



# Network Configuration Change Management

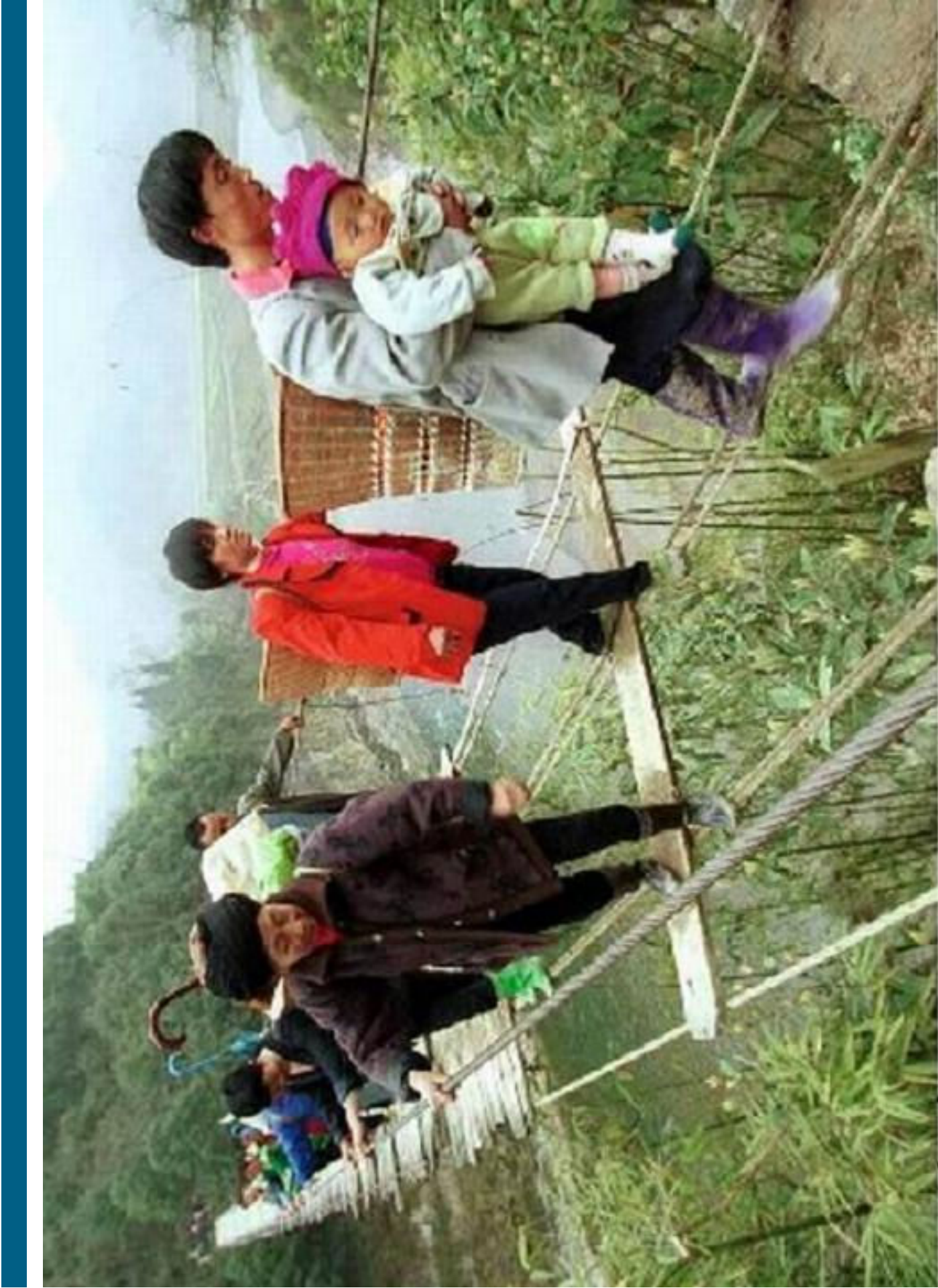
**Dirk Anteonis**  
**March 2008**





# Agenda

- Stable Infrastructure vs. Changing Demands
- What is Network Management ?
- The CFO's view
- NCM Product Overview
- Visibility
- Questions are welcome
- Mobile phone ringtones are not



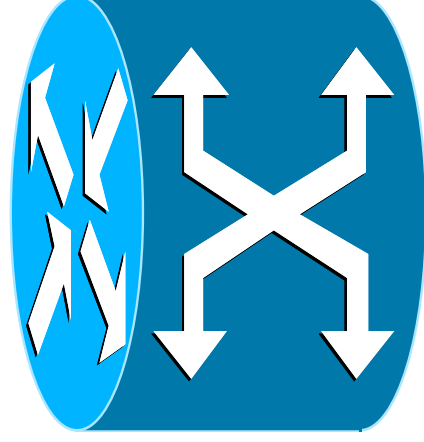
# Infrastructure =

```
r1#sh run
...
router bgp 12
no synchronization
bgp log-neighbor-changes
network 137.1.200.0 mask 255.255.255.0
neighbor 137.1.200.2 remote-as 12
no auto-summary
```

...

