Pulse2011

How Managing Network Change Can Reduce Operational Expenditure and Speed Delivery

Mark Armstrong
Program Manager: Tivoli Network Management

Disclaimer

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion

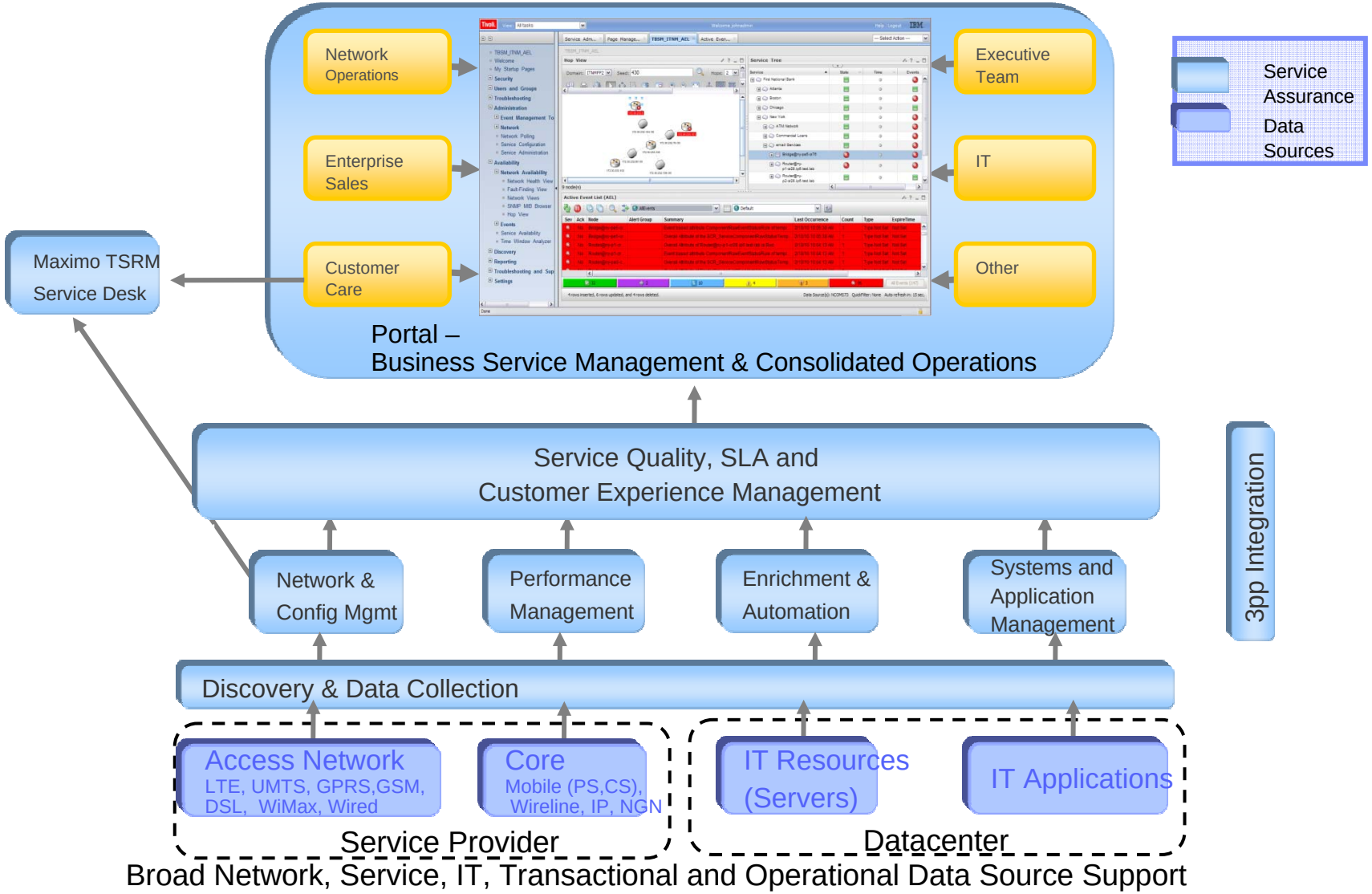
© 2011 IBM Corporation

Agenda

- The business impact of Network Complexity
- IBM Tivoli Netcool Configuration Manager - Product Overview
- Immediate integration value for OMNIbus and Network Manager Customers
- Customer Scenarios
- Roadmap

© 2011 IBM Corporation

Tivoli Service Assurance Portfolio



© 2011 IBM Corporation

Network Complexity is the root cause of most network issues today…

Explosive Growth in number of Devices...

- 200% device growth
- Proliferating network heterogeneity
- Global network
- Multi-vendor

…And the Devices are Increasingly Complex…

- 10's of different OS's
- Dictionary sized configurations
- 100K's of parameters
- Complex services

…While the Burden of Compliance grows.

- Growing compliance costs
- Failed audits (PCI-DSS, SOX, HIPAA)
- Inconsistent policy enforcement

Accelerating Change Frequency…

- Thousands of device changes / shortening maintenance windows
- Multiple OS & patches upgrades

… is Outpacing Personnel and Driving up Workloads

- Flat to moderate IT & network budget growth
- Avg. 1 tech per 250 branch routers
- ~21K CCIEs worldwide

…While Security can Never be Compromised.

- Decentralized network access
- Limited management visibility
- Ad-hoc security

© 2011 IBM Corporation

Sources: Cisco, EMA, Gartner, Juniper Networks, Network World

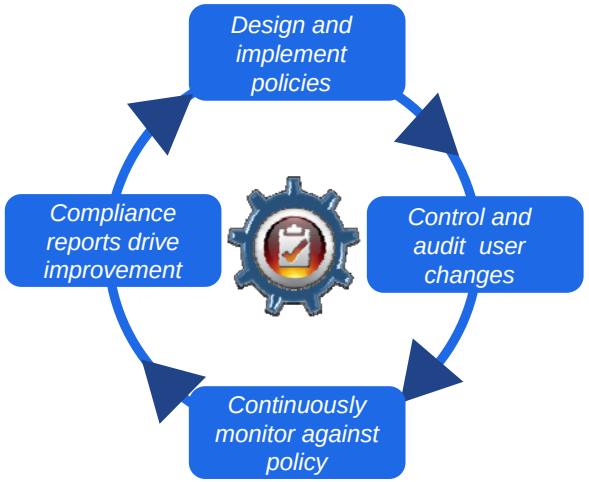
The Impact of Network Complexity

Errors largest cause of network outages	**60%**	caused by manual configuration errors
Network complexity outpacing scripting	**60**	average configuration errors per 1000 lines
Routine tasks consuming resources	**45%**	of engineering time spent on manual config
Incorrect provisioning and excess inventory	**35%**	of network assets lost or deployed erroneously
Inconsistent security posture open to threat	**80%**	of security breaches from non-compliant devices

© 2011 IBM Corporation

Reliable network configuration

- The impact of human error on the network reliability can only be addressed by **gaining control** of every aspect of configuration:
  - Put in place **operational policies** and **user processes** to guide the users as they configure the network.
    - Source these from industry best practices, regulators and standards bodies, vendor recommendations and local technical experts
  - **Control**: which **users** can make changes, which **devices** they can configure, what **changes** they can make to the devices
  - **Audit** every network device touch, whether automated or manual
  - Gather data on **compliance to policies** as a feedback mechanism to drive improvement



Tivoli Netcool Configuration Manager controls all aspects of network configuration, with a comprehensive set of functions covering manual and automated device change, full user security and audit history, and continuous monitoring against operational policies.

