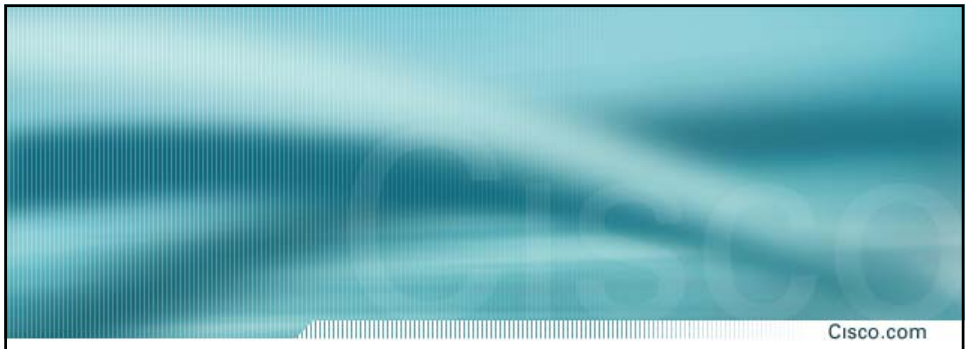


Permanente Netzwerküberwachung

Wolfram Maag

wmaag@cisco.com

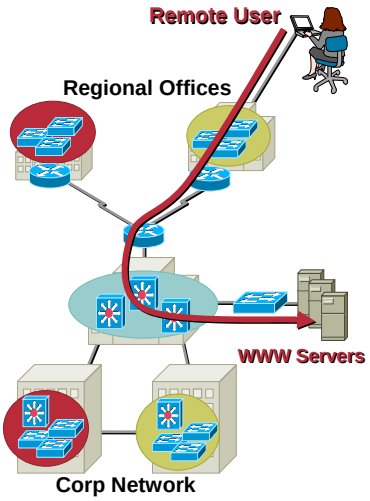
Agenda

- **Network Management**
  - **Protocols and Technologies**
  - **Functional Areas of Network Management**
  - **Real World Applications of Proper Management Practices**
- **Netflow**
- **Network Analysis**

The Case for Management

Cisco.com

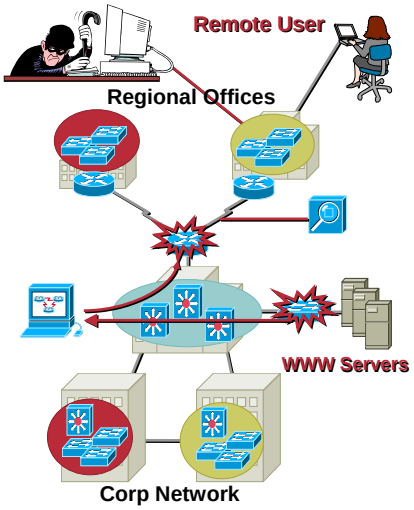
- **Typical problem**
  - Regional user arrives at work and experiences slow or no response from corporate web server
- **Where do you begin?**
  - Where is the problem?
  - What is the problem?
  - What is the solution?
- **Without proper network management, these questions are difficult to answer**



The Case for Management

Cisco.com

- **With proper management tools and procedures in place, you may already have the answer**
- **Consider some possibilities**
  1. What configuration changes were made overnight?
  2. Have you received a device fault notification indicating the issue?
  3. Have you detected a security breach?
  4. Has your performance baseline predicted this behavior on an increasingly congested network link?

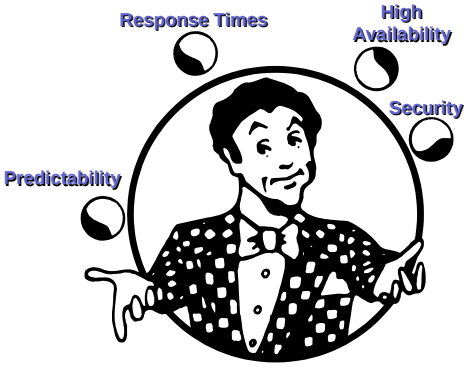


The Case for Management

Cisco.com

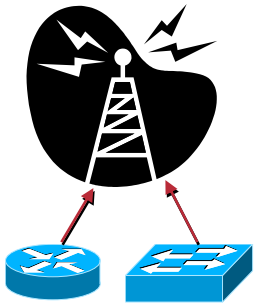
Solving a Typical Problem Like This Includes the Following:

- An accurate database of your network's topology, configuration, and performance
- A solid understanding of the protocols and models used in communication between your management server and the managed devices
- Methods and tools that allow you to interpret and act upon gathered information

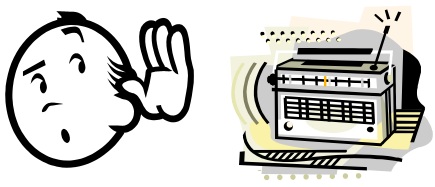


Communicating with the Network

Cisco.com



Managed Network Elements Are Waiting to Provide Us with Useful Information…

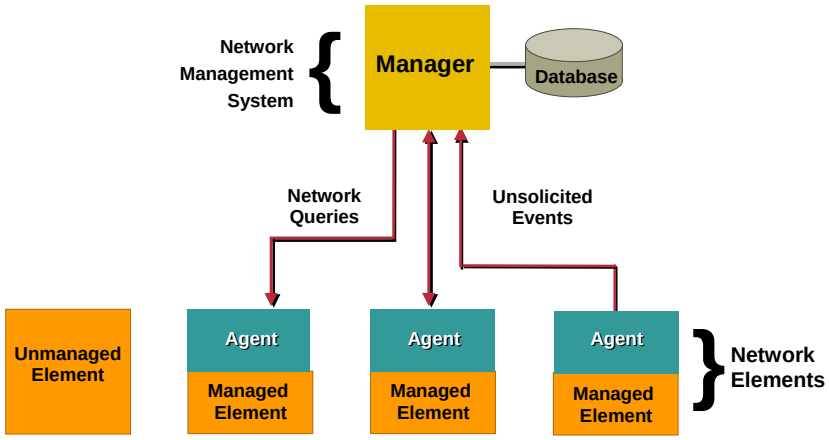


Network Management Begins with an Understanding of How to Collect and Interpret This Information