**+** **IOS 12.4(19)**

**+**



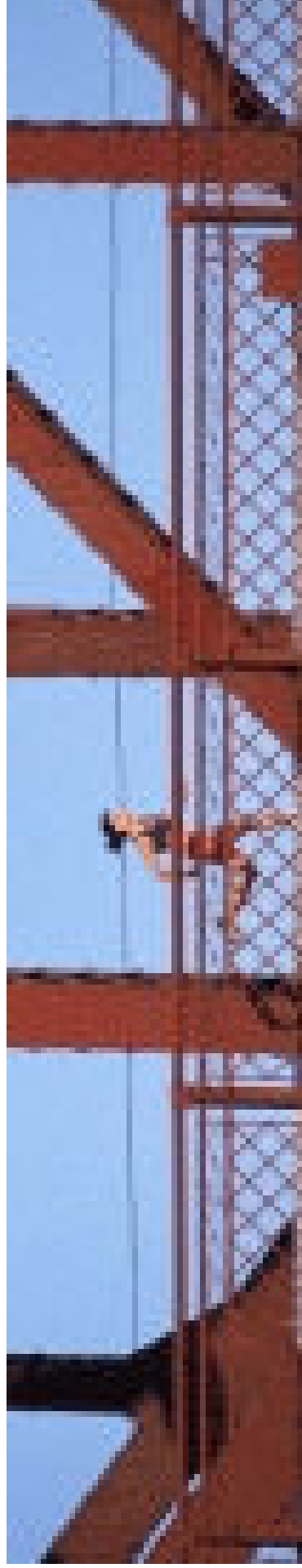


# Stable Network Infrastructure =

- Reliable hardware
- Reliable OS
- Well-known configuration
- Efficient processes



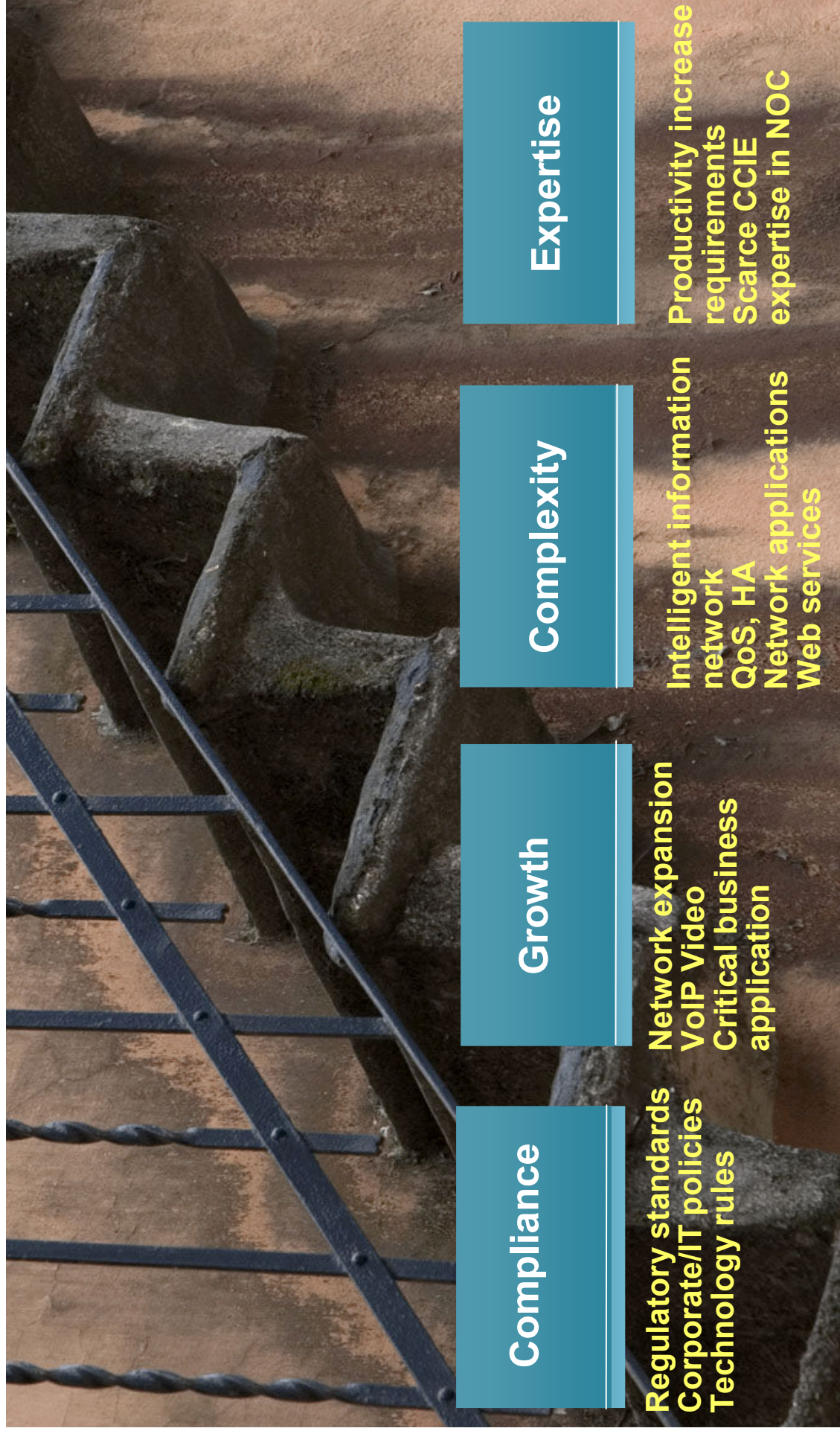
# Situation Analysis



## Automate configuration and change management operations to keep the network functional and compliant 24x7

- How do I set up and configure equipment for a new remote location?
- What policies should apply to a new location and new configuration?
- How do I give access to tools and devices for people to manage new network elements? Who can make different kinds of changes?
- How do I know the intended configurations were rolled out and the correct permissions set up?
- How can I replicate changes easily and quickly again?
- How do I comply to a new internal policy for accessing information?
- Who is making changes to data access permissions?
- How do I report on who has access and what changes to entitlement may have taken place?
- How do I analyze network integrity
- How can I perform an IOS upgrade with minimum downtime and with consistency throughout the network?
- How do I ensure that an upgrade which is correct for an element in one part of the network will also be correct for a similar element in a different part of the network?
- How do I audit after deployment to ensure compliance?
- How do I validate and report on the network's compliance to best practices?