© 2011 IBM Corporation

IBM Tivoli Netcool Configuration Manager

Answers to Your Network Complexity Challenges

Reliable and Verifiable Change Automation

- Track every change on every device even the ones that didn't go through "official channels"
- Push out 1,000's of complex network changes and verify each change, every time.
- Build intelligent command sets with built in error checking an control
- Provide repeatable templates and processes that can be used with confidence

Network Security and Access Control

- Control who can access what device and what commands and parameters they can use.
- Maintain a complete log of all changes, including full two keystroke logs for terminals
- Build effective change authorization workflows to maintain effective control of the network

Comprehensive Network Back-up and Recovery

- Builds a comprehensive backup of all network devices through intelligent change monitoring
- Enables recovery through Roll-back to a previous state without impacting the service

Prevent Errors and Ensure Compliance

- Industry first with pre-emptive compliance, prevent problems before they occur
- Full policy engine to enforce standards, engineering mandates, and security

© 2011 IBM Corporation

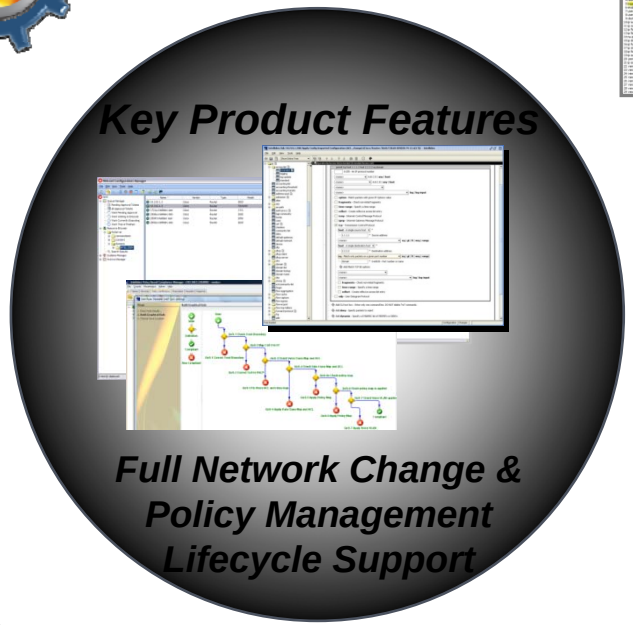
8

Agenda

- The business impact of Network Complexity
- IBM Tivoli Netcool Configuration Manager - Product Overview
- Immediate integration value for OMNIbus and Network Manager Customers
- Customer Scenarios
- Roadmap

© 2011 IBM Corporation

ITNCM: Intelligent Tool for Network Operations & Compliance



Backup Configuration
Single instance repository for all configuration and change information

Rollback or Restore Configuration
Restore configuration with or without a device reboot

SmartModel™ & Native Command Sets
Intelligently apply changes with full error control or with vendor native scripts

Bulk Configuration Changes
Automate bulk configuration changes through reusable command sets with full fallout management and error handling

Synchronize Changes
Update configuration repository with planned and un-planned configuration changes across the network

Pre-emptive and Current State Policy Compliance
Check the impact of changes BEFORE executing with Pre-emptive Compliance. Ensuring policy compliance of configuration for managed devices

Direct Device Access
Including command filtering and full keystroke logging for audit purposes

OS Upgrade Support
Automatically management the upgrade of a devices operating system

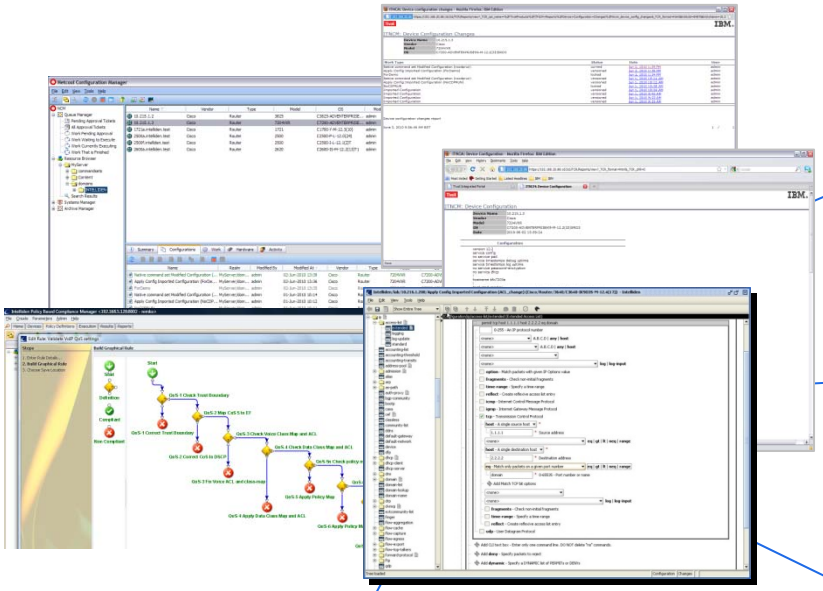
Open API's
Open API's enabling ITNCM to be integrated with existing customer systems e.g. network provisioning

Security
Role-based control of who accesses what devices and what changes they can make within the network, including full workflow approvals.

Device Discovery
Discover network devices in the network or utilize ITNM or flat file loads.

© 2011 IBM Corporation

Who benefits from TNCM in Your Organization?



CTO / CIO – the Architect and/or Standard Setter

- *Sets the network standards, and needs to enforce them*
- *Wants to deploy new services, but needs to understand what Devices and OSs are deployed*
- *Responsible for network audit capabilities and network compliance*
- *Wants Automation solutions which don't require fork-lifting current point solutions*

Chief Security Officer – the Enforcer

- *Responsible for setting and implementing network security standards*
- *Responsible for policing network access by insiders*
- *Requires automatic way to enforce network device level security*
- *Wants audit trail of changes to identify and plug breaches*

Local NOC / Operations Engineer – the Solder in the Trench

- *Needs to find and fix service effecting incidences quickly*
- *Wants ability to run comprehensive ad-hoc reports to indentify today's issue*
- *Just can't keep up with demands of all the C-Level guys – Make it easier for me to keep up!*

Chief Operations Officer – the Operator

- *Responsible for day to day operations, backup the network and recover when necessary*
- *Responsible for identifying and correcting network faults –NOC*
- *Responsible for enforcing the standards and security guidelines while keeping people productive*
- *Wants automation to reduce headcount and improve efficiency*
- *Wants dependable provisioning automation across multiple vendors*

© 2011 IBM Corporation

Control network changes: User security & audit

- Control and audit what different user groups can do to reduce accidental or deliberate misconfiguration
- NCM imposes fine granularity authorization using user groups by controlling:
  - The **NCM functions** they can access (*e.g. view or edit device configs, view reports, create templates, edit or apply policies*)
  - The **set of devices** they can view or configure (*network partitioning into realms*)
  - The parts of the **device configuration** they can see or edit.
  - The commands they can issue directly to devices through a terminal session (*command filtering*)
- NCM has a comprehensive audit log for every device:
  - **Every access** to a device through NCM is recorded, whether done via a template, manual edit in a terminal session, or via an API integration.
  - For manual sessions, retain a **full keystroke log**
  - Record **who made the change**, **what they changed**, and capture additional associated information such as a **reason** and a **ticket number**
  - NCM also **detects and records all changes** made through other routes (e.g. direct console port connection)

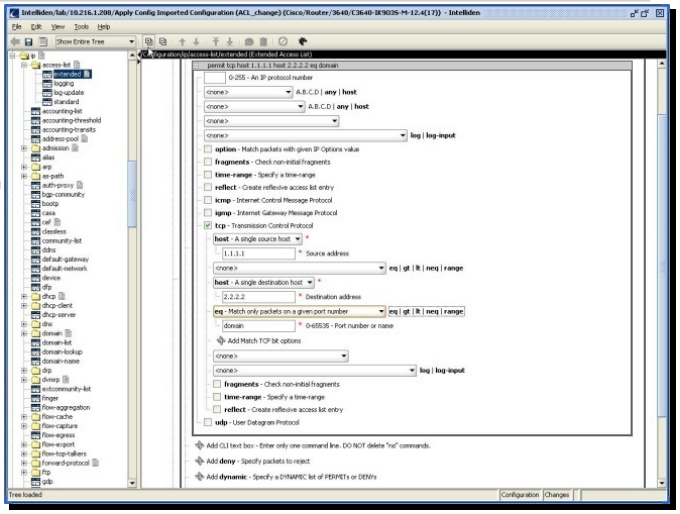
- Control and audit of every network device operation reduces the number of errors, and makes it easier and faster to find the source of problems when errors do occur

© 2011 IBM Corporation

SmartModels – Improving the reliability of Configuration Changes

- Errors are the largest cause of network outages
  - 60% caused by manual configuration errors
- IBM's patented SmartModels dramatically reduce the expertise required to understand, define, and make changes to any device.

