
!
snmp-server engineID local
0000000902000049ACDA900
snmp-server chassis-id ABC12345
snmp-server community public RO 10
snmp-server community private RW 11
snmp-server location Site 10 : Bldg 5 : Rack 5c
snmp-server contact Cisco NOC : 888-555-1234
snmp-server system-shutdown
 --More--
```


Example Configs

IOS 12.0 Router config example

SNMP trap config

```
snmp-server enable traps snmp authentication
linkdown linkup coldstart
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps ipmulticast
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps dsp card-status
 --More--
```


Example Configs

IOS 12.0 Router config example

Restrict TFTP access with ACL? It's up to you!

SNMP trap receivers defined

RMON alarm and events defined for broadcasts (value of 500 pkts is low to test trigger)

```
snmp-server enable traps voice poor-qov
snmp-server enable traps xgcp
snmp-server tftp-server-list 11
snmp-server trap-source Loopback0
snmp-server host 192.168.1.25 public
snmp-server host 192.168.2.11 public
rmon event 1 trap public description "High
broadcast on interface" owner operator
rmon event 2 log description "Normal broadcast
reset on interface" owner operator
rmon alarm 1 ifEntry.12.1 60 delta rising-
threshold 500 1 falling-threshold 30 2 owner
operator
!
dial-peer cor custom
!
 --More--
```

Example Configs

IOS 12.0 Router config example

AAA/TACACS+ server definitions and NTP servers defined

Multiple AAA/TACACS+ servers or rely on fallback? If using AAA/Radius/TACACS+ for other uses then do redundant servers, else fallback is OK

```
tacacs-server host 192.168.1.26
tacacs-server key cisconmcons
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password REMOVED
 login
line vty 5 15
 login
!
no scheduler allocate
ntp clock-period 17180224
ntp server 192.168.1.26
ntp server 192.168.2.11
```


Example Configs

CatOS 5.5 Switch config example

```
SwitchA> (enable) show config all
begin
!
# ***** ALL (DEFAULT and NON-DEFAULT)
CONFIGURATION *****
!
#time: Mon May 7 2001, 17:05:30 EDT
!
#version 5.5(2)
!
set password $1$JnCd$6Bg6VvfQKMFE9sIhT/nlT.
set enablepass $1$Ozci$elU5MFG.XQutGBzd1sBUq1
set prompt SwitchA>
set length 24 default
--More--
```


Example Configs

CatOS 5.5 Switch config example

Banner are nice—unless you feel security through obscurity is warranted

SNMP MIB-2 info set

```
set logout 20
set banner motd # Lab Cat6000 #
!
#test
set test diaglevel minimal
!
#errordetection
set errordetection inband disable
set errordetection memory disable
!
#system
set system baud  9600
set system modem disable
set system name  SwitchA
--More--
```

Example Configs

CatOS 5.5 Switch config example

More SNMP MIB-2 info set

```
set system location Site 10 : Bldg 5 : Rack 5c
set system contact Cisco NOC : 888-555-1234
set system countrycode
set traffic monitor 100
set system highavailability disable
set system highavailability versioning disable
!
#power
set power redundancy enable
!
#frame distribution method
set port channel all distribution ip both
!
--More--
```


Example Configs

CatOS 5.5 Switch config example

SNMP community strings set

RMON enabled

SNMP traps enabled

```
#snmp
set snmp community read-only      know1kanpowl
set snmp community read-write     iyam2kewl
set snmp community read-write-all 4urisonly
set snmp rmon enable
set snmp trap enable  module
set snmp trap enable  chassis
set snmp trap enable  repeater
set snmp trap enable  vtp
set snmp trap enable  auth
set snmp trap enable  ippermit
set snmp trap disable vmps
set snmp trap enable  entity
set snmp trap enable  config
--More--
```


Example Configs

CatOS 5.5 Switch config example

SNMP trap receivers defined

AAA/TACACS+ defined

```
set snmp trap enable  stpx
set snmp trap enable  syslog
set snmp trap 192.168.1.25    public
set snmp trap 192.168.1.26    public
!
#tacacs+
set tacacs server 192.168.1.26 primary
set tacacs server 192.168.2.11
set tacacs attempts 3
set tacacs directedrequest disable
set tacacs key cisconmcons
set tacacs timeout 5
!
#radius
--More--
```

Example Configs

CatOS 5.5 Switch config example

AAA/TACACS+ authentication for logins configured