# Multi-faceted Demands



# What is Network Management ?





# What is Network Management ?

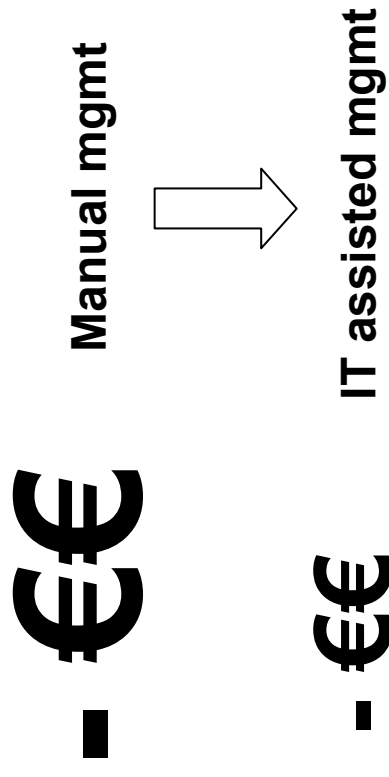
- Similar to a doctor treating a patient, similar to managing national health
- Because somebody wants to *achieve a goal*
- Steps:
  - 1) Observe or Monitor
  - 2) Interfere; i.e. change the behaviour
  - 3) Measure; similar to Monitor, but more precise data
  - 4) Report; produce intelligible info for others

# The CFO's view



# Why NMS ?

- Why Network Management **Systems** ?
- Enable owners of (Cisco) Kit to save on spending €€ while managing the kit



# Why Use a NCCM tool ?

**47% of changes are unauthorized or not accounted**

**Configuration  
Is Still Manual**

**Most Problems  
Detected After  
Deployment**

**Even Small Errors  
Can Cause Large  
Issues**

**Compliance Is  
Usually Poorly  
Understood**

**Extreme Control  
Measures Are  
Often Used**

**“Process” Often  
Limited to Paper  
Flow Diagrams**

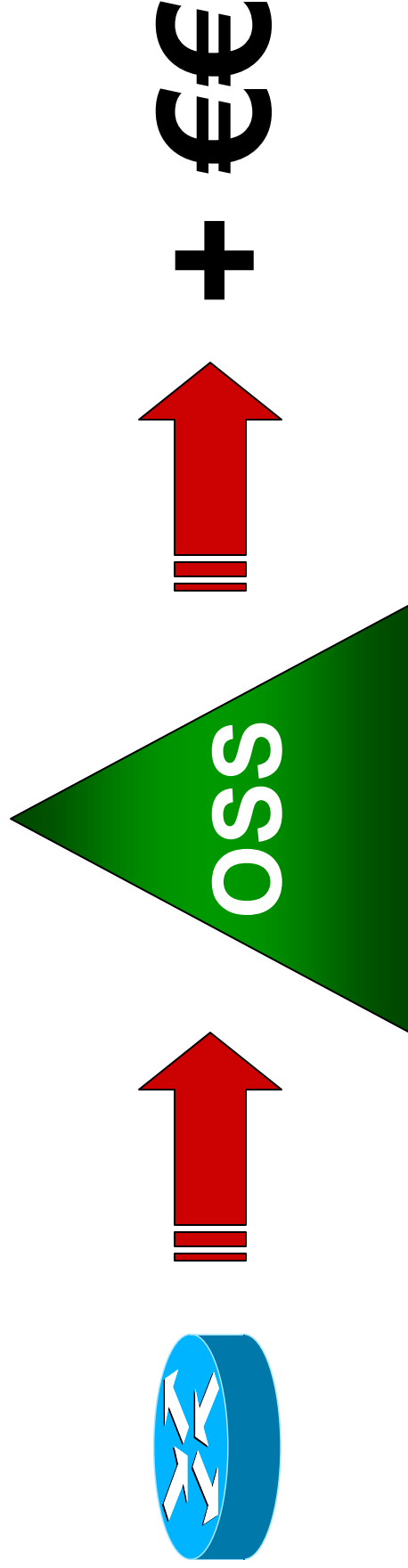
**60% of network downtime is due to human error**



---

## About OSS

- Operations **S**upport **S**ystems help Service Providers to make €€ from (Cisco) Kit
- Some non-networking issues are taken care of also



---

## Customer statement

“

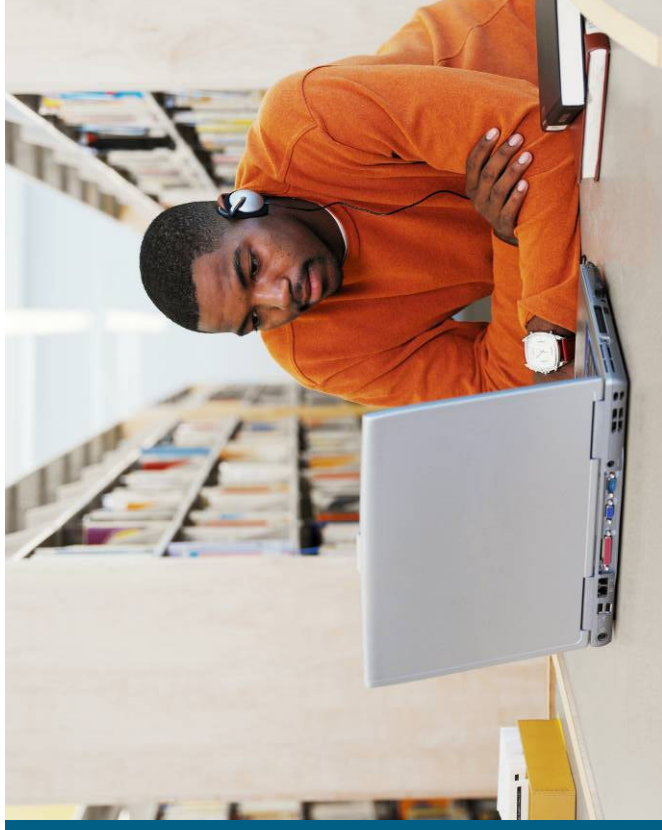
**"Cisco, Alcatel, it doesn't matter. What matters is how quickly you can offer new services. VPN, voice, you can only do it once the [OSS] systems are in place."**