Two-Tier Management Communication

Cisco.com

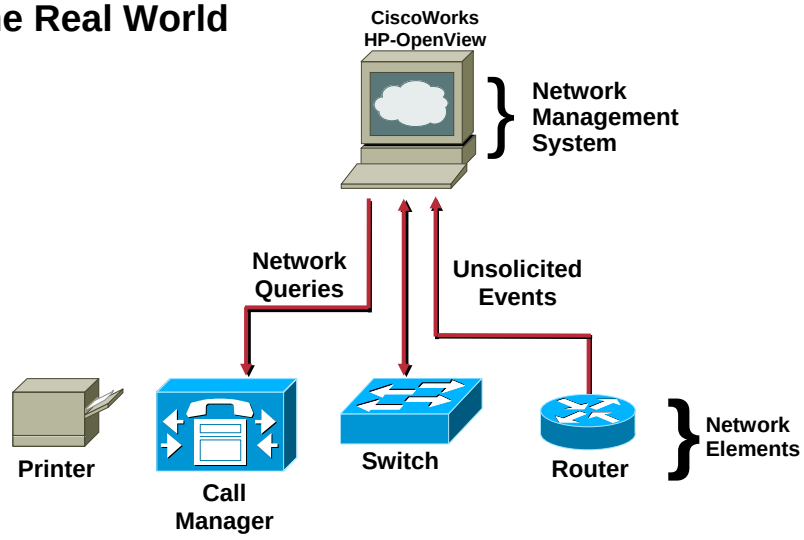
The Model



Two-Tier Management Communication

Cisco.com

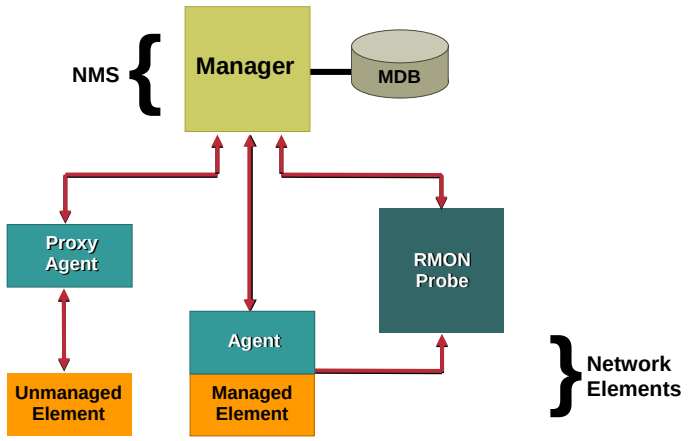
The Real World



Three-Tier Management Communication

Cisco.com

The Model



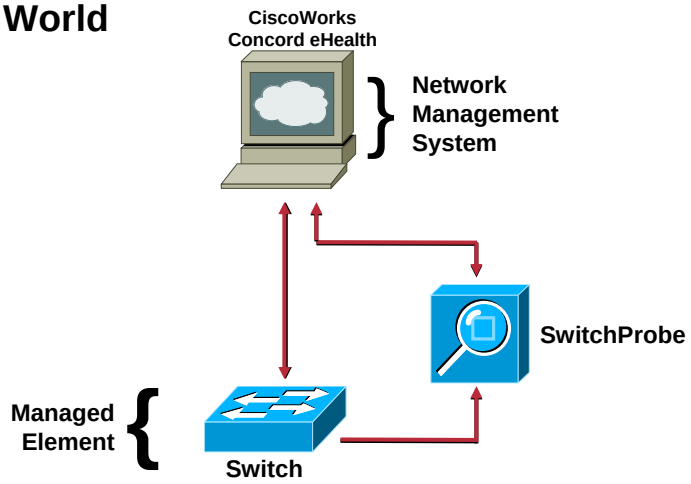
NMS-1001
8230_06_2003_X2

9

Three-Tier Management Communication

Cisco.com

The Real World

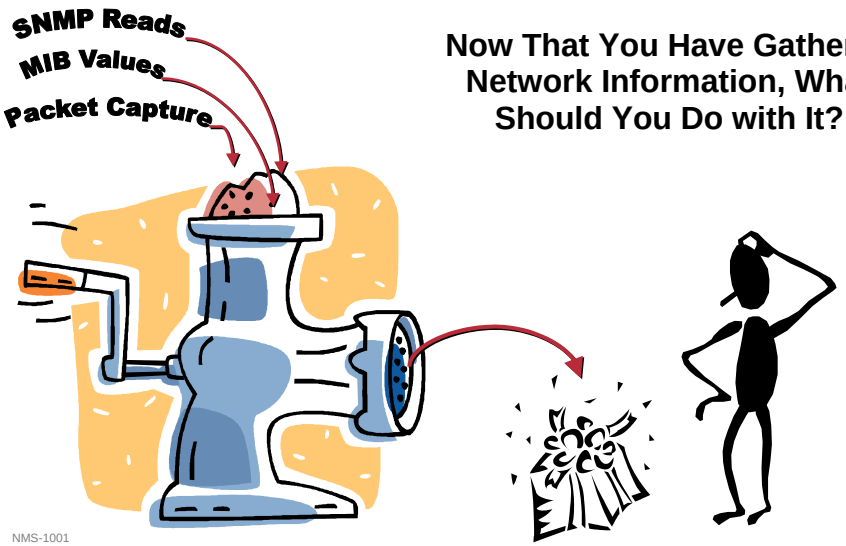


NMS-1001
8230_06_2003_X2

10

Applying a Management Model

Cisco.com



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

Cisco.com

Network Management Station

The Five Facets of Proper Network Management

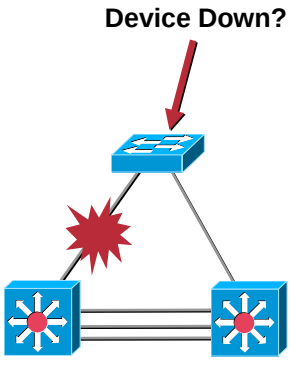
Cisco.com

- Addresses the network management applications that reside upon the NMS
- OSI model categorizes five areas of function (sometimes referred to as the FCAPS model):
  - Fault
  - Configuration
  - Accounting
  - Performance
  - Security