```
set radius deadtime 0
set radius timeout 5
set radius retransmit 2
!
#kerberos
!
#authentication
set authentication login tacacs enable console
primary
set authentication login tacacs enable telnet
primary
set authentication login tacacs enable http
primary
set authentication enable tacacs disable
console
--More--
```


Example Configs

CatOS 5.5 Switch config example

```
set authentication enable tacacs disable telnet
set authentication enable tacacs disable http
set authentication login radius disable console
set authentication login radius disable telnet
set authentication login radius disable http
set authentication enable radius disable
console
set authentication enable radius disable telnet
set authentication enable radius disable http
set authentication login local enable console
set authentication login local enable telnet
set authentication login local enable http
set authentication enable local enable console
set authentication enable local enable telnet
--More--
```


Example Configs

CatOS 5.5 Switch config example

```
set authentication enable local enable http
set authentication login kerberos disable
console
set authentication login kerberos disable
telnet
set authentication login kerberos disable http
set authentication enable kerberos disable
console
set authentication enable kerberos disable
telnet
set authentication enable kerberos disable http
!
#vtp
#(Removed for brevity)
--More--
```

Example Configs

CatOS 5.5 Switch config example

If you are using RCP to transfer images make sure this syncs with CW2k set-up

```
#ip
#(Removed for brevity)
!
#command alias
!
#vmps
#(Removed for brevity)
!
#rcp
set rcp username
!
#dns
set ip dns disable
!
--More--
```


Example Configs

CatOS 5.5 Switch config example

Syslog config

Logging levels should be set to what is appropriate for your environment and informational requirements

```
#spantree
#(Removed for brevity)
!
#syslog
set logging console enable
set logging server enable
set logging server 192.168.1.25
set logging server 192.168.2.11
set logging level cdp 4 default
set logging level mcast 2 default
set logging level dtp 5 default
set logging level earl 2 default
set logging level ip 2 default
set logging level pruning 2 default
--More--
```


Example Configs

CatOS 5.5 Switch config example

```
set logging level snmp 2 default
set logging level spantree 2 default
set logging level sys 5 default
set logging level tac 2 default
set logging level tcp 2 default
set logging level telnet 2 default
set logging level tftp 2 default
set logging level vtp 2 default
set logging level kernel 2 default
set logging level filesys 2 default
set logging level pagp 5 default
set logging level mgmt 5 default
set logging level mls 5 default
set logging level protfilt 2 default
--More--
```

Example Configs

CatOS 5.5 Switch config example

```
set logging level security 2 default
set logging level radius 2 default
set logging level udld 4 default
set logging level gvrp 2 default
set logging level cops 3 default
set logging level qos 3 default
set logging level acl 5 default
set logging level rsvp 3 default
set logging level ld 2 default
set logging level privatevlan 2 default
set logging server facility LOCAL7
set logging server severity 5
set logging timestamp enable
set logging buffer 500
--More--
```


Example Configs

CatOS 5.5 Switch config example

NTP configuration

```
set logging history 400
!
#ntp
set ntp broadcastclient disable
set ntp broadcastdelay 3000
set ntp client enable
set ntp authentication disable
set ntp server 172.18.86.71
set ntp server 172.18.86.73
set timezone Eastern -5 0
set summertime enable EDT
set summertime recurring
!
--More--
```


Example Configs

CatOS 5.5 Switch config example

Let's add some 'ip permit' security—this restricts telnet and snmp—flexible

```
#set boot command
#(Removed for brevity)
!
#permit list
set ip permit enable telnet
set ip permit enable snmp
set ip permit 192.168.1.0 255.255.255.0
!
#permanent arp entries
!
#igmp
set igmp enable
set igmp fastleave disable
!
--More--
```

Example Configs

CatOS 5.5 Switch config example

```
#rgmp
set rgmp disable
!
#protocolfilter
set protocolfilter disable
!
#mls
#(Removed for brevity)
!
#vlan mapping
!
#gmrp
set gmrp disable
!
--More--
```


Example Configs

CatOS 5.5 Switch config example

