Network Configuration Change Management

Dirk Anteunis

March 2008

Agenda

- Stable Infrastructure vs. Changing Demands
- What is Network Management ?
- The CFO’s view
- NCM Product Overview
- Visibility

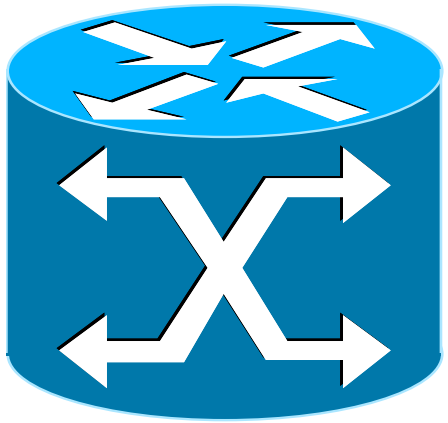
- Questions are welcome
- Mobile phone ringtones are not

Infrastucture =

```
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)

+

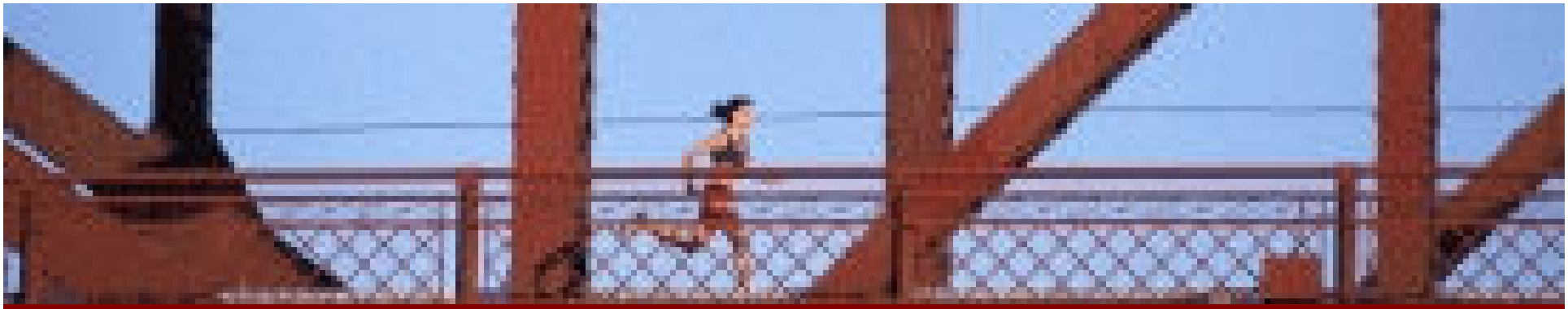


Stable Network Infrastructure =

- Reliable hardware
- Reliable OS

- Well-known configuration
- Efficient processes

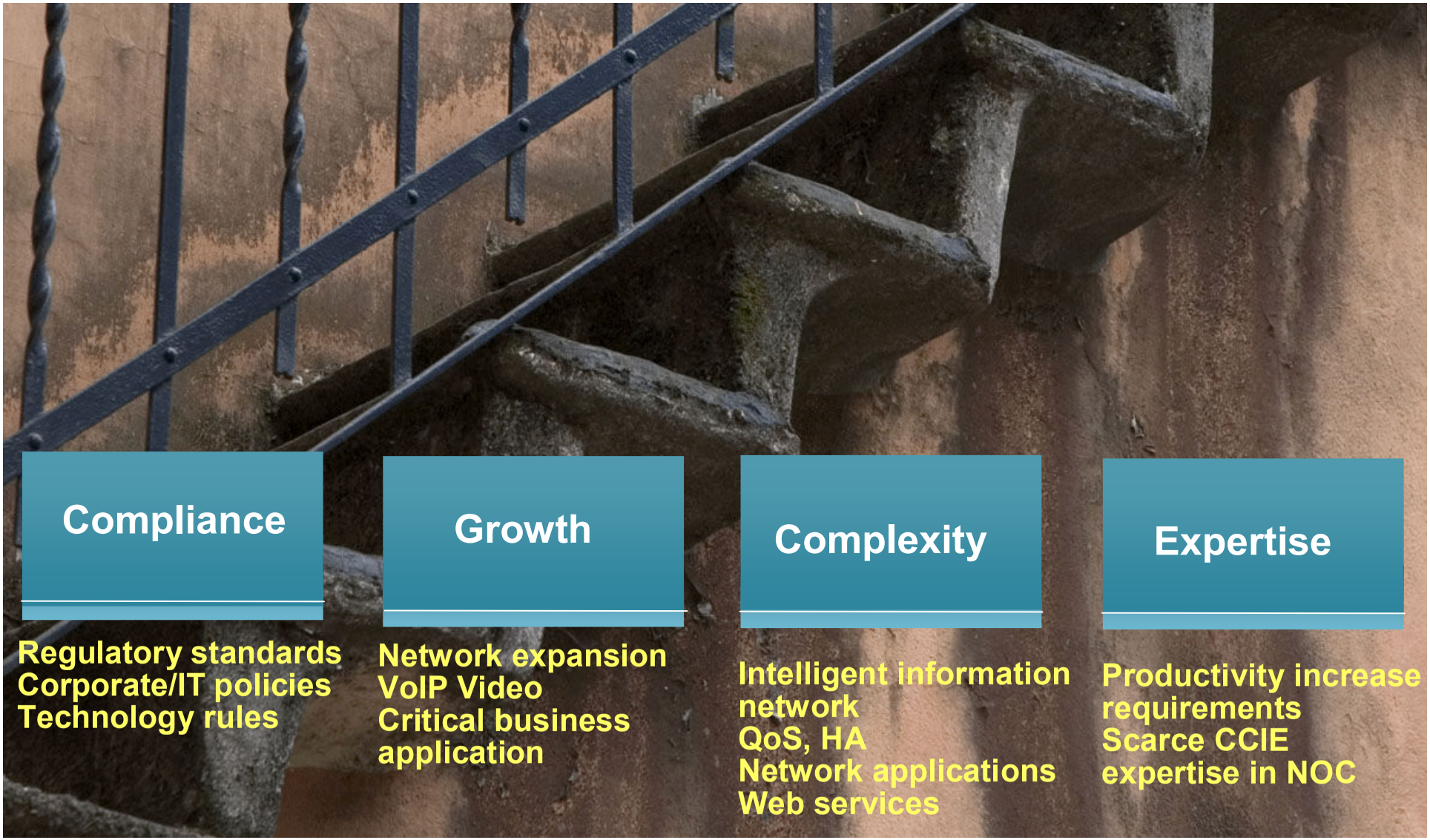
Situation Analysis



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 ?