Fault Management

Cisco.com

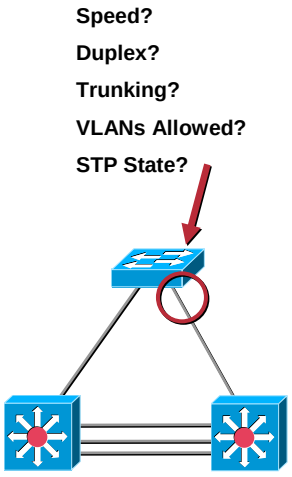
- "The process of locating, diagnosing, and correcting network problems"
- Increases network reliability and effectiveness
- More than just "firefighting"
- Increases the productivity of network users



Configuration Management

Cisco.com

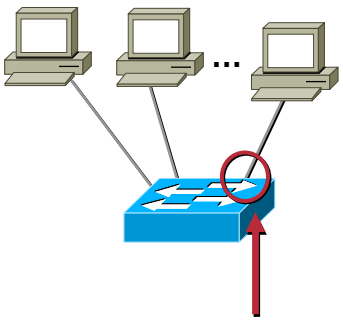
- "The process of obtaining data from the network and using that data to manage the setup of all network devices"
- Allows rapid access to configuration information
- Facilitates remote configuration and provisioning
- Provides an up-to-date inventory of network components



Accounting Management

Cisco.com

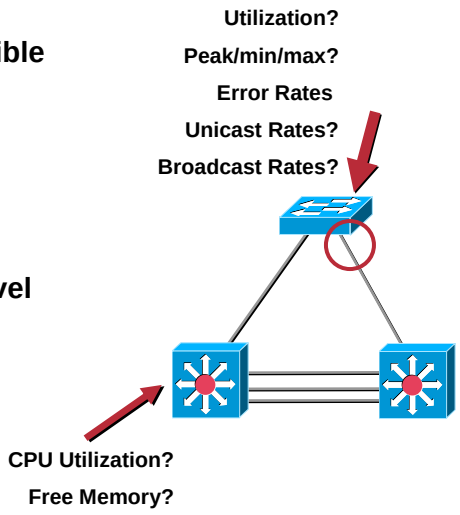
- "Measuring the usage of network resources by users in order to establish the metrics, check quotas, determine costs, and bill users"
- Measures and reports accounting information based on individual groups and users
- Administers the cost of the network
- Internal verification of third-party billing for usage



Performance Management

Cisco.com

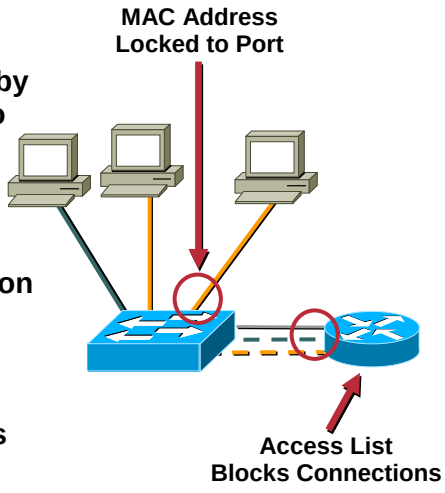
- "Ensuring that the data network remains accessible and as uncongested as possible"
- Reduces network overcrowding and inaccessibility
- Provides a consistent level of service to the network user
- Determine utilization trends to proactively isolate and solve performance problems



Security Management

Cisco.com

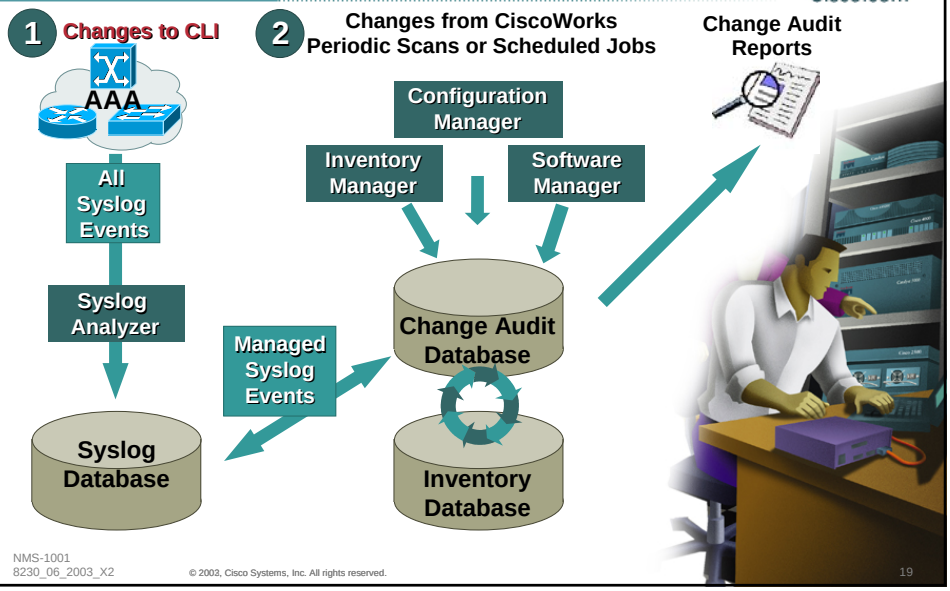
- "Protecting sensitive information on devices attached to a data network by controlling access points to that information"
- Builds network user confidence
- Secures sensitive information from both internal and external sources
- Protects the network functionality from malicious attacks



Configuration Management

Resource Manager Essentials Change Audit Service

Cisco.com



Configuration Management
RME Change Audit Setup

Cisco.com

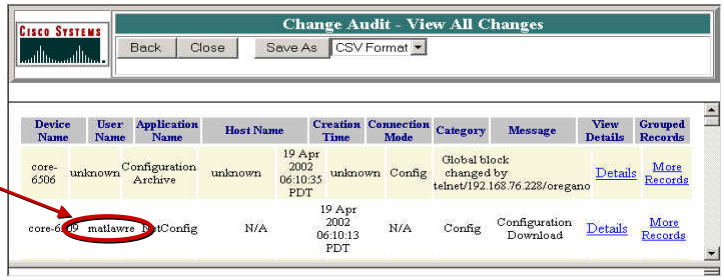
Change Audit relies on syslog messages to operate