”

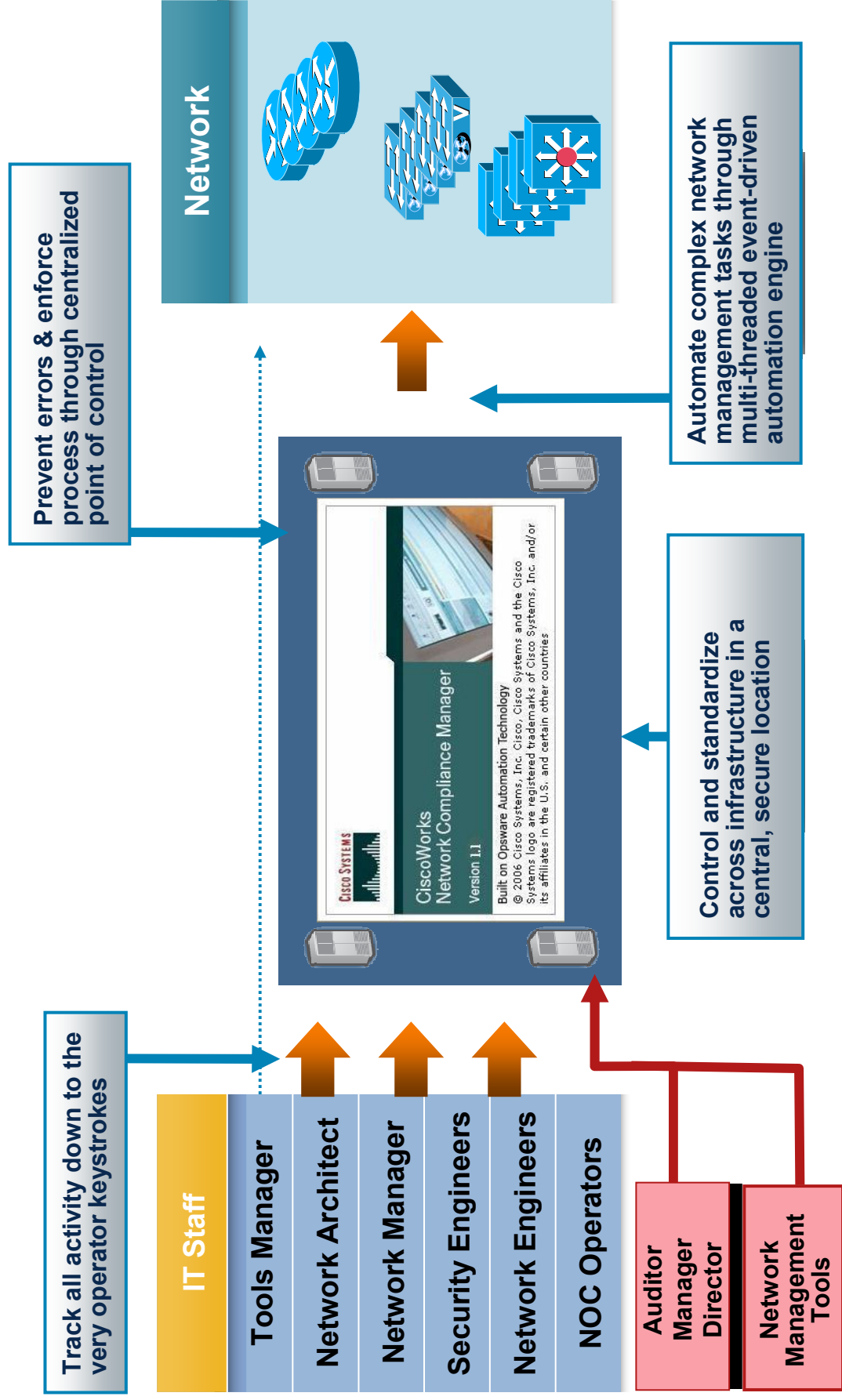


Hans Rietkerk, Managing Director BB-Ned

# NCM Product Overview



# Network Compliance Manager (NCM)





# CiscoWorks NCM Objectives

**Software used by  
organizations to automate change management  
and compliance of network devices**



## Immediate Benefits

- Automated config. mgmt
- Improved visibility
- Ensure compliance
- Improve security
- Improve network uptime