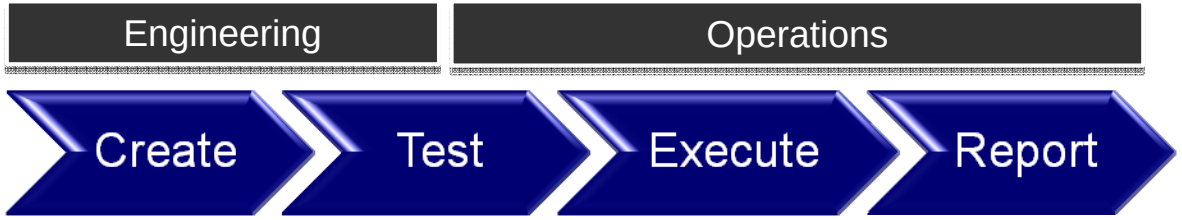
```
!
no ip http server
no ip http secure-server
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.216.1.254
!
!
!
ip access-list extended WORDExtended
 permit tcp host 1.1.1.1 host 2.2.2.2 eq domain
ip access-list extended enable
translate ruleset RULEs from pad to telnet
translate ruleset ee from telnet to pad
translate ruleset eee from pad to telnet
translate ruleset test1 from pad to telnet
translate ruleset weeek from pad to telnet
translate ruleset word from pad to telnet
 description word
 match cud word xot-source-addr word dest-addr word windowsize word dlci word ma
c word
 match cud word dest-addr word windowsize word mac word
 match packetsize word reversed word cud word dest-addr-ext word dlci word xot-s
ource-addr word
 match cud word
```



- ***Scripts are the number one cause of mis-configuration on network devices, because they cannot be tested against the device state that they will change.***
- ***Every network engineer loves scripts, until they pull the network down by accident…***

© 2011 IBM Corporation

SmartModel Command Sets



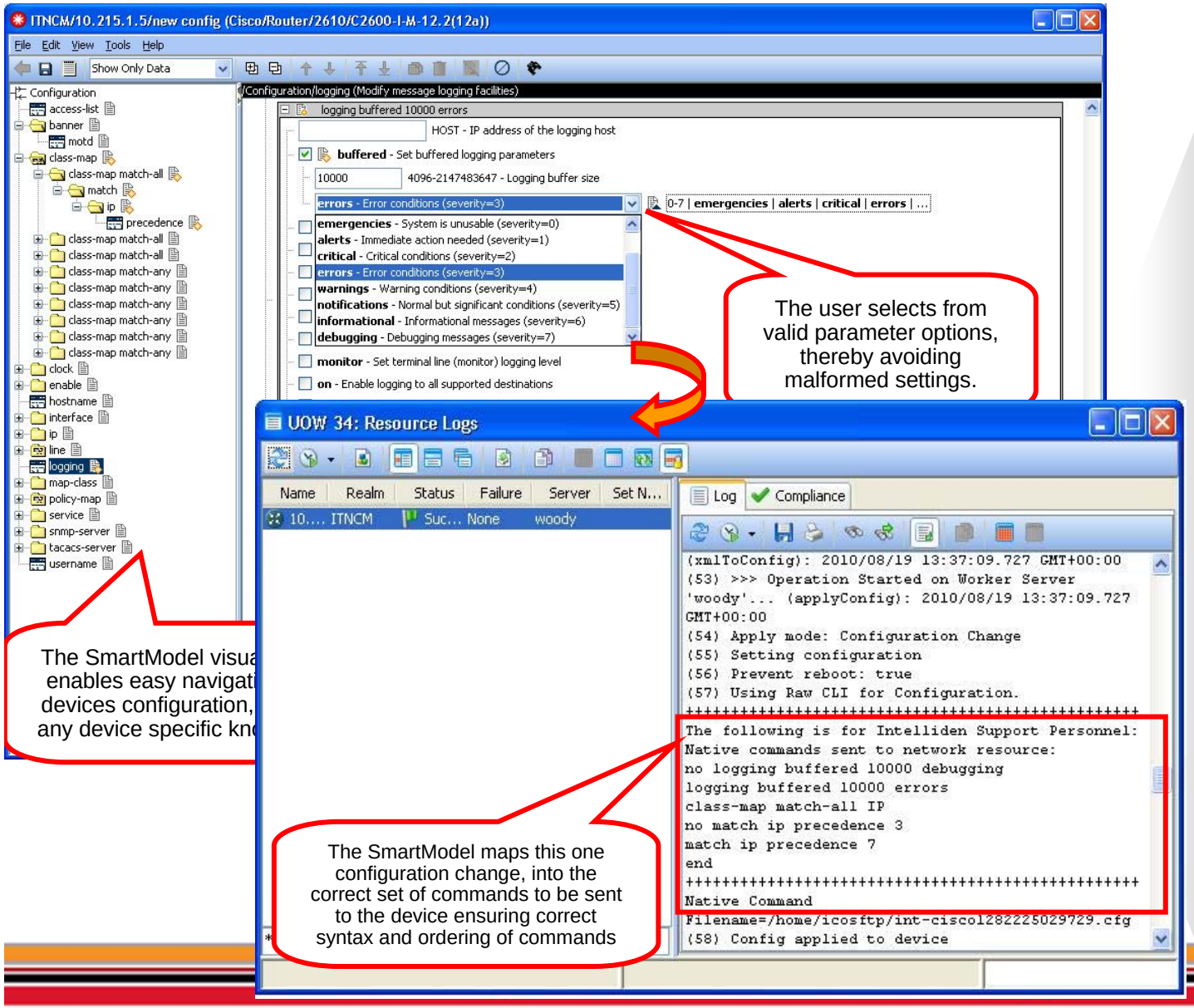
Requires no knowledge of native device language. Ensures that every change is syntactically & semantically correct, and based on the real-time configuration state

Key Features

- Reusable templates for single or bulk changes
- Contain all enacted commands, necessary parameters/relationships, logic for selected device
- Support for parameters and approvals
- Report only mode for testing changes before execution
- Commands automatically modify any “child attributes” e.g. settings associated with deleting an interface
- Can be invoked via Open APIs
- All changes logged
- Semantic-driven UI for configuration

© 2011 IBM Corporation

SmartModels - Reliable Configuration changes



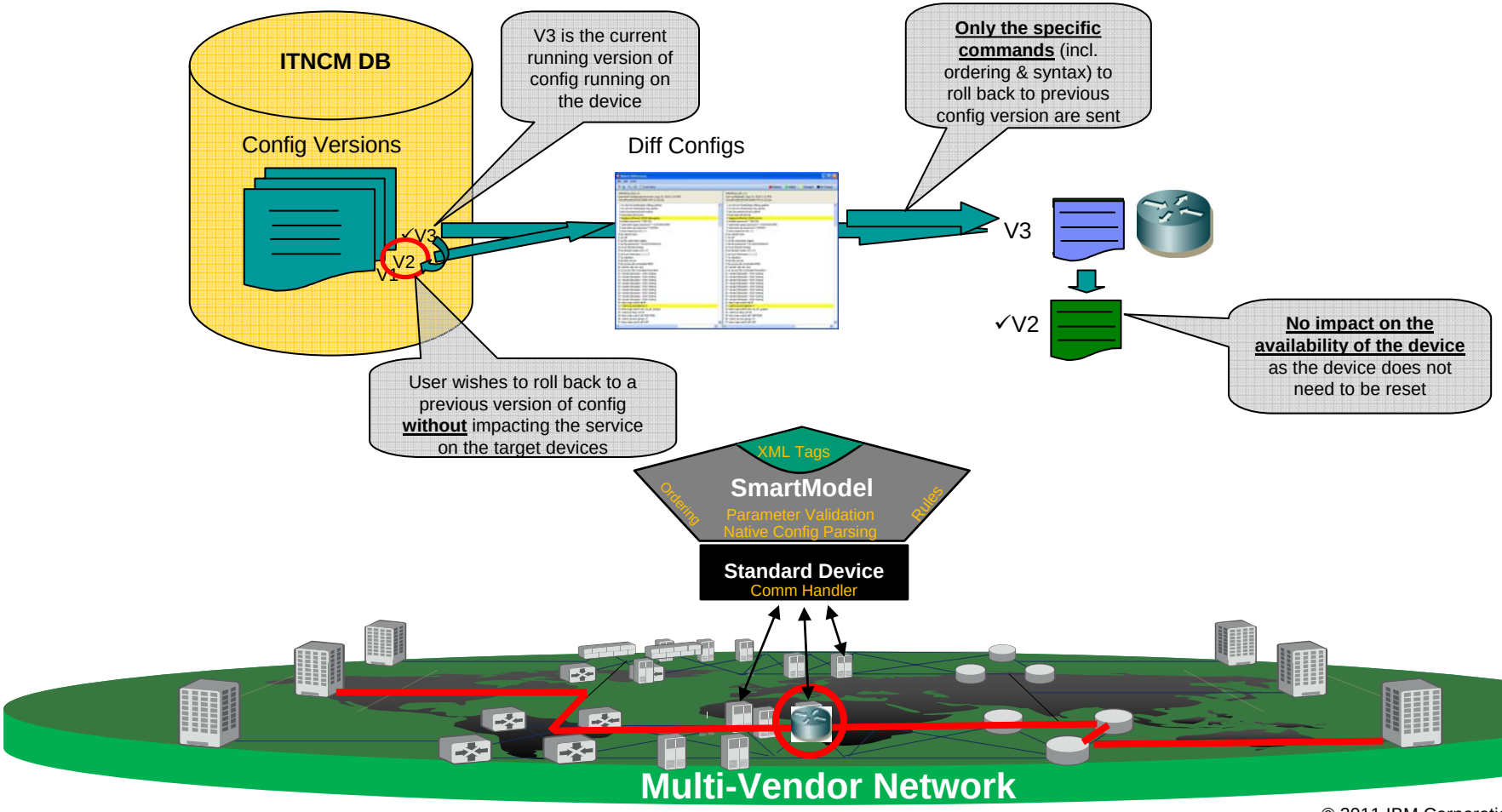
- **How does it work?**
- The user navigates the device configuration and visually selects the settings (with inbuilt sanity checking of selections) required for the configuration changes.
- The SmartModel will then, map these settings into the exact set of commands needed for the specific device.
- Other tools will require the user to have a detailed knowledge of the device specific commands – here the SmartModel takes care of that.