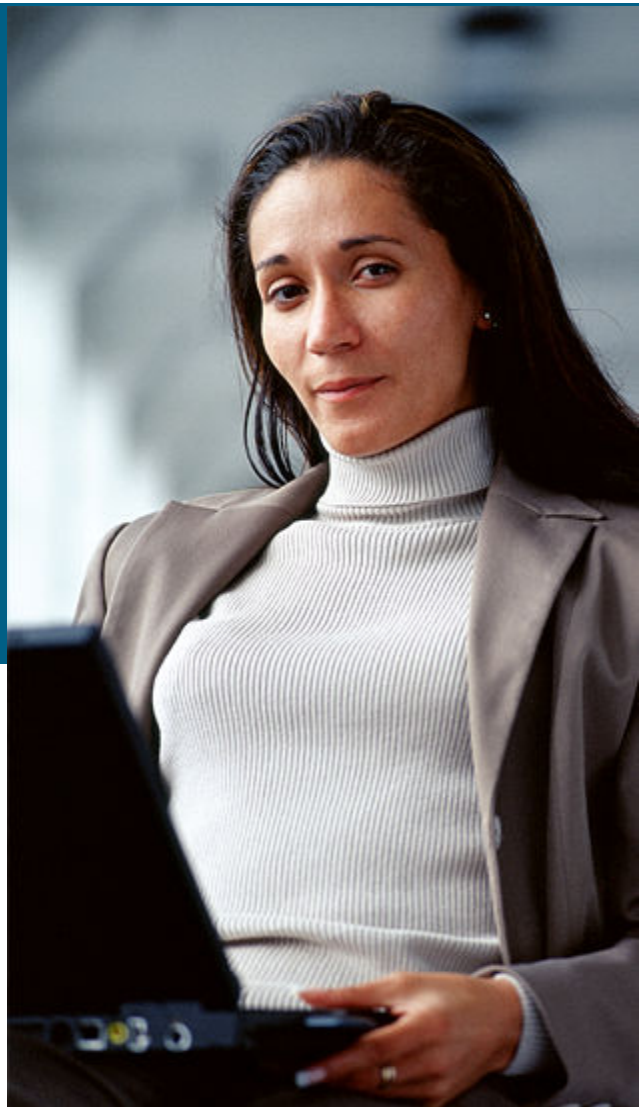
What is Network Management ?

- Similar to a doctor treating a patient, similar to managing national health

- Because somebody wants to *achieve a goal*

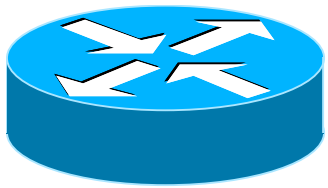
- Steps:
  1) Observe or Monitor
  2) Interfere; i.e. change the behaviour
  3) Measure; similar to Monitor, but more precise data
  4) Report; produce intelligible info for others

The CFO’s view



Why NMS ?

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

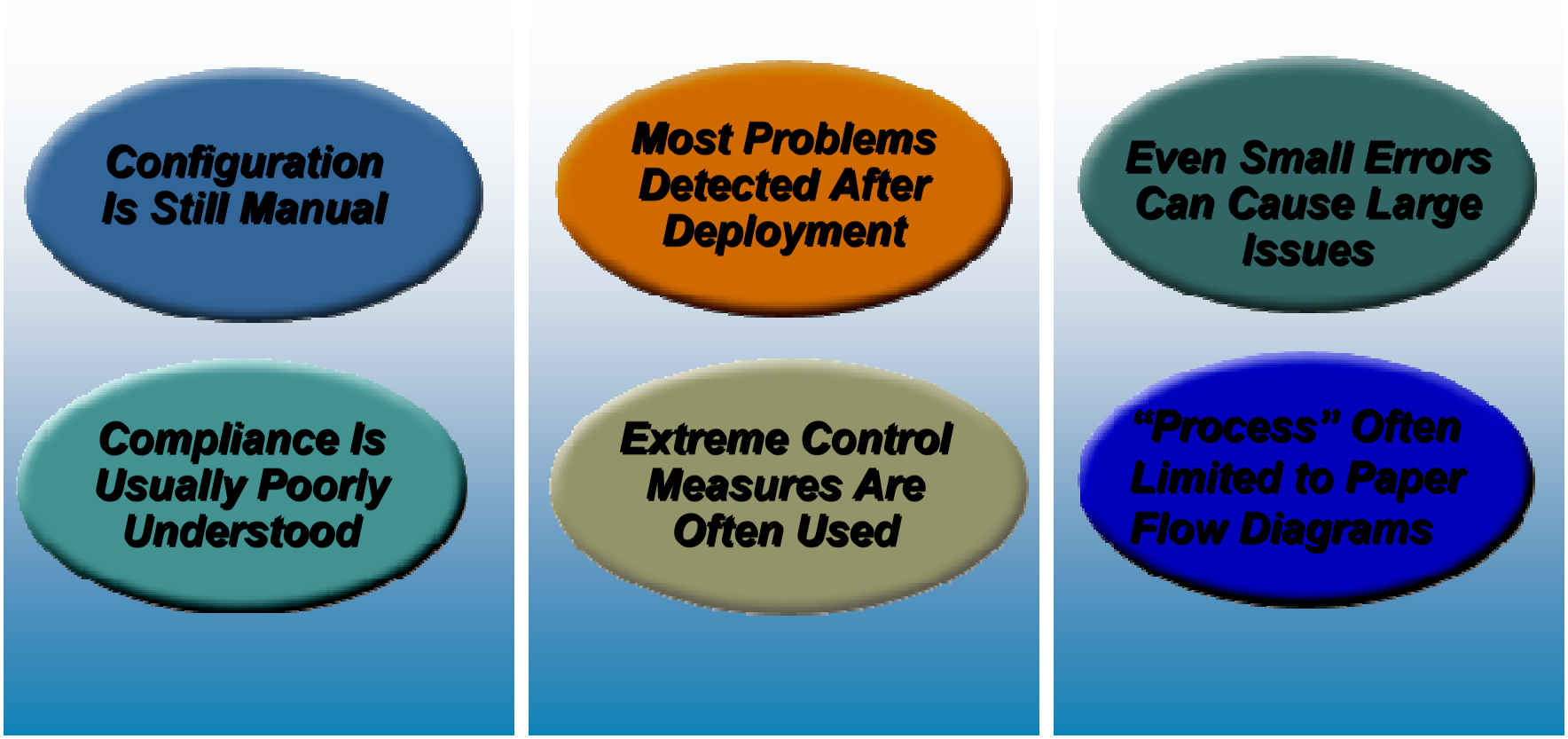


- €€ Manual mgmt

- €€ IT assisted mgmt

Why Use a NCCM tool ?