- Point syslogs from all managed devices (except Pix firewalls) to the RME server

Collection of usernames occurs in 3 ways:

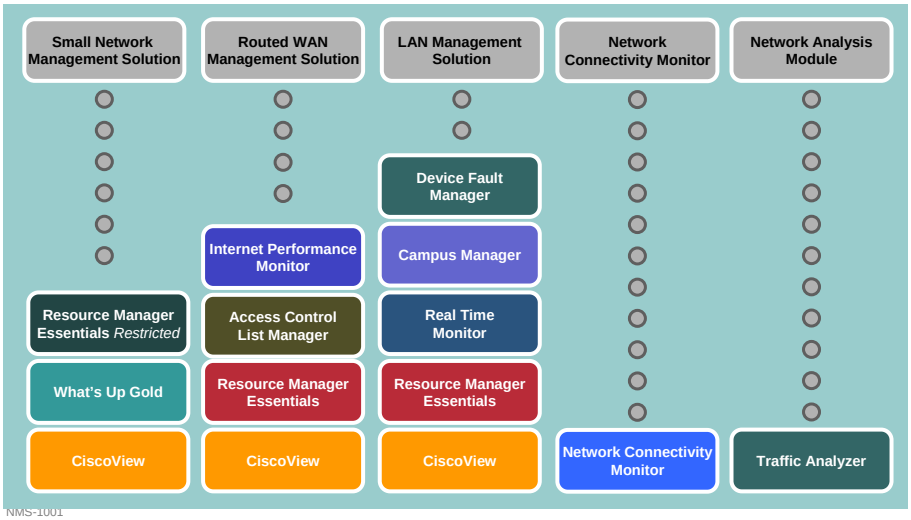
1. Using usernames on devices themselves
2. Using a RADIUS or TACACS server
3. Using a configurations change tool in RME (NetConfig, Config Editor)

That User Name Field Is Important to Most Customers



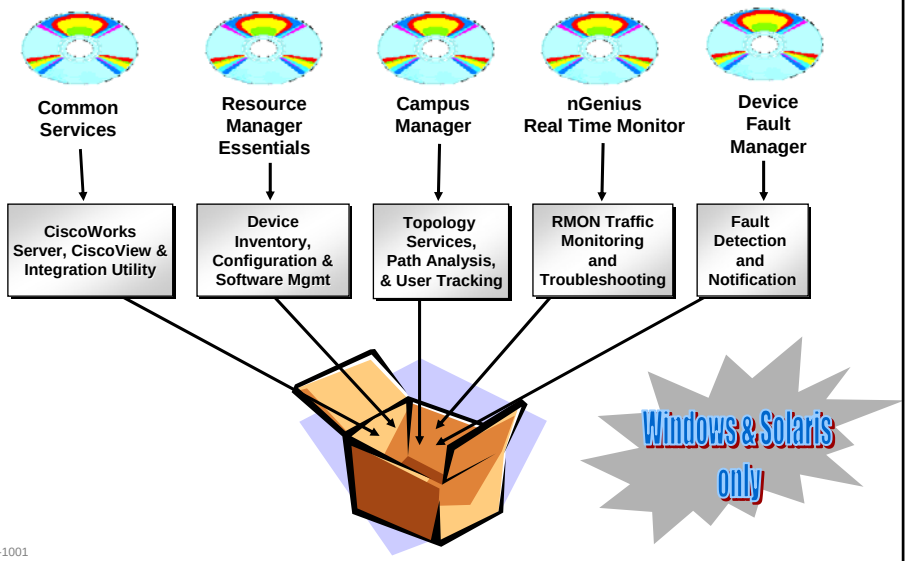
Routing and Switching Management

Cisco.com

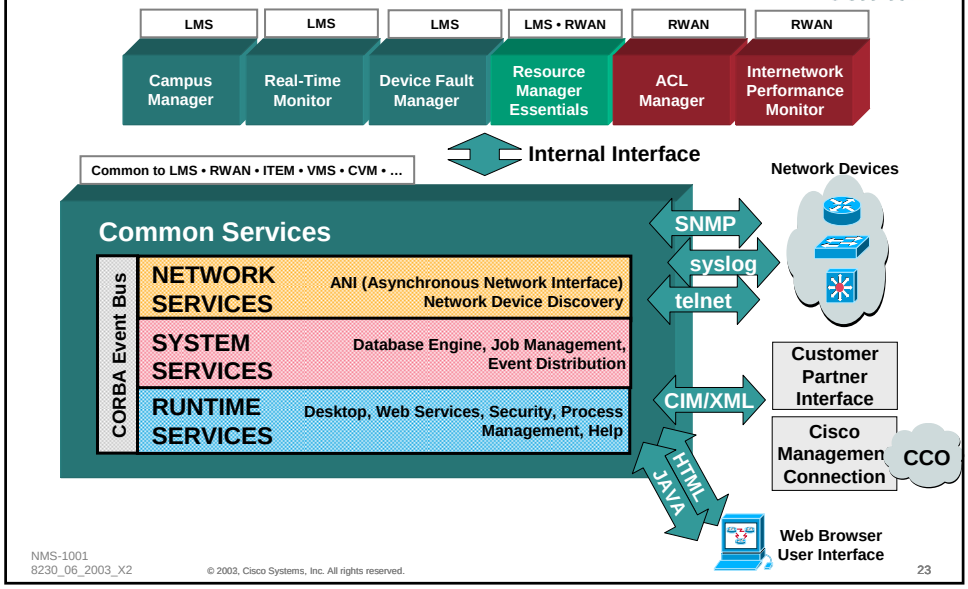


LMS Bundle Contents

Cisco.com



Common Services: Common Management Foundation

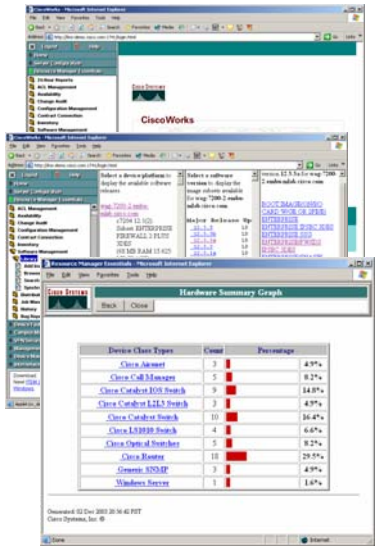


Resource Manager Essentials

Cisco.com

Cornerstone application of CiscoWorks family that delivers lifecycle management of Cisco network devices