- **What are the benefits?**
- **Ease of use** in making device configuration changes.
- **Reduce the time** it takes in making device configuration changes
- **Ensure reliable changes** every time across the network.

© 2011 IBM Corporation

SmartModels - Intelligent Rollback

- ***The ability to send the exact set of required commands and parameters necessary to bring a device back to an exact known good configuration without having to reset or reboot the network device or impact customers service.***



© 2011 IBM Corporation

SmartModels – De-provision with confidence

- The majority of inventory and configuration "ghosting" occurs during the de-provisioning process.
- When turning down services, all the configuration parameters below the physical interface remain even after the interface is turned "off".
- Scripts can't properly turn down services, because they have no awareness of the scope of the device configuration or the actual state of the interface at time its being turned down.
- A user would have know the exact state of configuration below the physical interface and then methodically clear all the parameters in the correct order, and not make any mistakes in the process. One mistake and now a "ghost of configurations past" will be in the next configuration applied to the Interface.
- SmartModels enable automatic, one-step de-provisioning

- ***FACT: 80% of all inventory synchronization errors are created during the de-provisioning process***
- ***FACT: A Cisco 10K interface can have over 10K device parameters that must be cleared to properly return it to a null state. Do your engineers have a few hours to kill (parameters that is…)***

© 2011 IBM Corporation

SmartModels - Granular Security

- Security - of course it's the most important aspect of ensuring network integrity. But you can't simply stop people from getting access to a device, you need to control access AND what they can do on the device.
- SmartModels allow you to control exactly what commands, parameters, and even what parts of a configuration a user and see and make changes to, without writing a single line of regex.
- You can also establish workflows to allow user to make changes to otherwise restricted parts of device configurations. When they try to make a change to a restricted configuration, their manager is automatically notified via email and ask to approve the change.
- If the change is approved, then ITNCM tracks the change through to completion and notified the originator of completion.
- SmartModels allow you to control without preventing work from getting done quickly and efficiently.

- ***FACT: Security is required, but so is making sure your people can get their jobs done, it's often a process of trial and error to know what and where to limit users access.***
- ***FACT: ITNCM provides the ability to react in real time to identified internal threats.***

Maintaining network compliance in the face of change

- Despite the importance of regulatory compliance, **most organizations lack the ability to automatically and intelligently monitor and enforce the policies** that enable their networks to meet industry standards or even corporate best practices.
- **Enforcing compliance policies can be a challenge** in complex, dynamic, multivendor environments.
  - Once policies are established, their status **must be constantly monitored**, unauthorized and incorrect changes must be prevented, and alerts must be issued when compliance is not maintained.
- **Failure to ensure compliance** with properly managed policies can incur consequences that range from **fines** or other regulatory agency **penalties** to increased network downtime, vulnerability in network security, lost productivity and a higher cost in network operations.
- **Effective enforcement is necessary** when even a single configuration error can jeopardize the entire network's compliance status or open it to a security breach.

- Tivoli Netcool Configuration Manager is a comprehensive network solution designed to **define and manage policies, continually validate device configurations, alert users when policies have been or are about to be violated** as a result of a change or potential change, and intelligently remediate non-compliant conditions.

© 2011 IBM Corporation

Compliance & Audit

Support for regulatory, security and operational policies.

Intelligent remediation via a central policy repository & policy engine

Support for **SmartModel (i.e. no script) based policies**

Compliance dashboards with point-in-time and trending data.

The **pre-emptive compliance** capability enables customers to evaluate the impact of configuration changes against pre-defined compliance policies for a device.

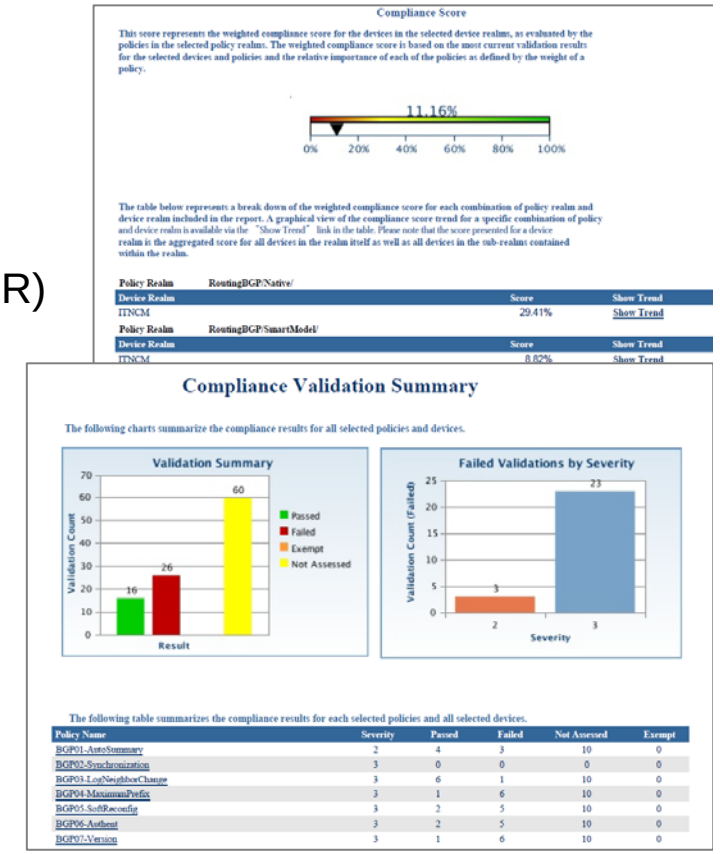
Key Features

- Manages the entire compliance lifecycle
- Allows specific devices to be exempt from policy checks
- Comprehensive audit reports
- Drag-and-drop interface
- Proven high volume validations
- Out-of-the-box policies (e.g. NSA router guidelines; operational policies)

© 2011 IBM Corporation

Network Policy Examples

- **Operational**
  - Engineering Standards
  - QoS (e.g. Traffic type queues on device interfaces, CIR)
  - Enable SNMP traps for MPLS
  - Specify NTP or TACACS servers for core devices etc.
- **Security**
  - Block RFC1918 addresses inbound
  - Apply inbound anti-spoof filters
  - Do not use default SNMP community strings
  - Disable source routing etc.
- **Regulatory**
  - Examples: SOX, HIPAA, PCI, EU Data Protection Directive
  - AAA (authentication, accounting & access) e.g. properly configured firewalls
  - Policies to protect regulated data e.g. IP Security
  - Security patch updates