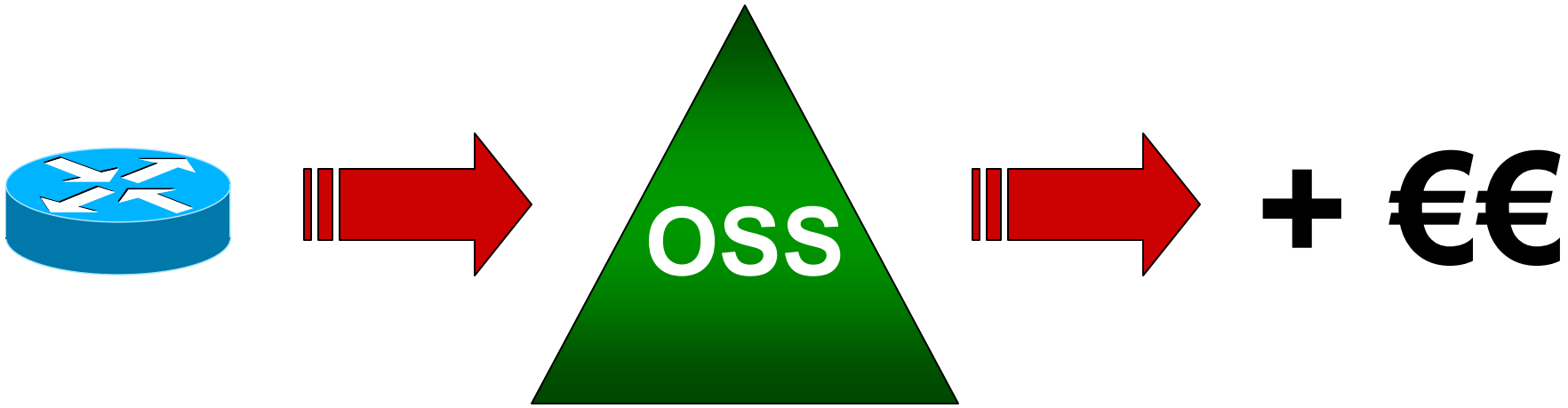
47% of changes are unauthorized or not accounted



60% of network downtime is due to human error

About OSS

- Operations Support Systems help Service Providers to make €€ from (Cisco) Kit
- Some non-networking issues are taken care of also



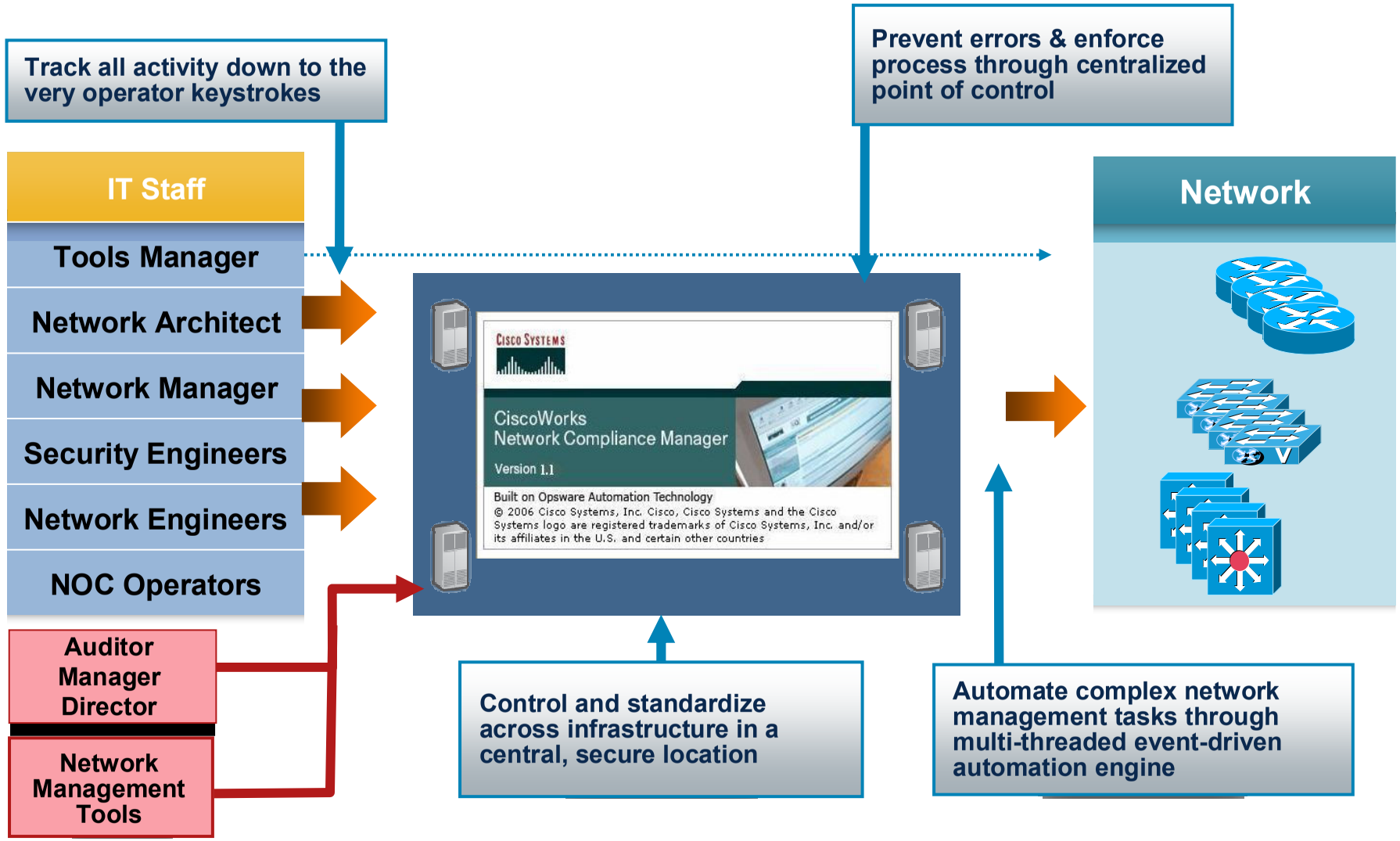
Customer statement

"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."