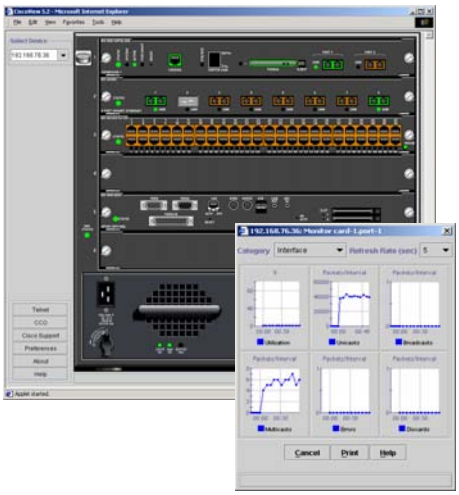
- Inventory Manager
- Device Configuration Manager
- Software Image Manager
- Change Audit Service
- Syslog Analyzer
- Cisco Management Connection
- CCO Service Tools



CiscoView

Cisco.com

- **Web-based access for distributed, multi-user operations**
- **Real-time monitoring and tracking of key data related to traffic and performance**
- **Comprehensive device support with PSU**
- **Open interfaces for integration into 3rd party network management systems**



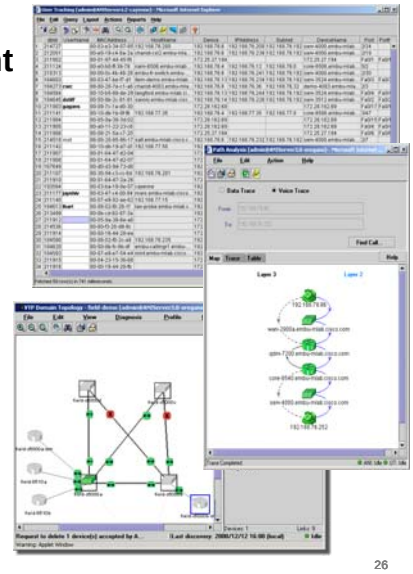
NMS-1001
8230_06_2003_X2

Campus Manager

Cisco.com

Operational network management tool designed for administration, monitoring and configuration of Layer 2 services

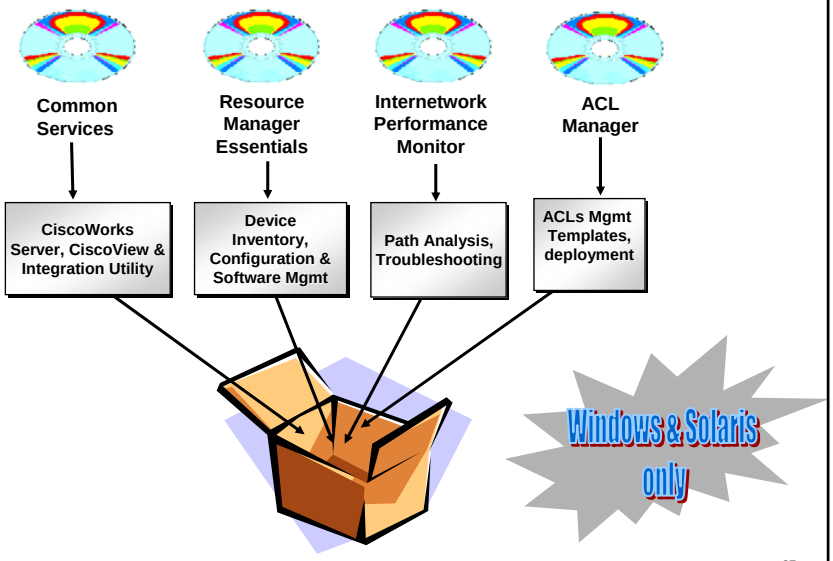
- **Topology Services**
- **VLAN Configuration**
- **ATM Management**
- **User Tracking**
- **Path Analysis**



NMS-1001
8230_06_2003_X2

RWAN Bundle Contents

Cisco.com

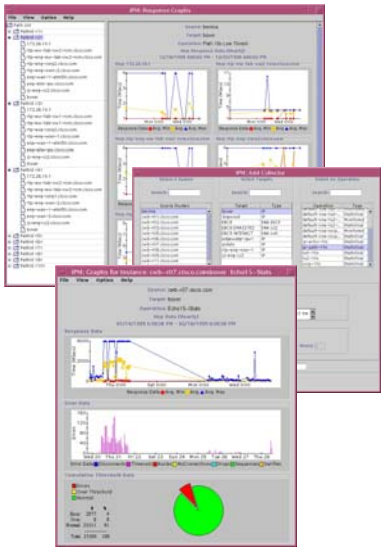


NMS-1001
8230_06_2003_X2

Internetwork Performance Monitor

Cisco.com

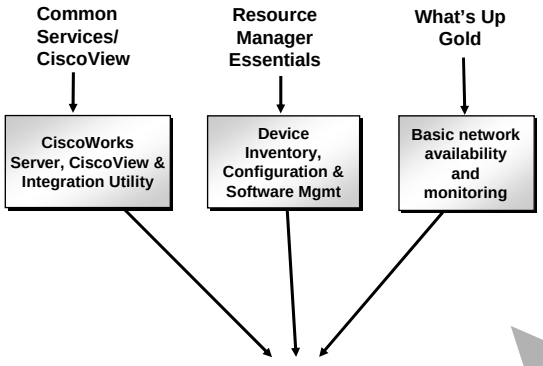
- Network response time and latency measurement tool
- Configuration and monitoring of specific network services – based on Cisco's Service Assurance Agent
- Network path analysis
- Historical reporting and trending
- Threshold definition for real-time alerts and notifications