© 2011 IBM Corporation

Compliance and Audit

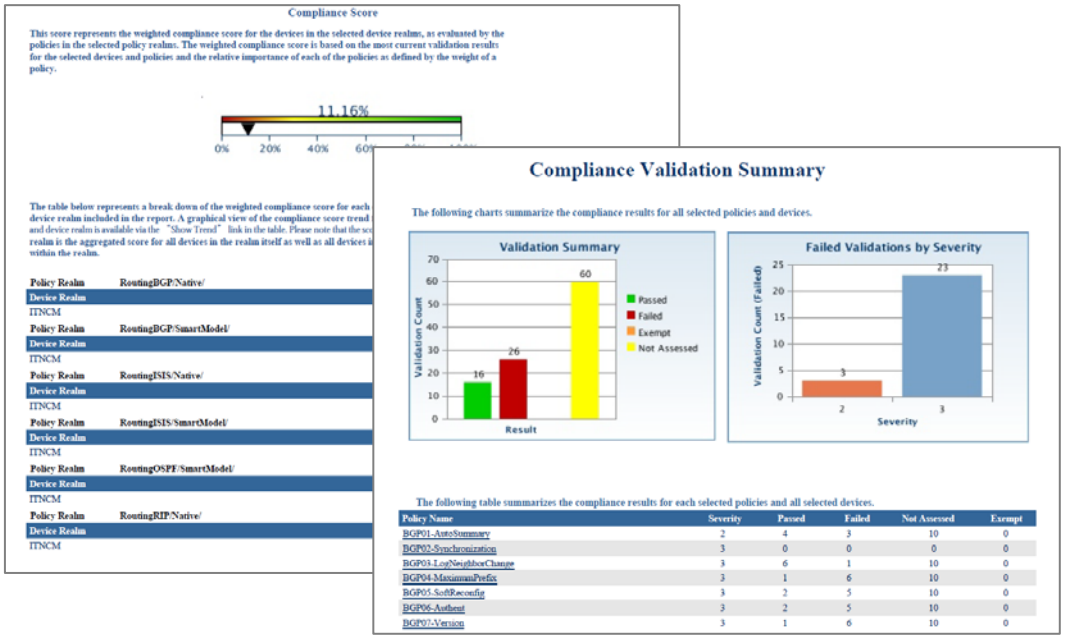
- **Closed-loop process**
  - Supports entire compliance lifecycle
- **Central policy repository, sophisticated policy engine**
  - Supports unlimited policy & device combinations
  - Provides continual policy validation
- **Intelligent remediation**
  - Resolves non-compliant conditions
- **Comprehensive reports**
  - Audit information for technical and business audiences
- **Easy to use**
  - Drag-and-drop interface
- **Built for scalability**
  - > 1,000,000 validations/hour
- **Out-of-the-box policies**
  - Growing library of sample Compliance Policies e.g. NSA router guidelines; Dynamic Routing Protocols (BGP, RIP, OSPF etc …) operational policies

- Continually validates device configurations against regulatory, security and operational policies, and intelligently resolves non-compliant conditions
- Allow specific devices to be exempt from policy checks (e.g. those under maintenance)

© 2011 IBM Corporation

Out of the box Compliance Reporting
- Auditing Network Compliance

Compliance & Audit



- Roll-based security determines access to reports, log info
- Users can define personalized reports with only those policies, devices and results that are relevant to them
- The Network Compliance Score can aggregates thousands of compliance validation results into a single number representing the state of the network. Trend data will show progression over time

Always-on automated logging of all info

- Roll-up of validation data into single network compliance score
- Quickly find validation results for individual devices
- Out-of-the-box reports: Dashboard, Summary, Policy, Device, Validation Detail
- Current and trend data
- Drill-down to data, from executive summary to detailed violations
- Support for email reports; save reports; save report definitions; schedule reports, etc.

© 2011 IBM Corporation

Agenda

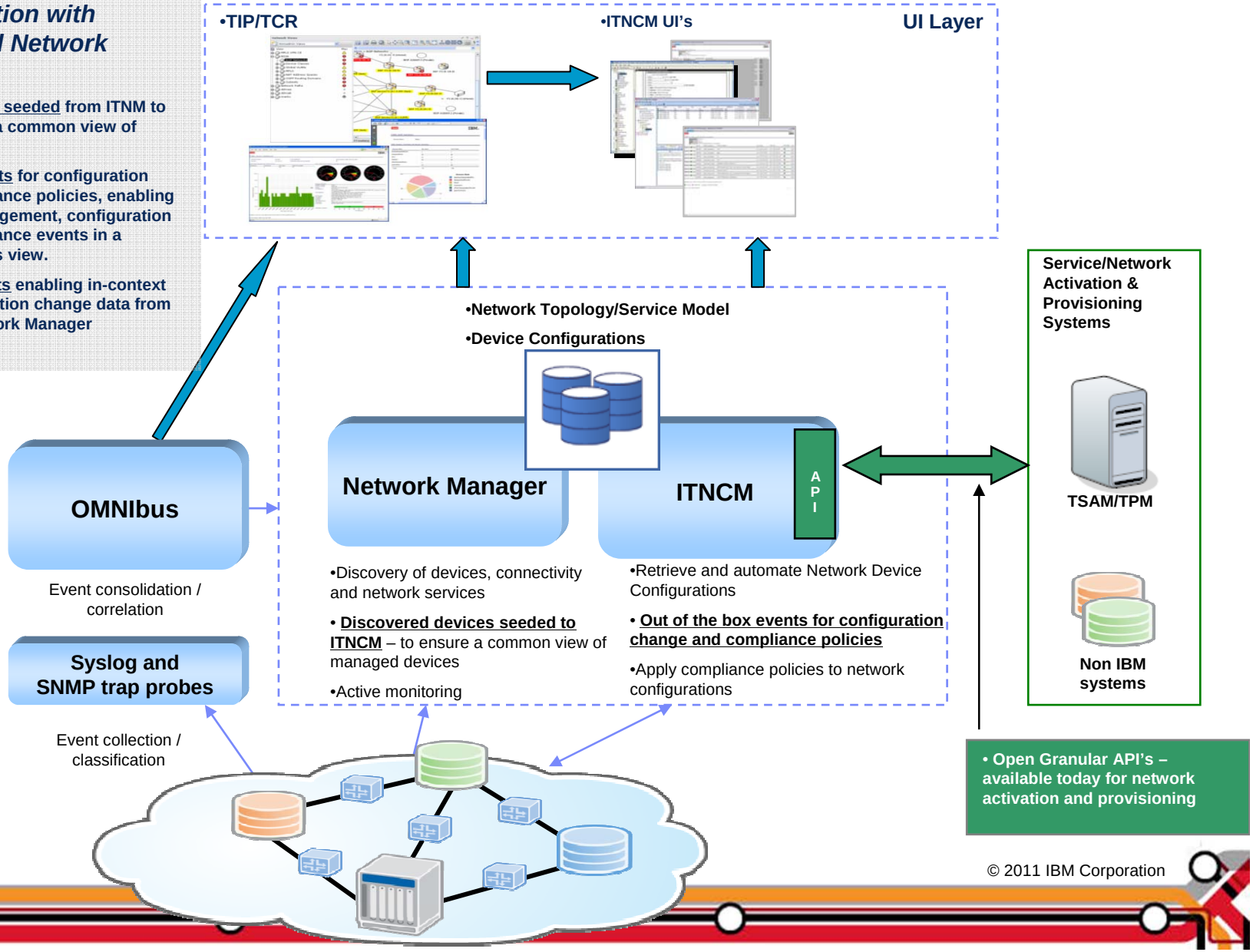
- The business impact of Network Complexity
- IBM Tivoli Netcool Configuration Manager - Product Overview
- Immediate integration value for OMNIbus and Network Manager Customers
- Customer Scenarios
- Roadmap

© 2011 IBM Corporation

Integrated Network Management Solution

- ***Tight integration with OMNIbus and Network Manager***

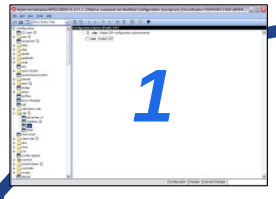
1. Discovered devices seeded from ITNM to ITNCM – to ensure a common view of managed devices.
2. Out of the box events for configuration change and compliance policies, enabling fault, network management, configuration change and compliance events in a consolidated events view.
3. Pre-built TCR reports enabling in-context access to configuration change data from OMNIbus and Network Manager



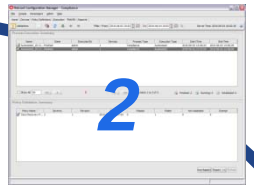
© 2011 IBM Corporation

IBM Netcool Product Suite Integration

Breaking the Cycle of Network Non-Compliance

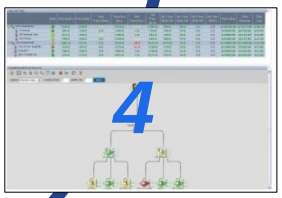


Changes are made to a device within TNCM or out-of-band

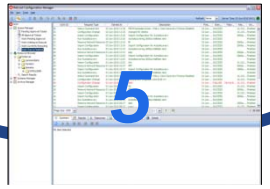


Device change causes a breach of a defined policy in TNCM which triggers a policy trap

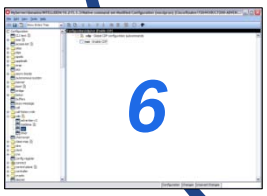
Omnibus collects SNMP events for all changes and policy breaches



TNM identifies the root cause of any faults and provide network hierarchy



If problem is new then user creates policy and defines remedial action (automatic or via manual approval queue) to be taken by TNCM to correct policy breach.