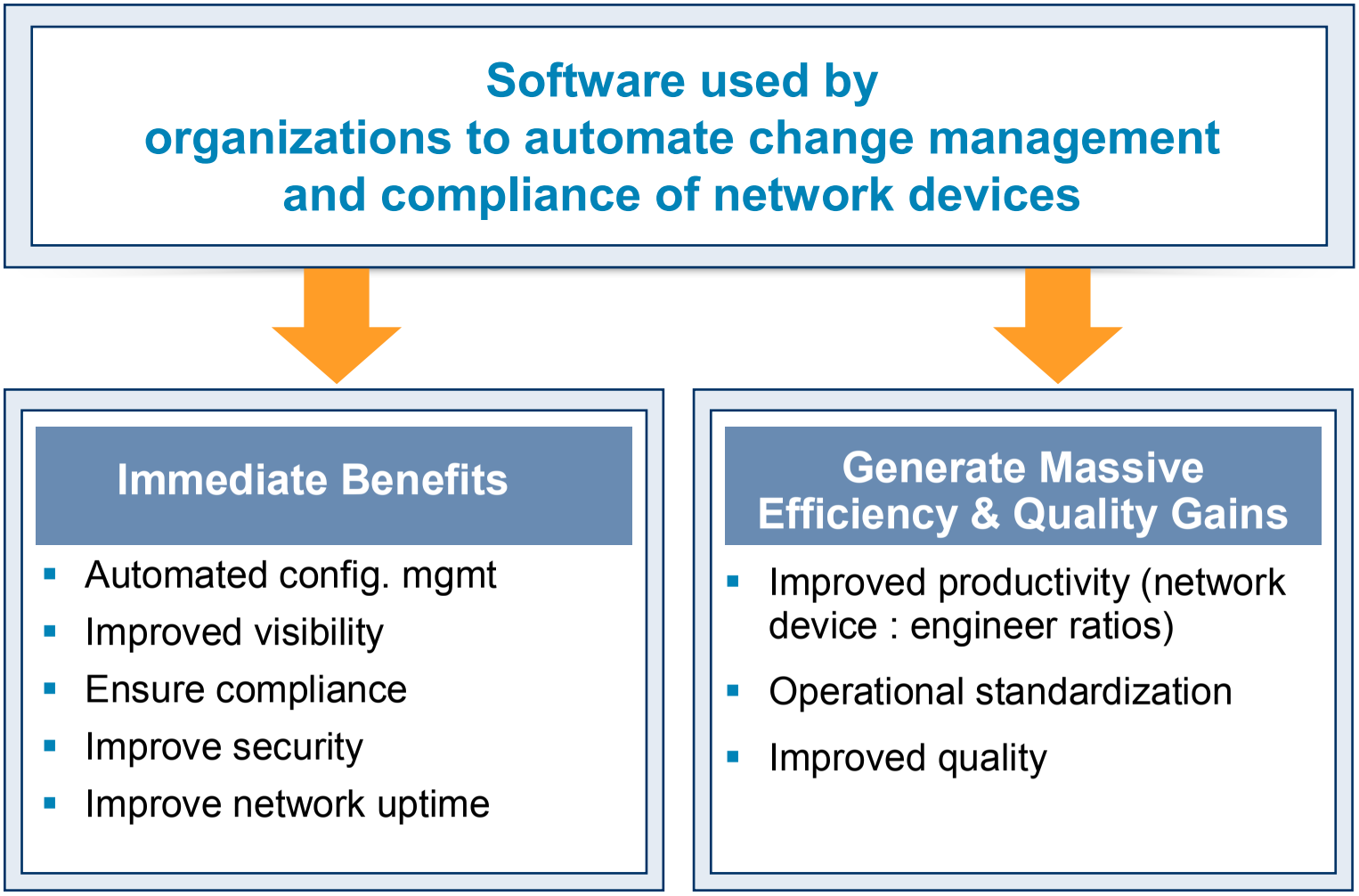
Hans Rietkerk, Managing Director BB-Ned

NCM
Product Overview

Network Compliance Manager (NCM)



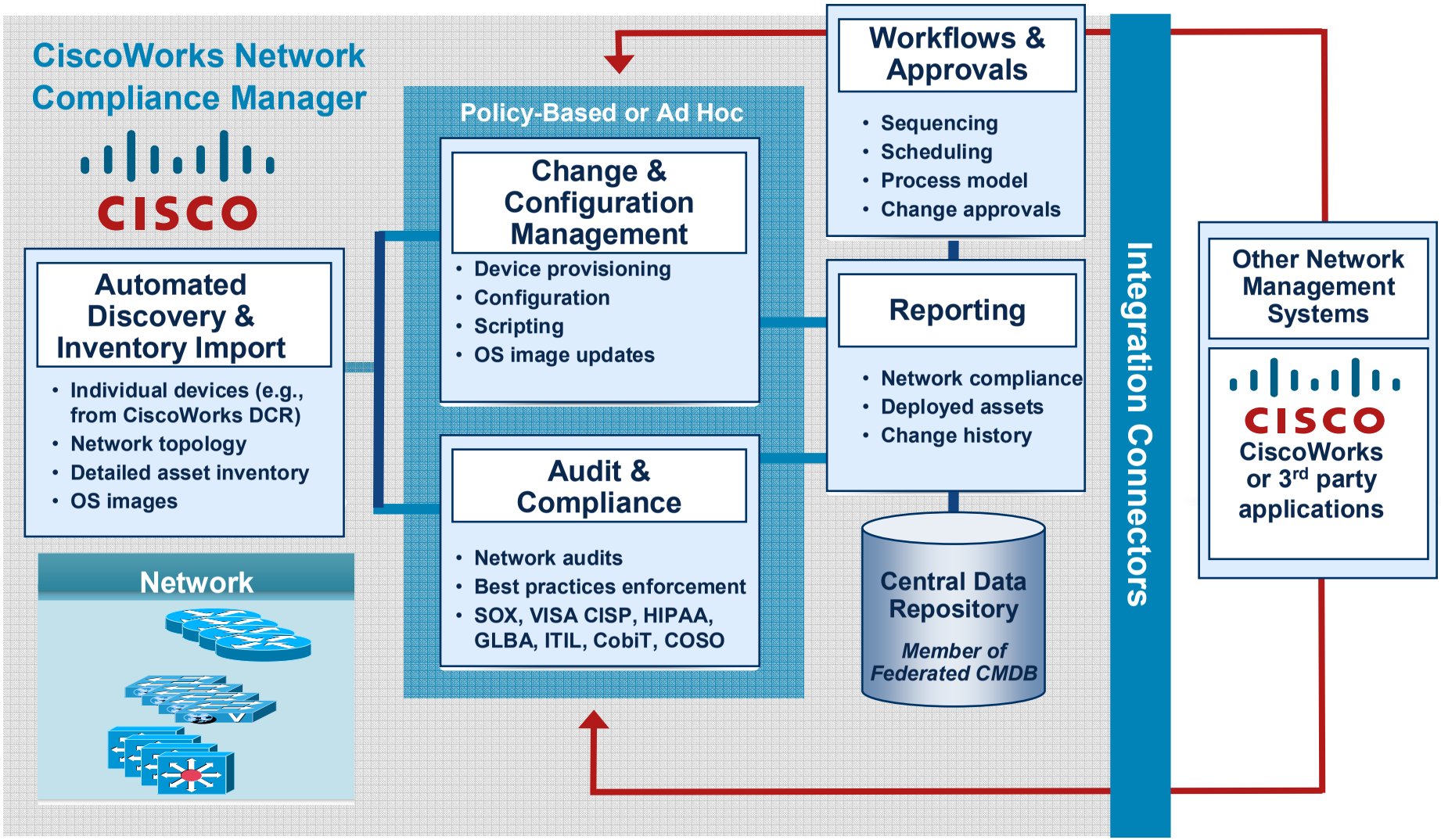
CiscoWorks NCM Objectives



How do we achieve the objectives?