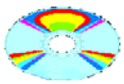
NMS-1001
8230_06_2003_X2

SNMS Components

Cisco.com



Single CD Installation

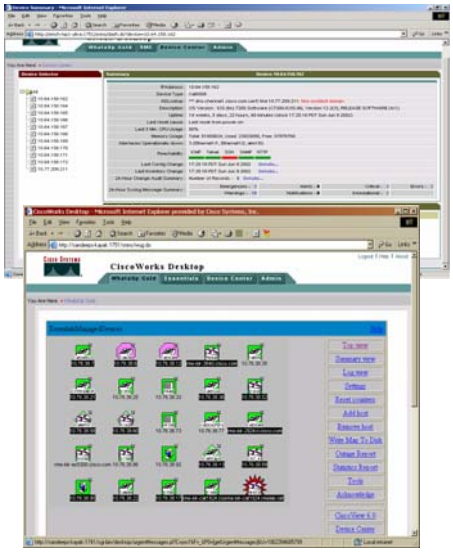


NMS-1001
8230_06_2003_X2

CiscoWorks SNMS

Cisco.com

- Designed for small to medium business networks with limited operations staff
- Tight integration between components within CiscoWorks Desktop
- New Device Center features a one-stop location for device-centric network operations
- Easy cross-launching linkages between What's Up Gold, Device Center, and CiscoView



NMS-1001
8230_06_2003_X2

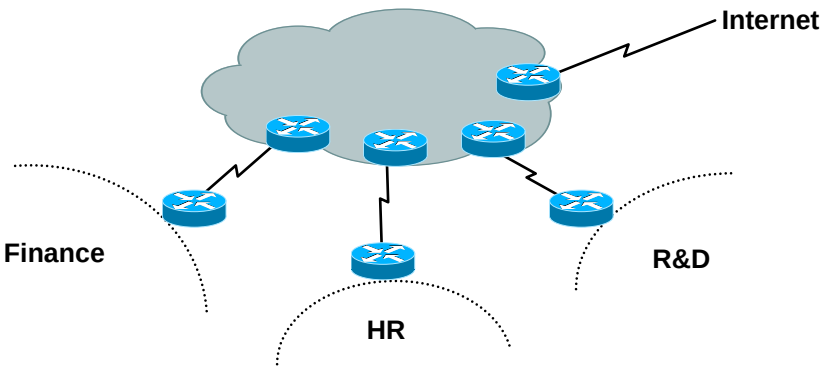
Cisco.com

Netflow

Case Study: Billing

Cisco.com

**I Want My Accounting per Network (Instead of IP Addresses)
For Example, to Charge Back to Department,
the Cost of the Internet Link**

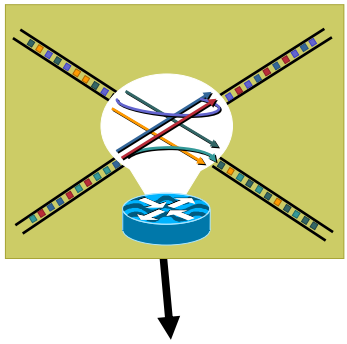


How Does NetFlow Define a Flow?

Cisco.com

7 Keys Define a Flow

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)



Exported Data

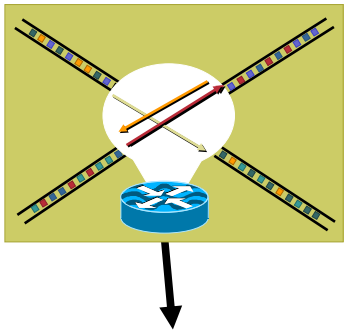
TOS=Type of Service, DSCP=Differentiated Services Code Point

How Does the NetFlow Cache Work?