## Generate Massive Efficiency & Quality Gains

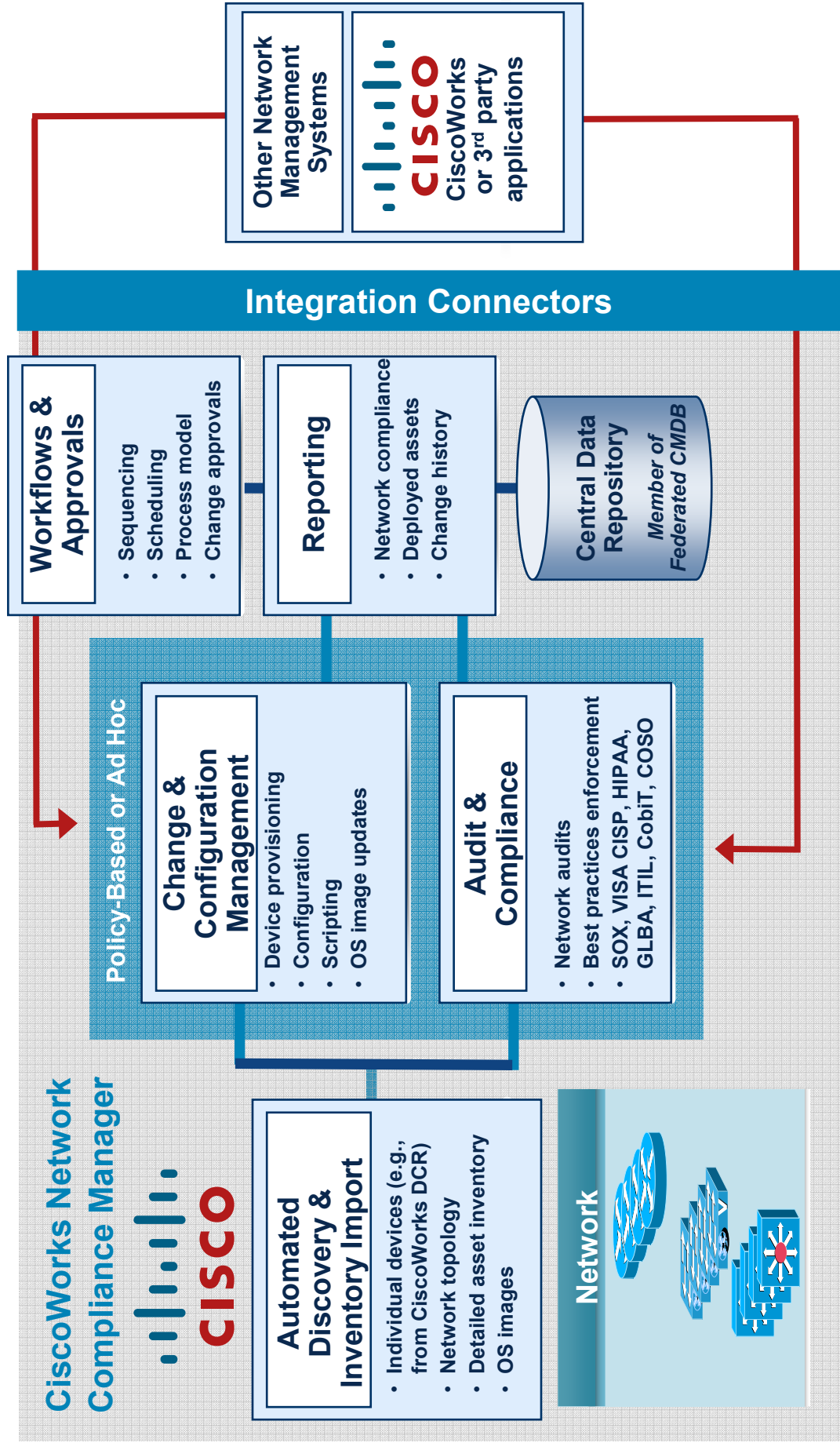
- Improved productivity (network device : engineer ratios)
- Operational standardization
- Improved quality

---

## How do we achieve the objectives?

- **Track**
- **Control**
- **Automate**
- **Prevent**

# NCM Functional Overview

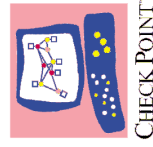


# CiscoWorks NCM Extensive, Multi-Vendor Device Support

Supports over 500 device models across Cisco and other vendors



**CISCO**





# Advanced Workflow and Approvals

## Close the change loop with real-time process enforcement

- Model complex projects
  - Combine automated and manual activities
- Define custom approval policies
  - Require approval based on user, activity and/or device affected
  - Require approvals for manual or automated activities
  - Grant permission for approval overrides
  - Integrate with external workflow and process systems
- Daily activity calendar
- Conflict alerts
- Flexible reporting & notification
  - Change reporting dashboard
  - Email /other notifications

The screenshot shows the Cisco Systems Workflow Wizard interface. The main content area is titled "Step 3: Manage Approval Rules". It contains a list of approval rules with arrows indicating their priority. The rules are:

- All Users approved by Administrators
- Tier 2 Must Approve Tier 1
- Ops, Security, and NOC Mgr Approvals

A callout box on the right side of the screenshot is titled "Change Approval Rules" and contains three arrows pointing to the right, indicating the direction of the workflow.



# NCM Alert Center

## What is it?

Optional subscription service that provides NCM users with ongoing updates of security alerts and automation packs