- **T**rack
- **C**ontrol
- **A**utomate
- **P**revent

NCM Functional Overview



CiscoWorks NCM
Extensive, Multi-Vendor Device Support

Supports over 500 device models across Cisco and other vendors

Advanced Workflow and Approvals

Close the change loop with real-time process enforcement

- Model complex projects
  - Combine automated and manual activiti
- 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

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

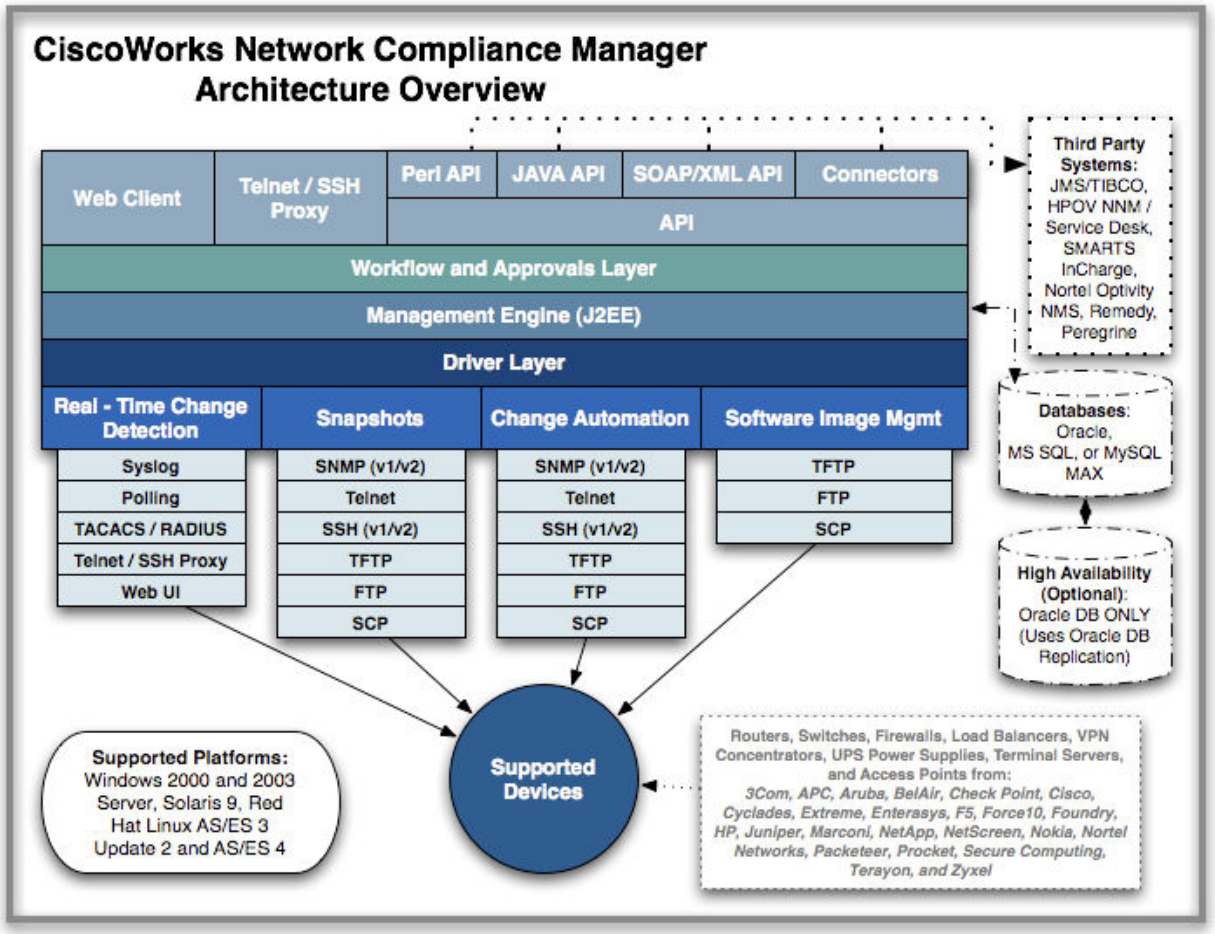
Shared Product Extensions – leverage scripts, packages and policies

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

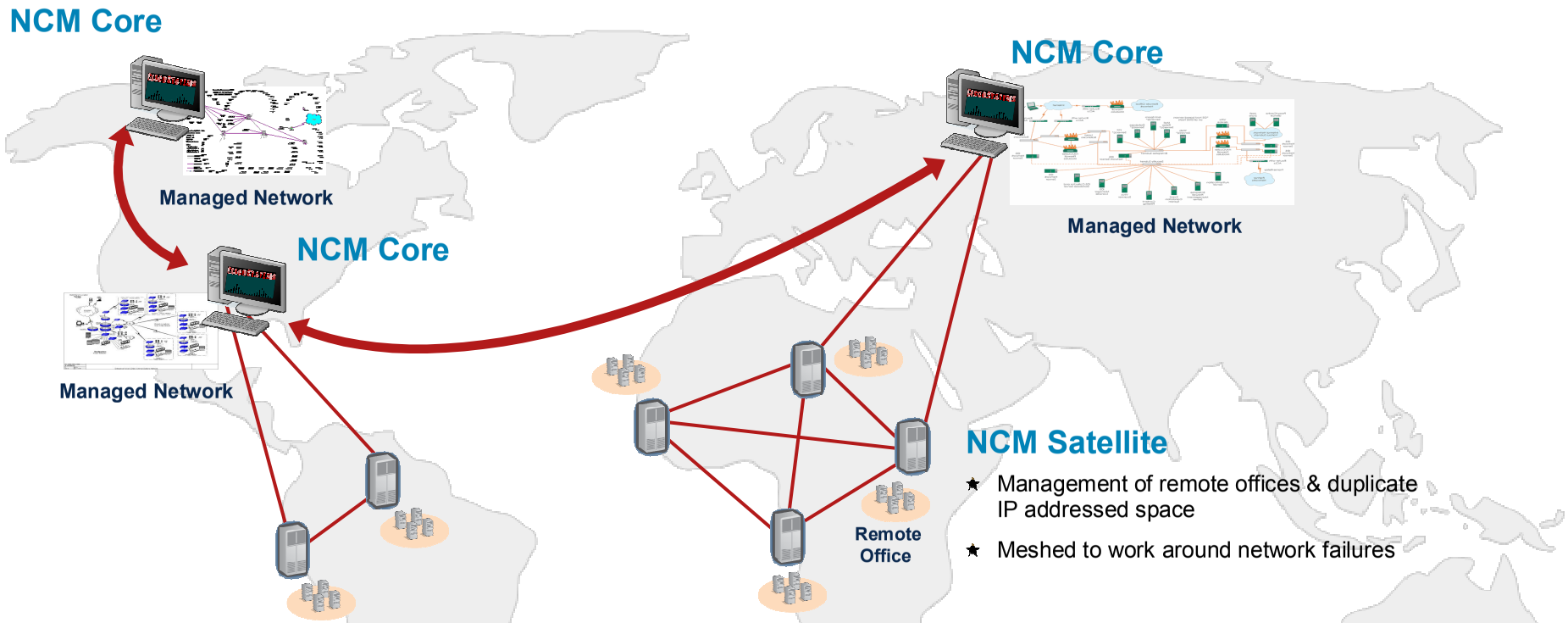
- High Availability Replication
- Satellite Off-loading
- Microsoft and Veritas (Solaris) Clustering

Extensibility

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

CiscoWorks NCM
High Availability Features

Active/Active Management via High Availability Database Replication



NCM Satellite

- Management of remote offices & duplicate IP addressed space