```
#garp
set garp timer all 200 600 10000
!
#cdp
set cdp interval 60
set cdp holdtime 180
set cdp enable
set cdp version v2
!
#qos
#(Removed for brevity)
!
#cops
set cops retry-interval 30 30 300
--More--
```


Example Configs

CatOS 5.5 Switch config example

AAA/TACACS+ accounting

```
#udld
set udld disable
set udld interval 15
!
#port channel
#(Removed for brevity)
!
#security ACLs
!
#accounting
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop
tacacs+
set accounting system enable start-stop tacacs+
--More--
```

Example Configs

CatOS 5.5 Switch config example

```
set accounting commands enable all tacacs+
set accounting suppress null-username disable
set accounting update new-info
!
#errdisable timeout
#(Removed for brevity)
!
#http configuration
set ip http server disable
set ip http port 80
!
#private vlans
!
# default port status is enable
--More--
```


Example Configs

CatOS 5.5 Switch config example

Label your modules and ports (24 characters max)

Enable traps on uplinks, server connects and other important ports

(Next 13 slides worth of config deleted due to minimal NM content)

```
#module 1 : 2-port 1000BaseX Supervisor
set module name    1    To Distr
set vlan 12   1/2
set vlan 100  1/1
set port enable     1/1-2
set port trap       1/1-2  enable
set port name       1/1  To SwitchB 1/2
set port name       1/2
set port security 1/1-2 disable age 0 maximum 1
shutdown 0 violation shutdown
set port broadcast  1/1-2  100.00%
set port membership 1/1-2  static
set port protocol 1/1-2 ip on
set port protocol 1/1-2 ipx auto
--More--
```


Example Configs

CatOS 5.5 Switch config example

AAA/TACACS+ authorization (optional)