User or TNCM fixes root cause of policy breach

Auto Re-evaluation of change by TNCM clears policy breach

Netcool Product Suite

Omnibus + ITNM + ITNCM

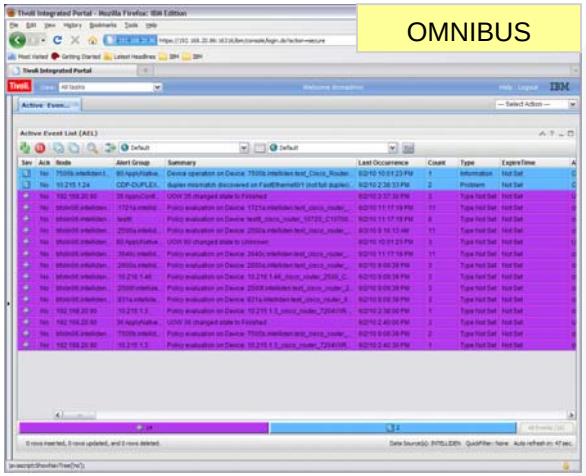
Through use of policies and change automation to address reoccurring network issues, operations staff can significantly reduce the number of total network events that require manual work to correct

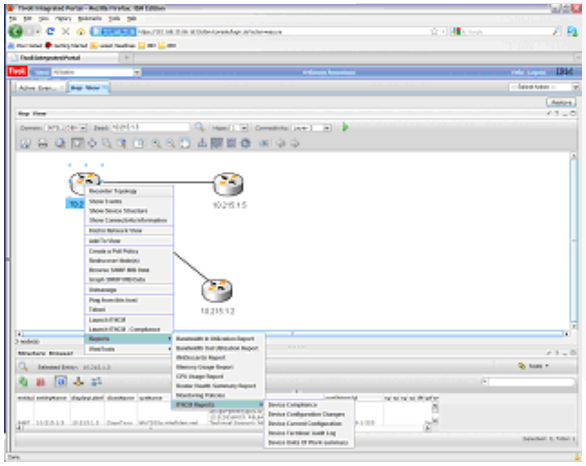
© 2011 IBM Corporation

Identify who made what changes when?

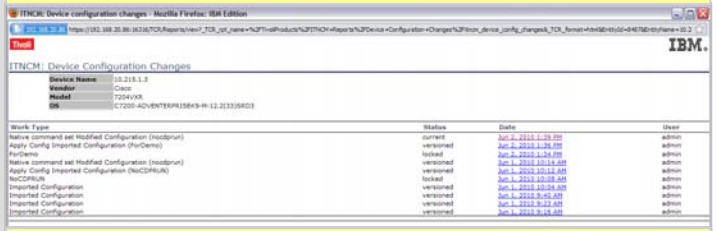
- Provides Netcool users with single-click access to ITNCM.
- Prebuilt TCR (Tivoli Common Reporting) reports which can be **launched in context** leveraging configuration data within OMNIbus and Network Manager.
- Helping to **diagnose problems quicker** resulting from configuration changes in the network.
- If permitted, Netcool users can perform configuration changes to resolve faults

OMNIBUS

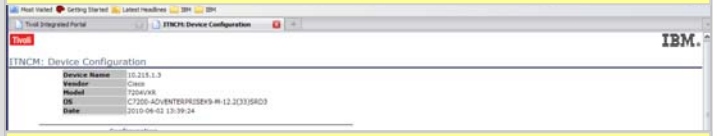




Last ‘n’ device changes, who made the changes & when?

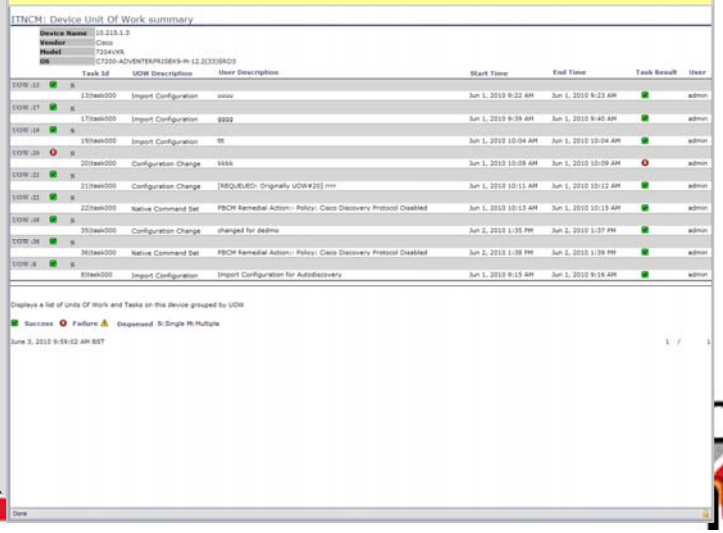


Configuration detail report



Device terminal audit log

Device Unit of Work (UOW) Summary



Agenda

- The business impact of Network Complexity
- IBM Tivoli Netcool Configuration Manager - Product Overview
- Immediate integration value for OMNIbus and Network Manager Customers
- Customer Scenarios
- Roadmap

© 2011 IBM Corporation

Very Large Managed Service Provider - Configuration & Compliance

BACKGROUND

Managed Services Provider to enterprises - One of the world's most advanced MPLS networks with 28,000 ports in 170 countries

CHALLENGES

- Provide an IP network with scale, resilience and security
- Accurately bid for new outsourcing contracts
- Meet stringent network availability & performance SLAs
- Ensure customer's network compliance obligations
- Reduce headcount to maintain multiple customer networks
- Reduce OPEX

Solution

- System of record for all network changes
- Service assurance
- Accuracy - "Getting things done right the first time"
- Business practices - "Single and consistent way of operating globally"
- Meet customer's network security & compliance obligations
- Ensures all devices within the networks meet's customers OS specifications
- Eliminates security threats posed by older OS releases

Deployment

- Devices: ~130K deployed; target ~500K devices
- Users: ~130 network engineers and support personnel
- Supported customers: >300 managed services enterprises (e.g. Leading financial institutions)

Results

- OPEX reduction
- Prevention of multiple SLA violations resulting in penalty reductions in the 100Ks GBP
- Prevention of customer down time
- Compliance remediation resulted in 10Ks of network changes to meet policy mandates

300 Enterprises & 55K devices operational in 6 months

© 2011 IBM Corporation

US based Telco - Zero Touch Network Provisioning

BACKGROUND

Leading US-based Managed Services Provider with ~42K SMB Customers

CHALLENGES

- Support aggressive growth plans – 3 new markets and 12K new customers per year
- Eliminate need for manual provisioning
- All-IP Cisco network
- Unlimited, carrier-class scalability not possible with existing internal solution
- 'No-touch' new service turn-up needed

TNCM Solution

- Network Provisioning, Configuration and Policy Management
- Unified solution for network engineering, operations and services teams

Deployment

- Devices: ~50K
  - Cisco IAD2400 Series (CPE) and 10,000 Series (aggregation) devices
- Users: ~160 Systems Engineers
- Supported Customers: 13 markets representing ~42K SMBs

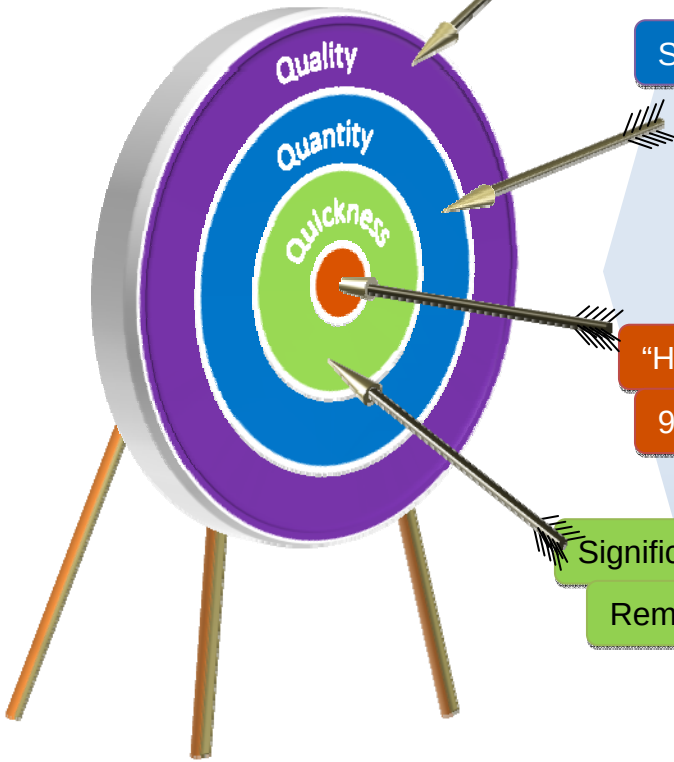
Expected Results

- Minimize need to send installation technicians for CPE provisioning
- Shield CLI complexities from services / OSS teams
- Reduce 'fat-finger' configuration errors
- Control access i.e. who can do what and when
- Test provisioning changes before they are implemented
- Greater standardization
- Meet Customer SLAs