- Meshed to work around network failures

NCM HA

- Real-time synchronization between all NCM cores
- Enables remote management, disaster recovery and global visibility
- Replicated database, software, user directory & routes commands to correct locations

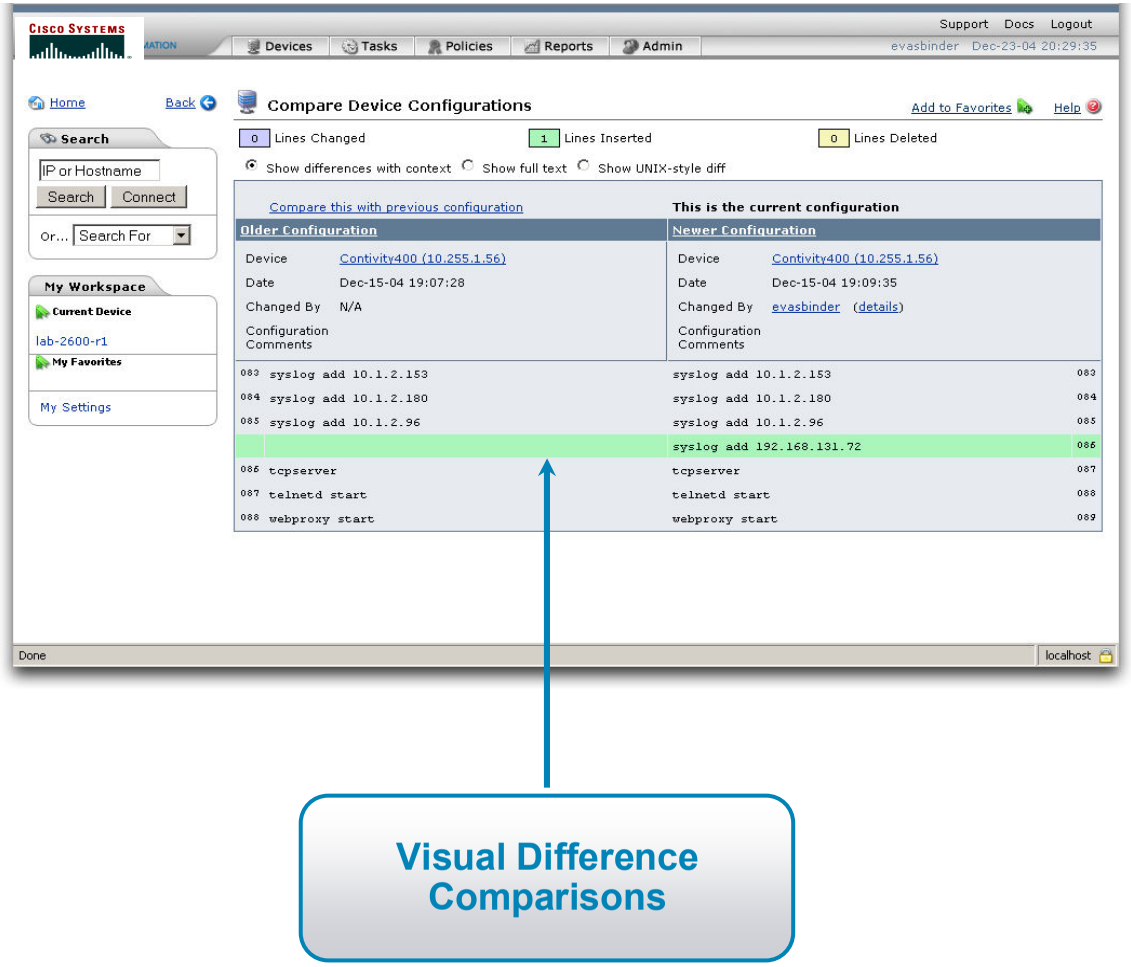
Key Elements	Key Attributes
★ Core ★ HA ★ Satellite	★ Secure, scalable ★ No single point of failure ★ Remotely manage any device—including duplicate addressed networks

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



Diagram, Visualization & Troubleshooting

Leverages network knowledge to create real-time topology diagrams

The Challenge

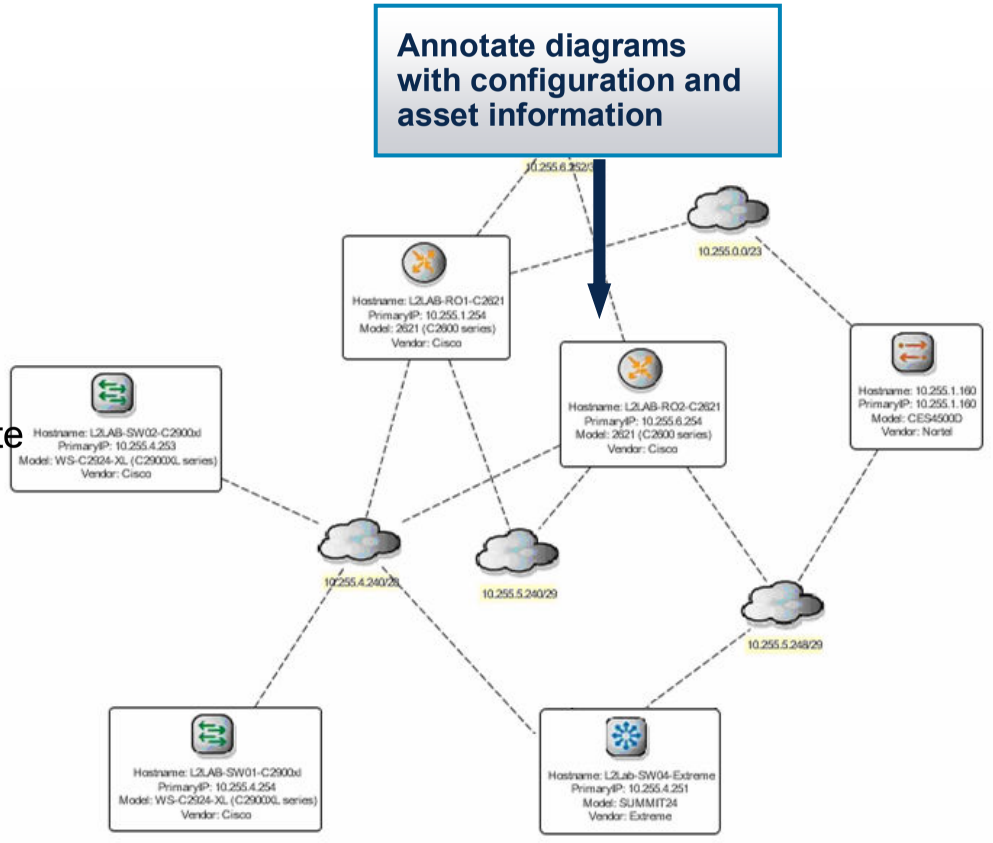
- Creating network diagrams is labor intensive process
- Diagrams often out of date with current state of the network causing increased downtime and less effective troubleshooting

NCM Solution

- Applies deep network understanding to generate real-time, accurate topology diagrams