Cisco.com

NetFlow Cache

7 Identifiers	Other Data
⋮	⋮



Exported Data

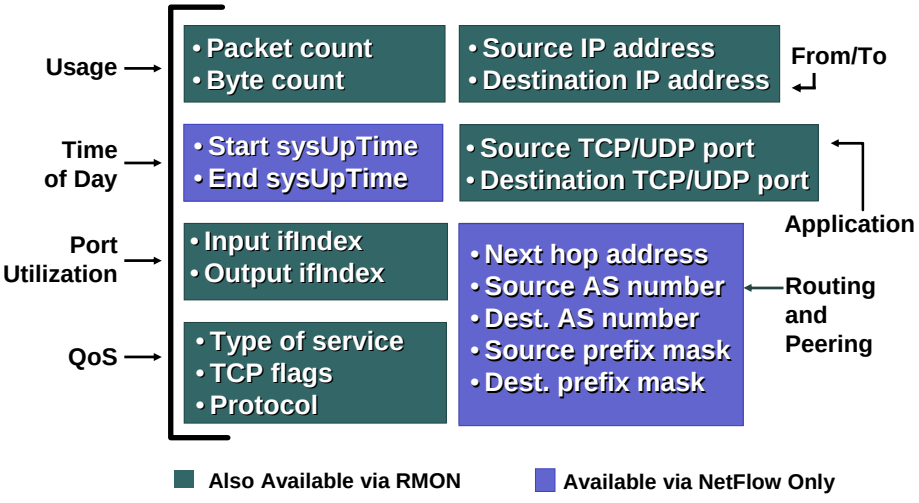
NetFlow: Principles

Cisco.com

- 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

Bsp: Version 5 Flow Format

Cisco.com



Version 5: Configuration

Cisco.com

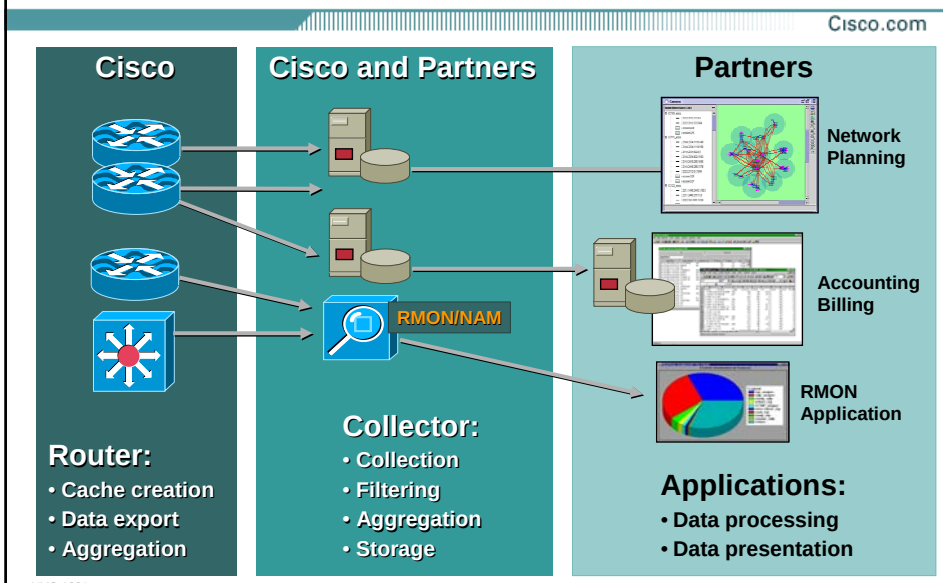
```
router (config-if)#ip route-cache flow
router (config)#ip flow-export destination
  172.17.246.225 9996
router (config)#ip flow-export version 5 <peer-as |
  origin-as>

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: Summary

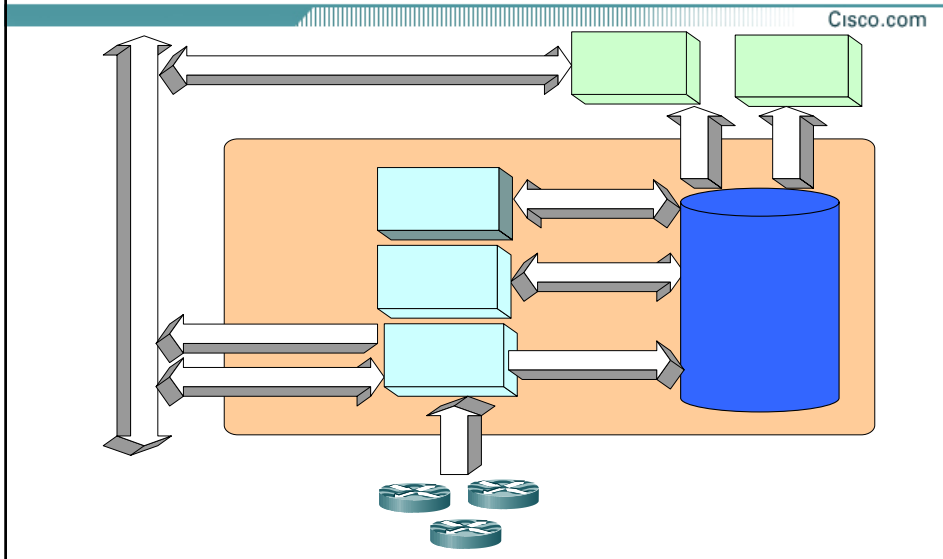
Cisco.com

- **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 Infrastructure

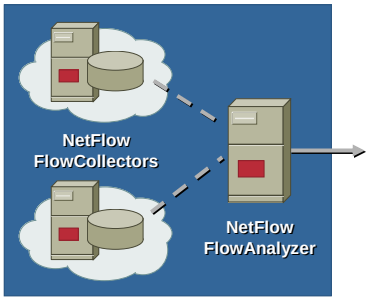


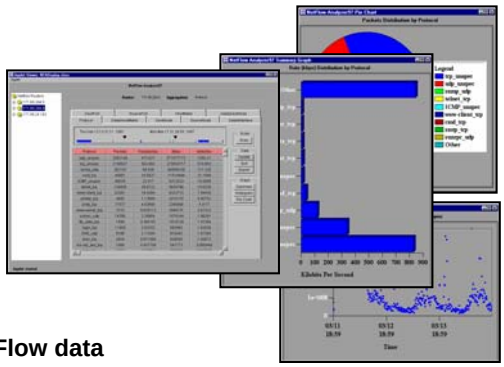
NFC 5.0 - System Overview



Network Data Analyzer (included)

Cisco.com





- Graphical display of NetFlow data
- Consumes from NetFlow FlowCollector(s)
- Time-based analysis ands data sorting
- Configure routers and FlowCollectors
- Histograms, bar charts, and pie charts
- Spreadsheet data export

Cisco.com

Network Analysis Module

Performance Management Traffic Analysis

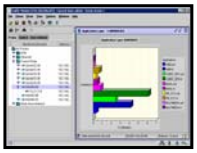
Cisco.com

- **Network Analysis Module**
  - Integrated Traffic Monitoring solution for Catalyst 6000 Family
- **Enables full Traffic Monitoring**
  - Real time traffic analysis
  - Performance monitoring
  - Troubleshooting
- **Web based embedded Traffic Analyzer**
  - VoIP, QoS(DSMON), ART, VLAN(SMON), RMON 1&2 monitoring
  - Data Capture and Decode, Alarms
- **Supported by other applications**
  - nGenius Real-Time Monitor, CiscoView, Concord eHealth

NAM Solution

Cisco.com

"Visibility" integrated into the network to serve variety of applications



nGenius Real Time Monitor
or 3rd party applications
(aggregation of multiple NAMs)

SNMP

Enhanced

HTTP/S

NAM Blade

NAM Integrated Traffic Analyzer
(easy to deploy and use)

Flexible data sources:
SPAN (detailed)
Netflow (broad)
VACL (specific)

Enhanced

Layer 2
Mini-RMON
Per Port

Layer 3-7
RMON I,II
HCRMON
SMON
DSMON
ART
Voice Analysis

Catalyst 6000/6500