## Benefits:

**Security Alerts**– vendor security alerts translated into NCM software policies

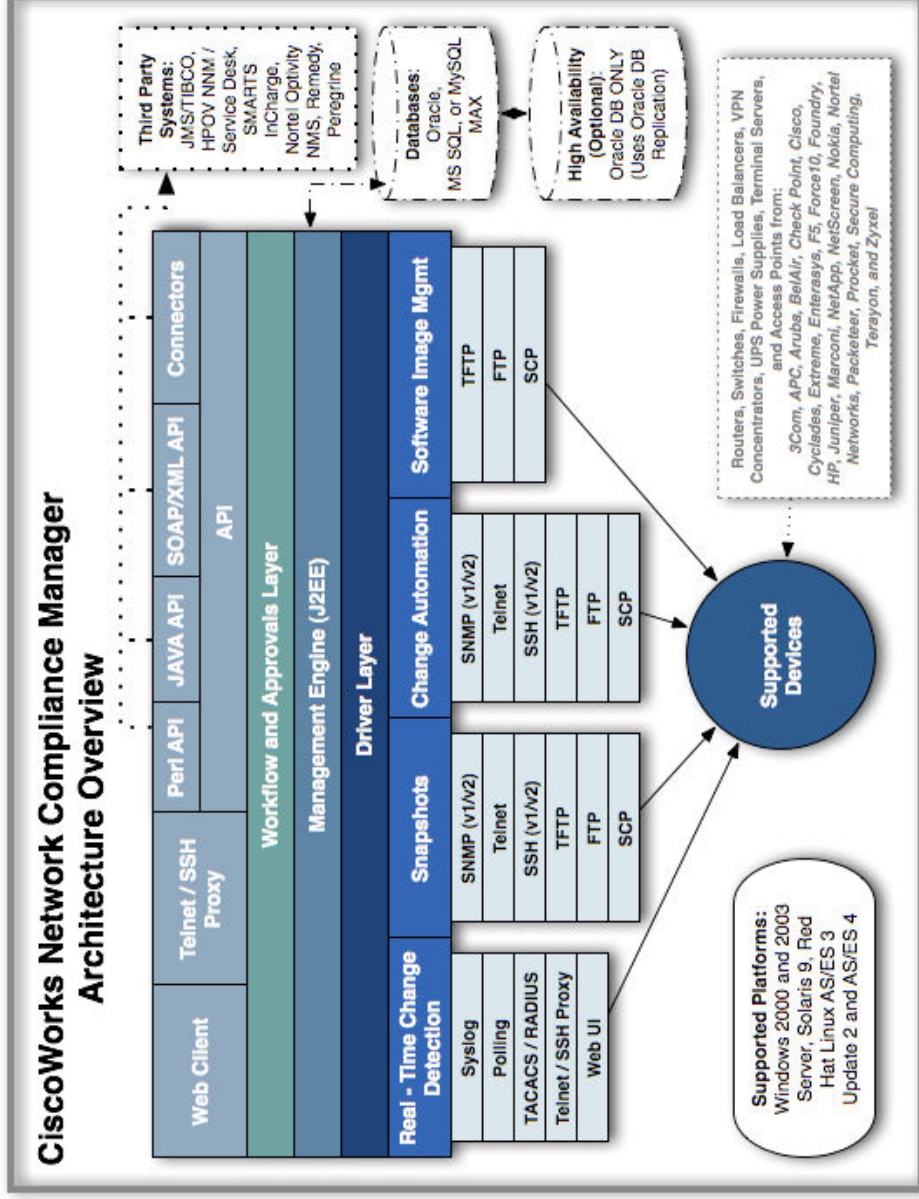
**Shared Product Extensions** – leverage scripts, packages and policies

**Functionality Updates** – new capabilities available outside the release cycle

## NCM Alert Center – Security Alerts

- Automatically downloads and continuously updates Network Vulnerability Alerts
- Based on industry leading alert service
- NCM translates alerts into Software Compliance Policies
- NCM server securely downloads new alerts (approx. ~3-5 per week)
- Users can review and activate desired policies in their environment

# NCM Architectural Overview



## Robust Security Model

- Device-level access per user
- Task-level access per user
- Sensitive Data Masking and Encryption

## Directory Services & AAA Integration

- LDAP / Active Directory
- RADIUS / TACACS
- SecureID

## High Availability Configurations

- High Availability Replication
- Satellite Off-loading
- Microsoft and Veritas (Solaris) Clustering