- Provides integrated server & network diagrams for complete picture of the IT infrastructure

Benefits

- Eliminate 99% of the time spent building diagrams
- Facilitates troubleshooting
- Allows server/network dependencies to be mapped



Layer 2 Modeling

Provides layer 2 networking intelligence

The Challenge

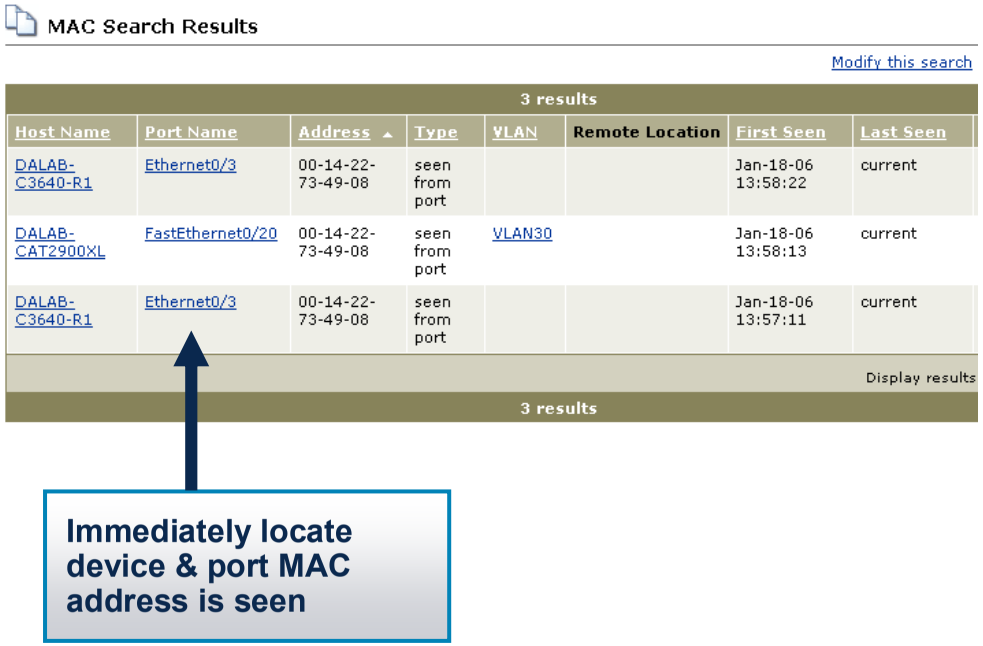
- No visibility into network <-> server dependencies
- Armed with the MAC address of a server, users are unable to complete the puzzle

  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



VLAN Management

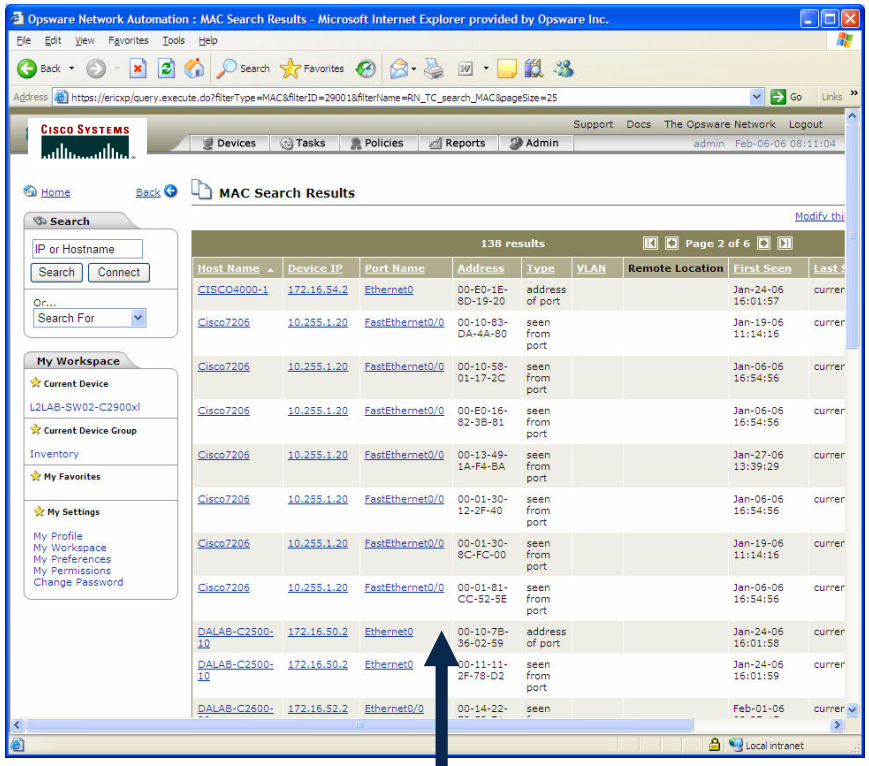
Provides VLAN networking intelligence

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



Prioritized Triage of Compliance Violations

Pushing the most critical violations to the forefront

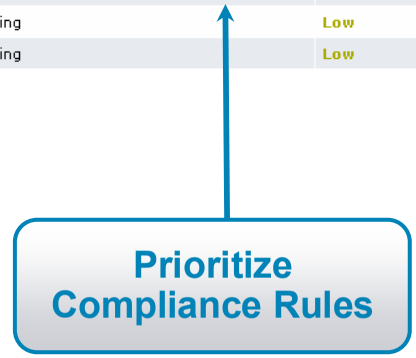
The Problem

- 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

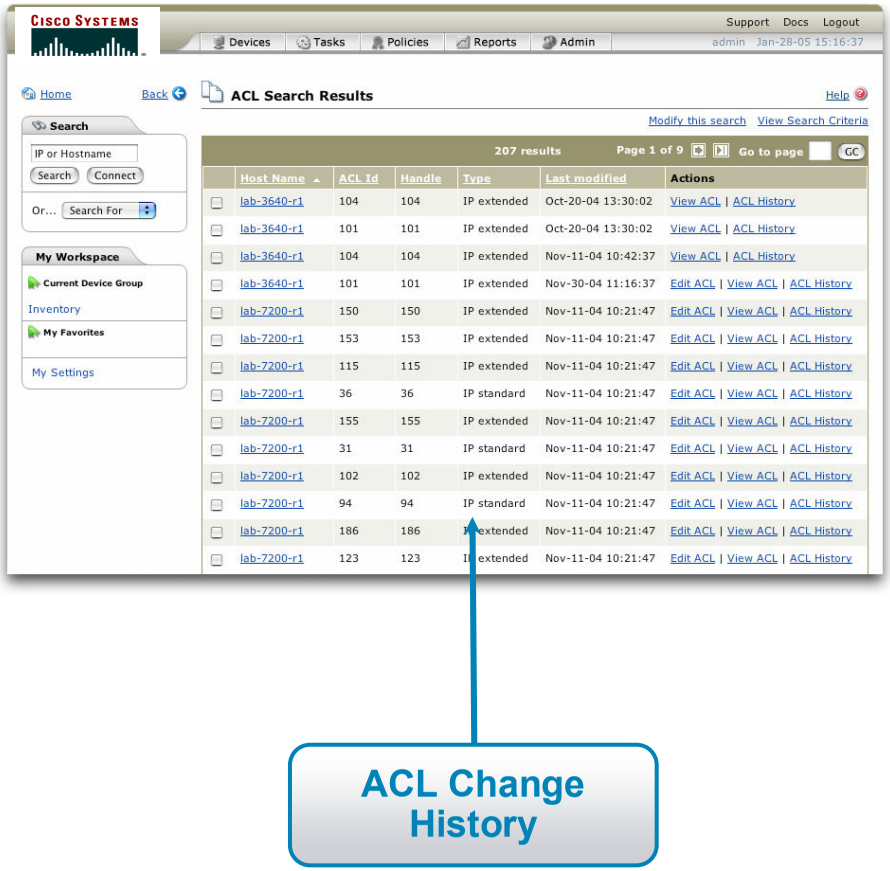
Rule Name ▲	Device Family	Description	Importance