```
set authorization exec disable telnet
set authorization enable disable console
set authorization enable disable telnet
set authorization commands disable console
set authorization commands disable telnet
end
```

A couple more things

Cisco.com

DNS

- At a minimum put your router loopback addresses and switch sc0 interface address in DNS
- Set hostname to match DNS nodename
- Forward/reverse lookups for interfaces?
- See CCO doc on how CiscoWorks2000 resolves a device's ID

  www.cisco.com/warp/public/cc/pd/wr2k/cpmn/prodlit/wk2ke_wp.htm

Processes and Procedures

Cisco.com

Network Design for Ease of Troubleshooting

- Add Network Analysis Modules (NAMs) to core switches
- Deploy RMON probes on critical infrastructure links and server connections
- Dedicate laptops for mobile analysis stations with packet sniffers, SNMP tools, and a terminal program for console connections
- When problems occur, you will have the ability to quickly run diagnostics and minimize downtime

A couple more things

Cisco.com

RMON

- NAM/Probes—Where to deploy
  - Data center/server farm
  - Network points of egress—WAN/ISP
- NAM/Probes—Considerations
  - Media type and speed
  - Inline tap (passive), SPAN or switch module

A couple more things

Cisco.com

RMON

- **RMON alarm and events capabilities in IOS**
  - **Allow the device to monitor itself and report back threshold violations**
  - **Reduces polling requirements on NMS**

A couple more things

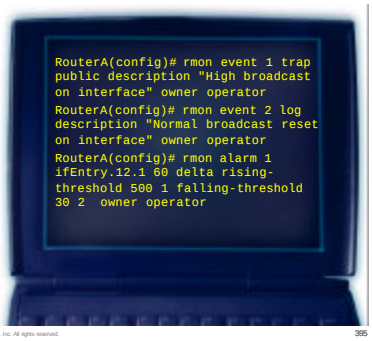
Cisco.com

IOS 12.0 RMON alarm & event configuration

Syntax:

rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]

rmon event number [log] [trap community] [description string] [owner string]



SNMP MIB Tools

Cisco.com

- **MIB Locator Tool (requires CCO account) – http://www.cisco.com/go/mibs**
- **SNMP Object Navigator (requires CCO account) - http://www.cisco.com/cgi-bin/Support/Mibbrowser/unity.pl**
- **SNMP Search & Translate – http://jaguar.ir.miami.edu/~marcus/snmptrans.html**
- **MIBs In Images Mail – Send email to mii@external.cisco.com with a subject of "help"**
- **Command line SNMP tools – http://net-snmp.sourceforge.net**

Performance Measurements

Cisco.com

Measurement \ Scope	Device	Network	Service
CPU/Memory Utilization	X		
Bandwidth Utilization		X	X
Availability	X	X	X
Packet Loss	X	X	X
Delay	(X)	X	X
Jitter	(X)	X	X

Polling Guidelines

Cisco.com

Object Name	Object Descr	OID	Poll Int	Threshold
bufferFail	Number Of buffer Allocation Failures	.1.3.6.1.4.1.9.2.1.46	15 Min	
bufferNoMem	Number Of buffer Create Failures Due To No Free Memory	.1.3.6.1.4.1.9.2.1.47	15 Min	
ciscoMemoryPoolFree	Indicates The Number Of Bytes From The Memory Pool That Are Currently Unused On The Managed Device	1.3.6.1.4.1.9.9.48.1.1.1.6	30 Min	
ciscoMemoryPoolLargestFree	The Largest Number Of Contiguous Bytes From The Memory Pool That Are Currently Unused	.1.3.6.1.4.1.9.9.48.1.1.1.7	30 Min	
ciscoMemoryPoolUsed	The Number Of Bytes From The Memory Pool That Are Currently In Use	.1.3.6.1.4.1.9.9.48.1.1.1.5	30 Min	

Polling Guidelines

Object Name	Object Descr	OID	Poll Int	Threshold
cpmCPUTotal5min	Overall CPU Busy Percentage in the Last 5 Min Period This Object Deprecates the Avgbusy5 Object from the OLD-CISCO-SYSTEM- MIB	.1.3.6.1.4.1.9.9.109.1.1.1.1.5	5 Min	
ifInDiscards	The Number of Inbound Packets which Were Chosen to Be Discarded Even though No Errors Had Been Detected to Prevent Their Being Deliverable to a Higher-Layer Protocol; One Possible Reason for Discarding Such a Packet Could Be to Free up Buffer Space	.1.3.6.1.2.1.2.2.1.13	30 Min	
ifInNUcastPkts	Number of Non-unicast Packets Delivered to a Higher-Layer Protocol	.1.3.6.1.2.1.2.2.1.12	30 Min	

Polling Guidelines

Object Name	Object Descr	OID	Poll Int	Threshold
ifInOctets	The Total Number of Octets Received on the Interface, Including Framing Characters	.1.3.6.1.2.1.2.2.1.10	30 Min	
ifOutDiscards	The Number of Outbound Packets which Were Chosen to Be Discarded Even though No Errors Had Been Detected to Prevent Their Being Transmitted; One Possible Reason for Discarding such a Packet Could Be to Free up Buffer Space	.1.3.6.1.2.1.2.2.1.19	30 Min	
ifOutNUcastPkts	The Total Number of Packets that Higher-Level Protocols Requested Be Transmitted to a Non-Unicast (i.e., a Subnetwork-Broadcast or Subnetwork-Multicast) Address, Including Those that Were Discarded or Not Sent	.1.3.6.1.2.1.2.2.1.18	30 Min	

Statistics Needed for Network Analysis

Basic Network Statistics Outline

- Reasons for understanding some basic statistics for network management and analysis
- Basic statistics needed for network and performance analysis
- Using statistics to:
  - Analyze or understand performance data