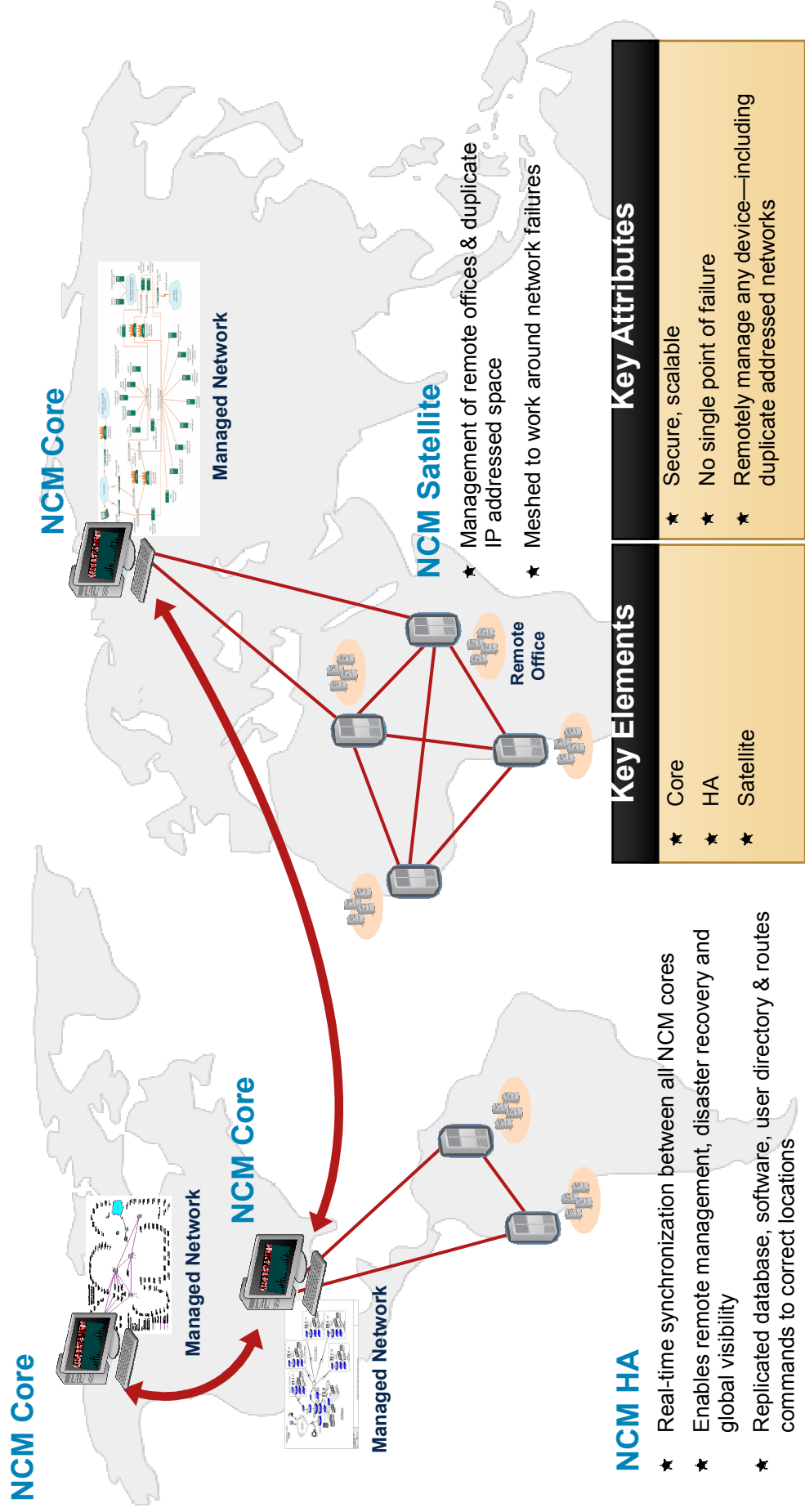
## Extensibility

- APIs (Perl, Java, Web Services (XML))
- Open database schema
- Integration with CiscoWorks and 3<sup>rd</sup> party NMS



# CiscoWorks NCM High Availability Features

## Active/Active Management via High Availability Database Replication



# Visibility



# Configuration Change Management

## Maximized uptime during change management

- Centralized software & configuration deployment
- Real-time change detection
- Visual configurations comparisons
- Configuration templates
- Pre-deployment validation of changes & pro-active policy enforcement
- Secure device access
- Historical configuration archive

The screenshot displays the Cisco Systems Configuration Manager interface. At the top, there are navigation tabs: Home, Search, My Workspace, My Favorites, My Settings, Devices, Tasks, Policies, Reports, Admin, Support, Docs, Logout. The main content area is titled 'Compare Device Configurations'. It shows a comparison between two configurations for device 'Contivhd00 (10.255.1.56)'. The 'Older Configuration' is compared with the 'Newer Configuration'. The interface highlights differences in configuration lines. A blue arrow points from a box labeled 'Visual Difference Comparisons' to a specific line in the comparison table.

Line	Older Configuration	Newer Configuration
083	syslog add 10.1.2.153	syslog add 10.1.2.153
084	syslog add 10.1.2.180	syslog add 10.1.2.180
085	syslog add 10.1.2.96	syslog add 10.1.2.96
086	syslog add 132.168.131.72	syslog add 132.168.131.72
087	tcpserver	tcpserver
088	telnetd start	telnetd start
089	webproxy start	webproxy start



# Layer 2 Modeling

## Provides layer 2 networking intelligence

### The Challenge

- No visibility into network <-> server dependencies
- Armed with the MAC address of a server, users are unable to complete the puzzle
  - what the IP Address of the server?
  - which network switch is that server attached to?

### NCM Solution

- Capture and store L2 information for managed devices and attached nodes
- Calculate L2 topology from device configurations and diagnostics
- MAC – port – switch – interface – router mapping tool

MAC Search Results [Modify this search](#)

3 results

Host Name	Port Name	Address	Type	VLAN	Remote Location	First Seen	Last Seen
DALAB-C3640-R1	Ethernet0/3	00-14-22-73-49-06	seen from port			Jan-18-06 13:58:22	current
DALAB-CAT2900XL	FastEthernet0/20	00-14-22-73-49-08	seen from port	VLAN30		Jan-18-06 13:58:13	current
DALAB-C3640-R1	Ethernet0/3	00-14-22-73-49-08	seen from port			Jan-18-06 13:57:11	current

3 results

Display results

Immediately locate device & port MAC address is seen

# VLAN Management

Provides VLAN networking intelligence

## The Challenge

- Distributed VLANs cause complexity
  - Which switches participate in VLAN 101?
- Tracking servers to VLAN segments
  - Which servers are in Finance VLAN?

## NCM Solution

- Instantly identify VLAN based on MAC/port/switch data
- Real-time VLAN reports

Opware Network Automation : MAC Search Results - Microsoft Internet Explorer provided by Opware Inc.

Address: https://ncpocquery.execute.ap.filterType=MAC&filterID=500138&filterName=NO\_TC\_search\_MACCopy&size=25

Support: Docs The Opware Network Logout

admin Feb-06-06 08:11:04

### MAC Search Results

138 results Page 2 of 6

Host Name	Device IP	Device Name	Address	Type	Remote Location
SI5CO0000-1	172.16.52.2	Ethernet0/0	00-0B-1E-80-19-20	address of port	Jan-24-06 16:01:57 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-10-03-0A-4A-09	seen from port	Jan-19-06 11:14:19 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-10-58-01-17-2C	seen from port	Jan-06-06 16:54:56 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-60-16-82-3B-81	seen from port	Jan-06-06 16:54:56 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-13-49-14-F4-BA	seen from port	Jan-27-06 13:39:29 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-01-30-12-2F-49	seen from port	Jan-06-06 16:54:56 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-01-30-8C-FC-00	seen from port	Jan-19-06 11:14:16 curr
SI5027206	10.255.1.20	FastEthernet0/0	00-01-81-CC-52-5E	seen from port	Jan-06-06 16:54:56 curr
DALAB-C2800-10	172.16.50.2	Ethernet0/0	00-10-7B-39-02-59	address of port	Jan-24-06 16:01:58 curr
DALAB-C2800-10	172.16.50.2	Ethernet0/0	00-11-11-2F-78-D2	seen from port	Jan-24-06 16:01:59 curr
DALAB-C2800-10	172.16.52.2	Ethernet0/0	00-14-22-	seen	Feb-01-06 curr