First-time 'right' provisioning and minimized truck-roll

© 2011 IBM Corporation

US Based Telco: Zero Touch Install Benefits



- Accurate device configurations
- Policy and compliance management
- Integration with Siebel CRM
- Service activation org working on exceptions only
- Integrated with provisioning workflow
- Increase number of installs per technician per day
- "Hands off" of the network
- 90% Zero touch installs
- Significantly reduce technician on site
- Remote push of device configs for post install changes

© 2011 IBM Corporation

Agenda

- The business impact of Network Complexity
- IBM Tivoli Netcool Configuration Manager - Product Overview
- Immediate integration value for OMNIbus and Network Manager Customers
- Customer Scenarios
- Roadmap

© 2011 IBM Corporation

Tivoli Netcool Configuration Manager Roadmap

NCM 6.1

- Seed ITNCM with Network Manager discovery
- OMNIbus and Network Manager event integration:
- - Send policy violation events;
- - Send network configuration change events;
- - report on the status of network configuration tasks
- Launch from OMNIbus and Network Manager to out of the box network configuration and change history reports (TCR)

NCM 6.2

- SNMP Based Configuration
- Preemptive Compliance
- Command Filtering in Device Terminal

Next

- **Launch key NCM UI components** in Tivoli Integrated Portal (e.g. apply command set, revert config, policy check)
- - Supporting **launch-in-context of NCM UI's** from OMNIbus and Network Manager
- **Activity Viewer** – allowing visualization of NCM activities in a timeline viewer portlet
- Common user/role definitions supporting **single sign-on**
- Out of the box compliance reports using **Tivoli Common Reporting (TCR)**
- **AIX & SUSE** Platform support
- Support additional databases including **DB2**
- Federal Market enabler: **FIPS 140-2**
- **Virtualization** ../1
- - Network proxy/gateway support
- - Improved visualization of virtual devices
- - Drivers for networking components within a virtualized solution (e.g. Configuration of Vswitches)
- **Service Activation**
- – Service Management Interface (Config) Enhanced API's for Network Configuration Management to support activation driven by external systems.
- Enhanced policy definition by enabling programmatic constructs

Next +1

- Service Management Interface (Compliance)
- Service Compliance
- - Cross Device Policies
- - External references in compliance policies (via command line call)
- Enhanced UI workflows
- - Consolidated Monitoring Portlet
- Globalization
- Consumability /TTV/ Infrastructure
- Multiple database support - Informix
- Continued Portfolio alignment
- Continued investment in virtualization
- SDK for device support (Improved Standard device & SmartModel tooling)

Device Roadmap

Normalize current device/technology support across both product and release in-step

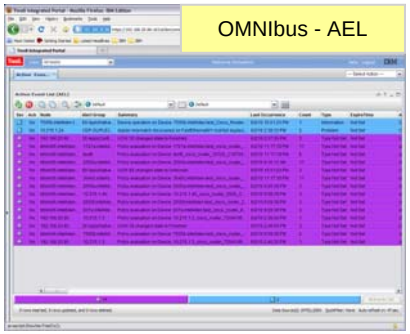
© 2011 IBM Corporation

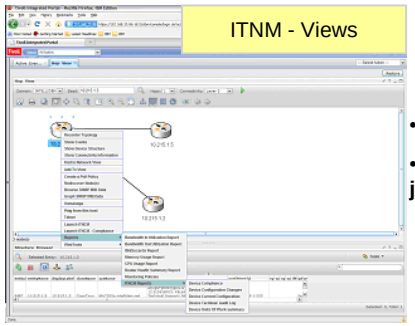
UI Plans for ITNCM

The focus is to enable targeted operational workflows seamlessly across OMNIbus, Network Manager and Netcool Configuration Manager through adoption of TIP and TCR for reporting.

TIP

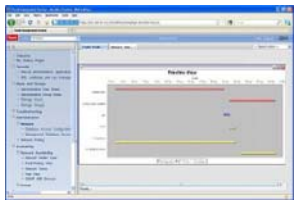
- Building on the UI flows introduced in ITNCM R6.1, the launch points within TIP will be the OMNIbus AEL and the ITNM Views





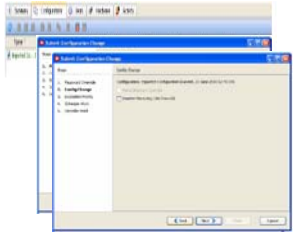
- **What NCM capabilities will be accessible within TIP?**
- Run Commandset
- Perform a policy check
- Synchronise (D->I)
- Revert (submit) configuration
- Activity Viewing

•Activity Viewer



•Apply Command set

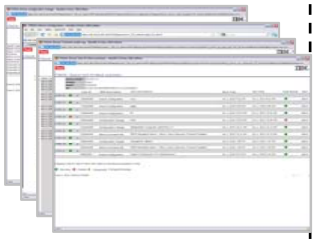
•Revert (submit) config



•Perform a Policy Check

•Synchronise (D->I)

•TCR Reports – Out of the box reports on NCM data

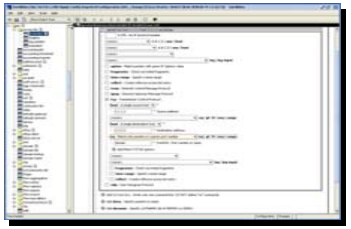


•Single sign on

•Launch in-context of NCM java clients

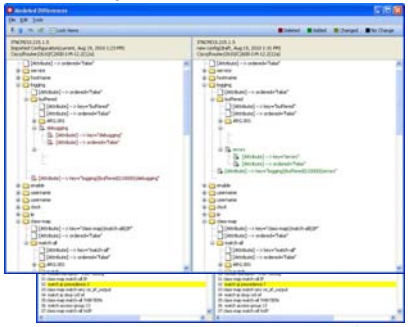
NCM UI's

•Config Viewing & Editing



•Integrated Device Terminal (IDT)

•Config Comparison (Modelled and Native)

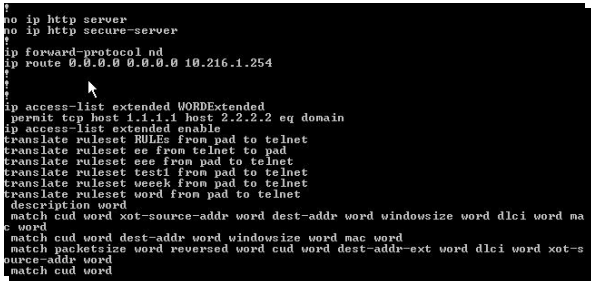


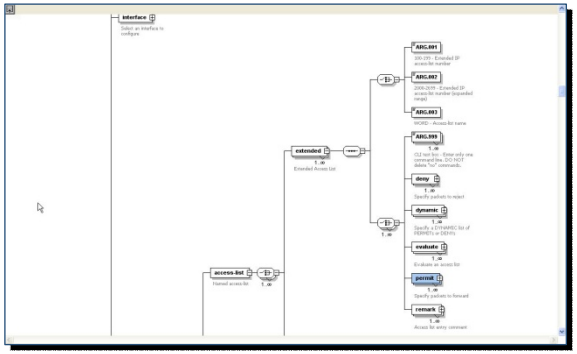
© 2011 IBM Corporation

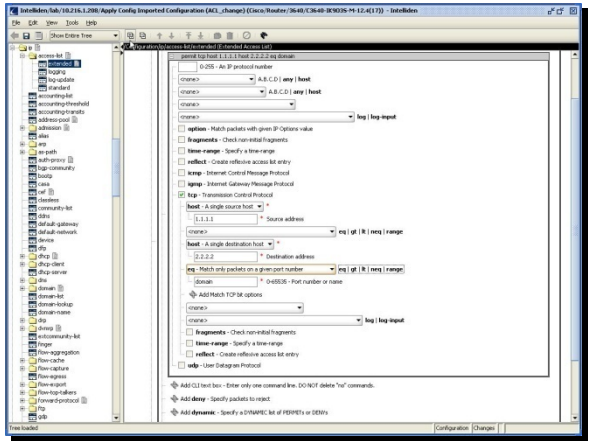
Backup

© 2011 IBM Corporation

ITNCM – The Power of SmartModels™







CLI

Native Text Config

- *Command Language Interface*
- *Text based with no structure or context*
- *Proprietary by vendor*
- *Varies by type, model, operating system (VTMOS)*
- *Stored in TNCM Repository as text for Native Command access*