Cisco 7600

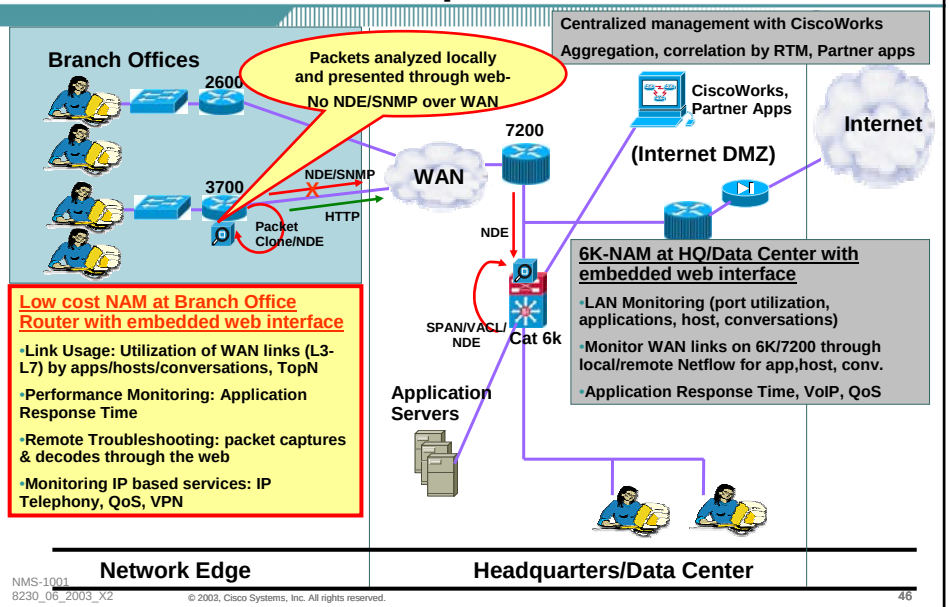
NEW

Network Analysis Module (NAM)

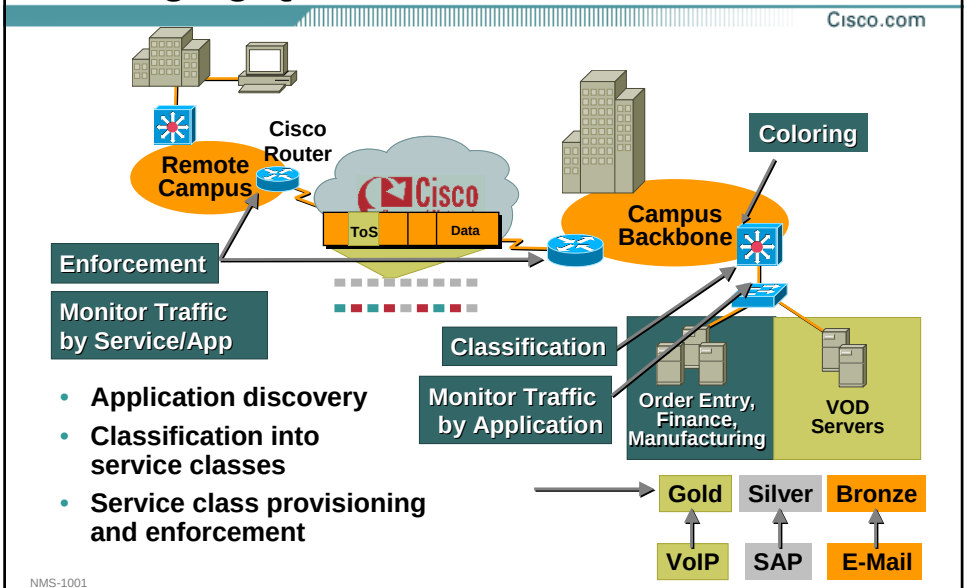
Enables standards based, real- time and historical monitoring of data/voice traffic

- **Integrated monitoring for LAN and WAN**
  - Utilize a variety of data sources and NetFlow for comprehensive LAN/WAN monitoring
- **Real time and historical traffic analysis**
  - Full RMON2, extended RMON, IP Telephony and QoS monitoring with in-built, web accessible Traffic Analyzer
- **Performance management**
  - Detect violation of QoS policies; application response time delays, VoIP quality degradation
- **Troubleshooting**
  - Web based packet capture and decodes to isolate problems

Customer Value Proposition



Performance Management
Managing QoS



- Application discovery
- Classification into service classes
- Service class provisioning and enforcement

NAM features

- Port Utilization (mini-RMON)
- Applications,Hosts, Conversations (RMON2)
- VLAN Monitoring (SMON)
- Server Response Time (ART)
- QoS Monitoring (DSMON)
- VoIP Monitoring
- WAN Traffic Monitoring (NDE/VACL) NEW
- Web based, real time packet capture & decode
- Alarms
- Historical Reporting NEW
- Aggregation with CiscoWorks Real Time Monitor
- Supports other standards based applications

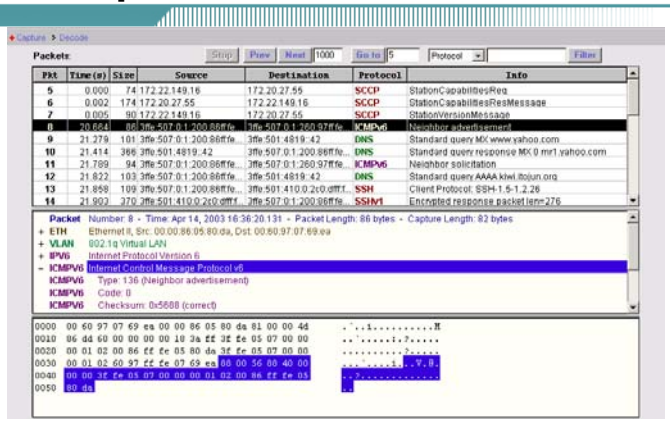
NAM applications

Cisco.com

- **Integrated visibility into LAN & WAN**
  - LAN monitoring with SPAN/VACL
  - WAN with NDE/VACL NEW
- **Real Time & Historical Monitoring**
  - Protocol distribution, Top Talkers
  - Unknown applications
  - Historical reports NEW
- **Performance Management**
  - Server/Application Response Time
- **Fault Isolation & Troubleshooting**
  - Threshold alarms
  - Web based packet capture & decode
- **QOS & VoIP Monitoring**
  - VoIP – calls/phones/protocols
  - QoS(DiffServ)
- **Capacity Planning & Extended Applications**
  - Reporting & Trending using external apps

NAM SW v3.1: Packet Capture & Decode Enhancements

Cisco.com



- New resizable 3 pane views with color coding
- Support for Mobile IP, SAN protocols
- Trigger based captures (start & stop)