  - Predict future network performance

Reasons for Understanding Statistics

Three key areas where statistical knowledge is applied to performance management

- Measuring network and service availability
  - Reliability of network components
  - Service level agreements
- Aggregating raw data
  - Reducing raw collected data from 1000's of devices into form that will quickly indicate the state of the network
  - Uses the following statistical methods: average, mode, median, standard deviation, and variance
- Analyzing performance data

Statistical Measures and Applications

- Statistical techniques are needed to:
  - Analyze and condense data collected from the network
  - Predict what data will be in the future
- Basic statistical applications
  - Sample size and polling interval
  - Measures of central tendency (average)
  - Measures of spread (standard deviation)
  - Probability and cumulative density functions

Importance of Sampling Rate and Sample Size

- Need to ensure data collected is good, and meaningful
  - Before we carry out any statistical analysis
  - Make any judgements based on our analysis
- This means:
  - Need to collect enough data points for accuracy
  - Sample at a high enough rate to provide the detail of data required
  - It may be necessary to adjust the sampling rate based on statistical analysis

Sampling Rate v Sample Size

- Sample size is the number of samples that have been collected
  - The more samples collected the higher the confidence that the data collected accurately represents the network
- Sampling Rate is the rate at which data is collected from the network

$$\text{Sampling} = \frac{1}{\text{Polling Interval}}$$

- The higher the sampling rate the more detailed the data collected
  - Example: polling data once every 15 minutes provides 4 times the detail of polling once an hour

Average

- Calculated by adding up all the sample data (x_i) and dividing by the total number of samples (N)

$$\text{ave} = \frac{\sum_{i}^{N} X_i}{N}$$

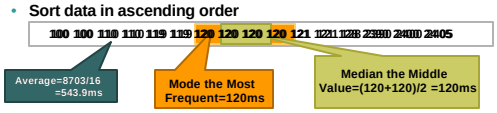
- Simple to calculate
- Good for long term trending
- Can be misleading if data has a large variation in values

Average, Mode, and Median

- Average, mode, and median are measures of how data clusters around the centre of a distribution
- Mode is the most common occurrence of a value in a distribution
- Median is the middle value in the distribution
- Mode and median good for verifying average and identifying skews in average results
- Example Ping (ms) collected on an hourly basis

  120 119 121 110 120 100 128 2400 2390 2405 120 121 100 110 119 120

- Sort data in ascending order



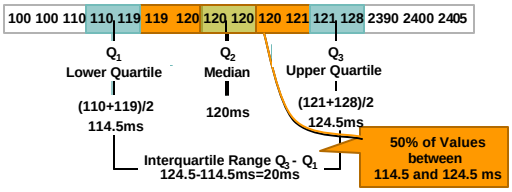
Measures of Spread: Range and Quartiles

- Range

  The difference between the highest and lowest value in a data set 2405-100 = 2305

- Quartiles

  Sort data set into ascending order and split into 4 equal parts



Deciles and Percentiles

- **Deciles**

  Sort data in ascending order and divide into 10 equal parts

- **Percentiles**

  Sort data in ascending order and divide into 100 equal parts

  Useful for data represented as utilization (0–100%)

Standard Deviation (DEV)

- Standard Deviation (DEV) is a measure of spread of data from the center of a distribution
- Standard deviation
  - Takes into account all values in the data (unlike mode and median)
  - Is the most well known and commonly used method for calculating the spread of data
  - Is easy to calculate by management systems and network devices
    - Equations are available that allow DEV to be calculated as data arrives
- Cisco SA Agents provide DEV for jitter probes

Standard Deviation (S)

- Standard deviation is the square root of the variance
  - If variance = 1620.6 ms^2
  - Standard deviation = SQRT(1620.6) = 40.25ms
- Standard deviation units are the same as the sampled data

$$S = \sqrt{\frac{\sum_{i}^{N}(ave - X_i)^2}{N}}$$

Application of Statistical Methods

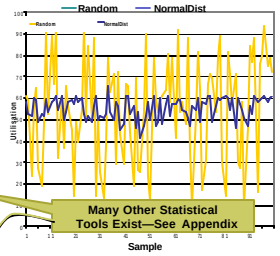
Which Is Worse?

Measures of Central Tendency

Stat	Random	Normal
Average	55	55
Median	58	56
Mode	79	61

Measures of Spread

Stat	Random	Normal
Q1	36.8	52
Q3	72.3	60
Max	94	66
Min	10	41
Interquatile Range	36	8
Standard Deviation	23.8	4.9



Many Other Statistical Tools Exist—See Appendix

Many Data Points Could Be Summarized by 2 Statistical Values

Variance (S^2)

- Variance is measure of spread that takes into account all values in the data
- Variance (S^2)

  Average of squared deviation in values from the average
- Example 6 pings with delay in ms of 1, 1, 1, 2, 2, 100

  Average = $\frac{1 + 1 + 1 + 2 + 2 + 100}{6}$ = 18ms

  Variance =