Access Lockout - Cisco IOS	Cisco IOS	Access to console or vty line is locked after unsuccessful attempts	High
Console Timeout - Foundry	Foundry	Specify a 10 min timeout on Console connections	High
Debug & Log Messages - Cisco IOS	Cisco IOS	Sequence number 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



Security Management

Patching, lock-down & centralized ACL management

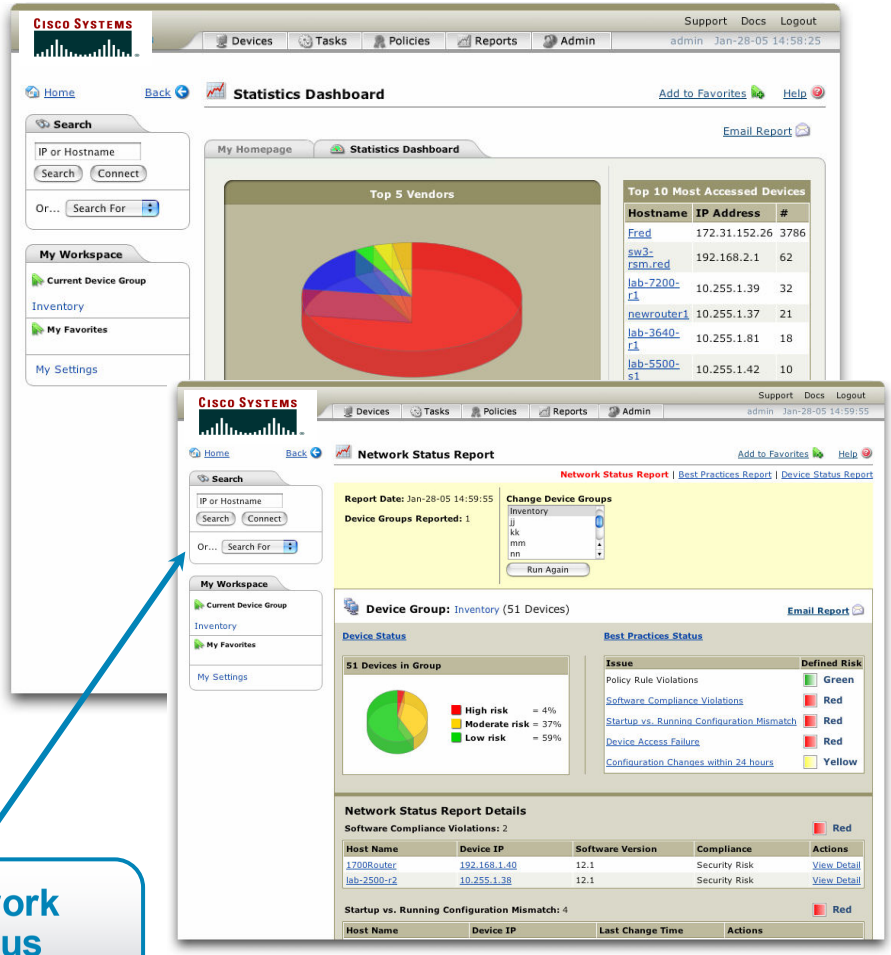
- Centralized patch management
- Telnet/SSH Proxy
  - Single sign-on
  - Full session logging
  - Centralized enforcement of privileges and approval policy
- Advanced ACL management
  - View & search current ACLs, historical ACLs and audit trails
  - Persistent ACL comments & handles
  - Batch ACL edits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



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



Take-Away

- Cisco provides a multi-vendor **N**etwork **C**onfiguration **C**hange **M**anagement 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 to automatically download policies