My Workspace  
Current Device  
L2LAB-SW02-C2900d  
Inventory  
Current Device Group  
My Favorites  
My Settings  
My Profile  
My Workspace  
My Permissions  
Change Password

Produce real-time reports of VLAN membership



# Prioritized Triage of Compliance Violations

Pushing the most critical violations to the forefront

## The Problem

- Compliance violations are not all created equal
- No way to filter and triage hundreds or thousands of compliance violations besides manual review

## Prioritized Compliance Rules

- Each violation has a risk rating
- Automated triage based on risk ratings, such as:
  - Auto-remediate
  - Open new trouble ticket
  - Send email / page
  - Email daily summary

Rule Name	Device Family	Description	Importance
Access Lockout - Cisco IOS	Cisco IOS	Access to console or vty line is locked after unsuccessful attempts	High
Console Timeout - Foundry	Foundry	Specify a 10 min timeout on Console connections	High
Debug & Log Messages - Cisco IOS	Cisco IOS	Sequence number and timestamps of all debug & log messages.	Low
Disable Bootp - Cisco IOS	Cisco IOS	Disable Bootp Service	Medium
Disable Finger - Cisco IOS	Cisco IOS	Disable IP Finger Services	Low
Disable Ident - Cisco IOS	Cisco IOS	Disable Identification Services	Medium
Enable CEF - Cisco IOS	Cisco IOS	Enable CEF or distributed CEF	Medium
Ensure Password Encryption - Cisco IOS	Cisco IOS	Enable Password Encryption	Critical
Min 6 Character Password Length - Cisco IOS	Cisco IOS	Enforce a minimum password length	High
No Gratuitous ARPS - Cisco IOS	Cisco IOS	don't allow gratuitous arps	Low
No PAD Service - Cisco IOS	Cisco IOS	Disable PAD	Low
No Proxy ARP - Cisco IOS	Cisco IOS	Disable Proxy-arp	Medium
No Proxy ARP - Foundry	Foundry	Disable Proxy-arp	Medium
No Source Routing - Cisco IOS	Cisco IOS	Disable IP Source Routing	Low
No Source Routing - Foundry	Foundry	Disable IP Source Routing	Low

Prioritize Compliance Rules

# Security Management

## Patching, lock-down & centralized ACL management

- Centralized patch management
- Telnet/SSH Proxy  
Single sign-on  
Full session logging  
Centralized enforcement of privileges and approval policy
- Advanced ACL management  
View & search current ACLs, historical ACLs and audit trails  
Persistent ACL comments & handles  
Batch ACL edits for rapid vulnerability response  
ACL Templates

The screenshot shows the Cisco Systems ACL Search Results page. The table displays 207 results. The columns are Host Name, ACL Id, Handle, Type, and Last Modified. The 'Actions' column contains links for 'View ACL | ACL History' and 'Edit ACL | View ACL | ACL History'. A callout box labeled 'ACL Change History' points to the 'View ACL | ACL History' link for the entry with ACL Id 186.

Host Name	ACL Id	Handle	Type	Last Modified	Actions
lab-3640-r1	104	104	IP extended	Oct-20-04 13:30:02	<a href="#">View ACL   ACL History</a>
lab-3640-r1	101	101	IP extended	Oct-20-04 13:30:02	<a href="#">View ACL   ACL History</a>
lab-3640-r1	104	104	IP extended	Nov-11-04 10:42:37	<a href="#">View ACL   ACL History</a>
lab-3640-r1	101	101	IP extended	Nov-30-04 11:16:37	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	150	150	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	153	153	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	115	115	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	36	36	IP standard	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	155	155	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	31	31	IP standard	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	102	102	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	94	94	IP standard	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	186	186	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>
lab-7200-r1	123	123	IP extended	Nov-11-04 10:21:47	<a href="#">Edit ACL   View ACL   ACL History</a>

ACL Change History

# Reporting

## Pre-defined and custom reports

- Report on device inventory
  - By group, vendor, user
- Change reporting
  - Who changed what, why & when
- Compliance reporting
  - Regulatory compliance
  - Corporate compliance
  - NSA Router best practices
- Network status reports
  - Policy compliance at-a-glance
  - Identify and address risk factors

**Top 10 Most Accessed Devices**

Hostname	IP Address	#
172.31.152.26	172.31.152.26	3786
192.168.2.1	192.168.2.1	62
10.255.1.39	10.255.1.39	32
10.255.1.37	10.255.1.37	21
10.255.1.81	10.255.1.81	18
10.255.1.42	10.255.1.42	10

**Network Status Report**

Report Date: Jan-28-05 14:59:55  
Device Groups Reported: 1

**Device Group: Inventory (51 Devices)**

High risk = 4%  
Moderate risk = 37%  
Low risk = 59%

**Network Status Report Details**

Host Name	Device IP	Software Version	Compliance	Actions
1208Router	192.168.1.40	12.1	Security Risk	View Detail
10-255-1-38	10.255.1.38	12.1	Security Risk	View Detail

Startup vs. Running Configuration Mismatch: 4

Host Name	Device IP	Last Change Time	Actions
			Red

Network Status Reports

---

## Take-Away

- Cisco provides a multi-vendor **Network Configuration Change Management** tool
- NCM scales to 1000nds and is highly available
- Analyses the configuration file for policy compliance, layer 2 topology
- Can be linked to [cisco.com](http://cisco.com) to automatically download policies