  $$\frac{(18 - 1)^2 + (18 - 1)^2 + (18 - 1)^2 + (18 - 2)^2 + (18 - 2)^2 + (18 - 100)^2}{(6 - 1)}$$

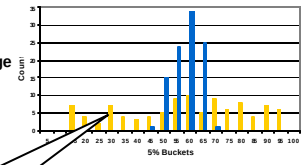
  = 1620.6 ms2

  Units are ms squared and not too meaningful in terms of delay

Probability Density Function

- Groups data into buckets
- Provides visualization of data's statistical properties

  Clearly shows the average and spread of data
- Blue has small dispersion around 60% utilization
- Orange is more random



Random Data Is Difficult to Predict
Bad for Performance Monitoring

Cumulative and Probability Density Functions

- Probability (PDF) density function

  Gives the probability of a data point being a given value

  Good for visualizing the statistical nature of data collected

  Predicting future values of data
- Cumulative (CDF) density function

  Gives the probability of a data point being less than a given value

  Good for calculating the percentiles

  Good for defining performance thresholds

Cumulative and Probability Density Functions

Cisco.com

PDF and CDF:

- Group data into buckets
- Simple to calculate
- Work better for larger sets of data
- Require some knowledge of average, and spread of data beforehand
  - Need to know how many buckets and size of buckets to provide a good visualization of statistical nature of data
  - Unless data is already normalised into a range of 1–100 such as utilization

Availability Trouble Ticketing Example

Cisco.com

- Network with 100 customers
- Time in reporting period is one year or 24 ´ 365 hours
- 8 customers have 24 hours down time per year

$$DPM = \frac{8 \times 24}{100 \times 24 \times 365} \times 10^6 = 219.2$$ failures for every 1 million user hours.

$$Availability = 1 - \frac{8 \times 24}{100 \times 24 \times 365} = 0.978082$$

$$MTBF = \frac{24 \times 365}{8} = 1095 \text{ (hours)}$$

$$MTTR = \frac{1095 \times (1-0.978082)}{0.978082} = 0.24 \text{ (hours)}$$

Availability Using Network-Based Probes

Cisco.com

- DPM equations used with network based probes as input data
- Probes can be
  - Simple ICMP Ping probe, modified Ping to test specific applications, Cisco IOS SAA
- DPM will be for connectivity between 2 points on the network, the source and destination of probe
  - Source of probe is usually a management system and the destination are the devices managed
  - Can calculate DPM for every device managed

$$DPM = \frac{\text{Probes with No Response}}{\text{Total Probes Sent}} \times 10^6$$

$$Availability = 1 - \frac{\text{Probes with No Response}}{\text{Total Probes Sent}}$$

Availability Using Network-Based Probes: Example

- Network probe is a Ping
- 10000 Probes are sent between management system and managed device
- 1 probe failed to respond

$$DPM = \frac{1}{10000} \times 10^6 = 100 \text{ probes out of 1 million will fail}$$

$$\text{Availability} = 1 - \frac{1}{10000} = 0.9999$$

Sample Size

- Sample size is the number of samples that have been collected
- The more samples collected the higher the confidence that the data accurately represents the network
- Confidence (margin of error) is defined by

$$m = \frac{1}{\sqrt{\text{sample size}}}$$

- Example data is collected from the network every 1 hour

After One Day

$$m = \frac{1}{\sqrt{24}} = 0.2041$$

After One Month

$$m = \frac{1}{\sqrt{24 \times 31}} = 0.0367$$

Polling Interval vs. Sample Size

- Polling interval is the rate at which data is collected from the network

$$\text{Polling interval} = \frac{1}{\text{Sampling Rate}}$$

- The smaller the polling interval the more detailed (granular) the data collected
  - Example polling data once every 15 minutes provides 4 times the detail (granularity) of polling once an hour
- A smaller polling interval does not necessarily provide a better margin of error
  - Example polling once every 15 minutes for one hour, has the same margin of error as polling once an hour for 4 hours

Basic Network Statistics Summary

- Key statistical measures
  - Measures of central tendency: average, mode, median
  - Measures of spread: standard deviation
  - Probability density function
- Many data points can be represented by a few key statistical measures
  - Allows aggregation of data
  - Provides an understanding of the statistical nature of the data
  - Enables prediction of what data will be like in the future

Process and Tools Development for Network Operations

What is a NOC?

Develop A Plan!

- Don't get stuck in "Analysis Paralysis"

Crawl

What is a NOC?

Cisco.com

Develop A Plan!

- **Don't get stuck in "Analysis Paralysis"**

Walk

What is a NOC?

Cisco.com

Develop A Plan!

- **Don't get stuck in "Analysis Paralysis"**

Run!!

What is a NOC?

Cisco.com

Develop A Plan!

- **Only then**

  Jump into HyperSpace/Warp 9.99