CLI > XML Schema

CLI transformed to XML

- *CLI is parsed and then tagged for device specific and general content*
- *XML schema contains all configuration commands, relevant parameters, allowed parameter ranges, inter-relationships, logic*
- *Constructs for device configuration settings*
- *XML schema and rules are maintained as the SmartModel*

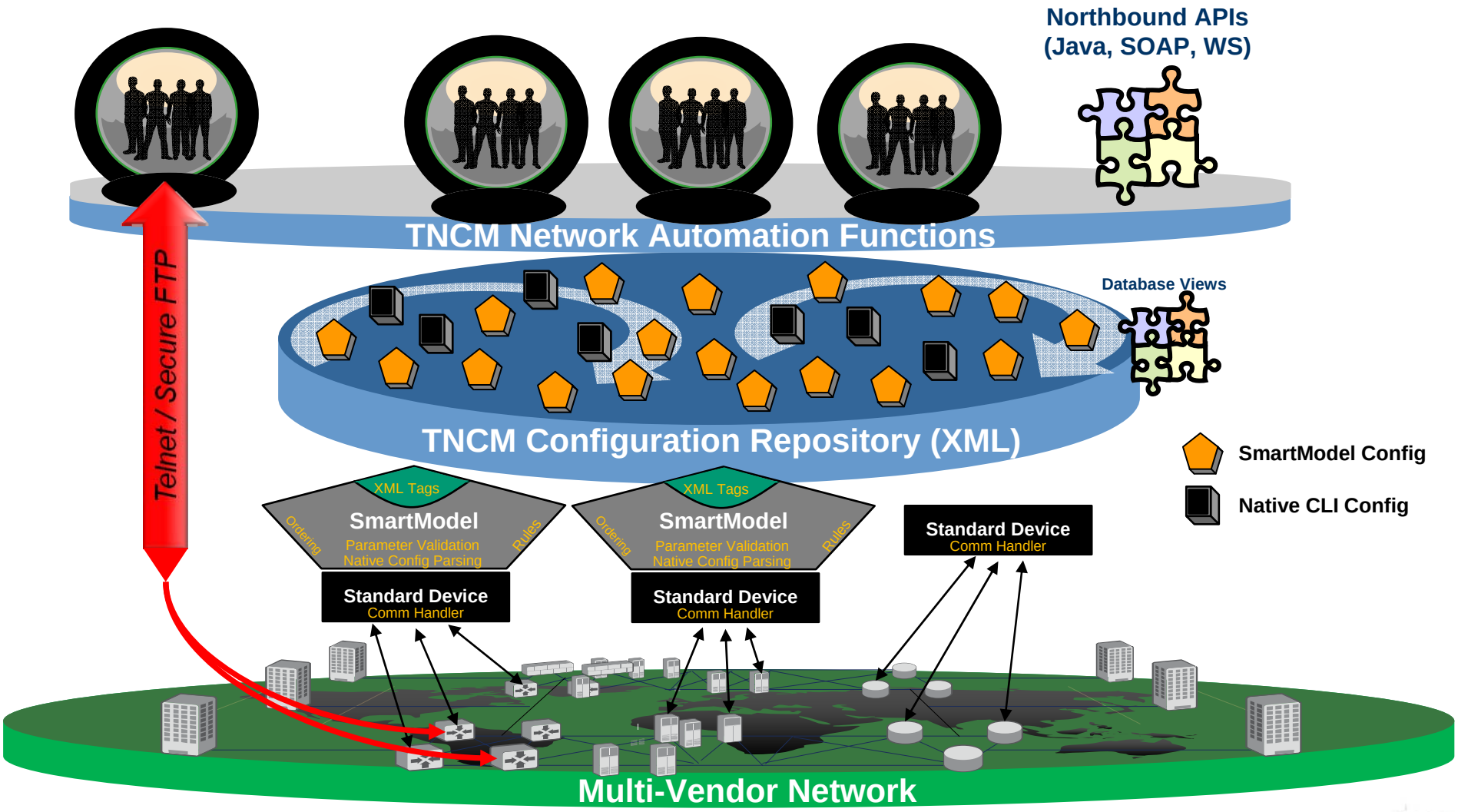
SmartModel™

SmartModel enables complex device functions

- *XML tags automatically generate UI*
- *Standardizes command syntax, automates command ordering*
- *Enables Roll Back instead of a device reboot.*
- *“Illegal” and incorrect commands not permitted to hit device.*
- *Automated add, modify, delete error flags for command reliability*

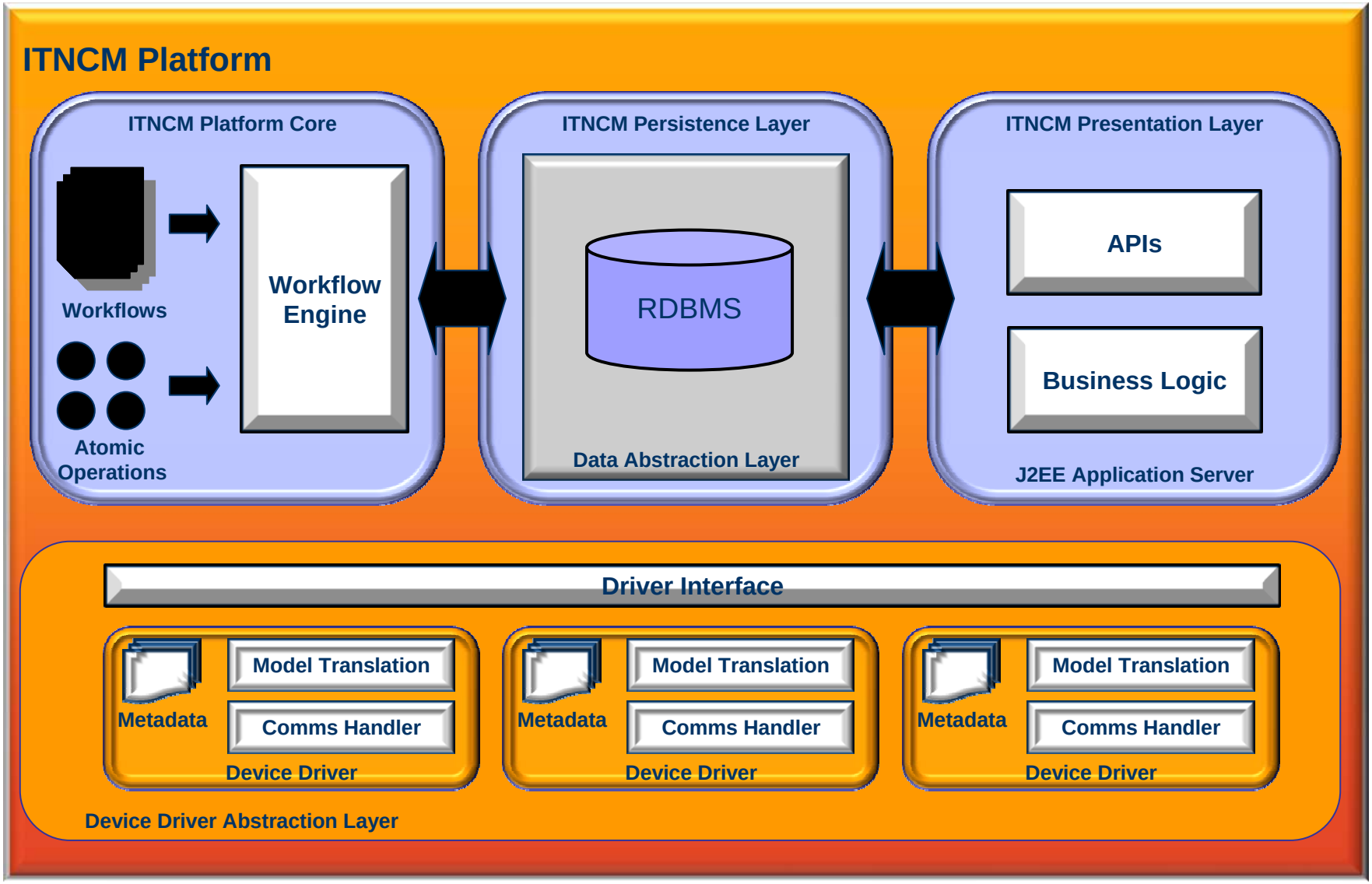
© 2011 IBM Corporation

TNCM – Functional Architecture



© 2011 IBM Corporation

ITNCM Architecture



© 2011 IBM Corporation

Highly Scalable, 3 Tier Architecture

Linear scalability through additional servers

Presentation Layer (*n* = 4)

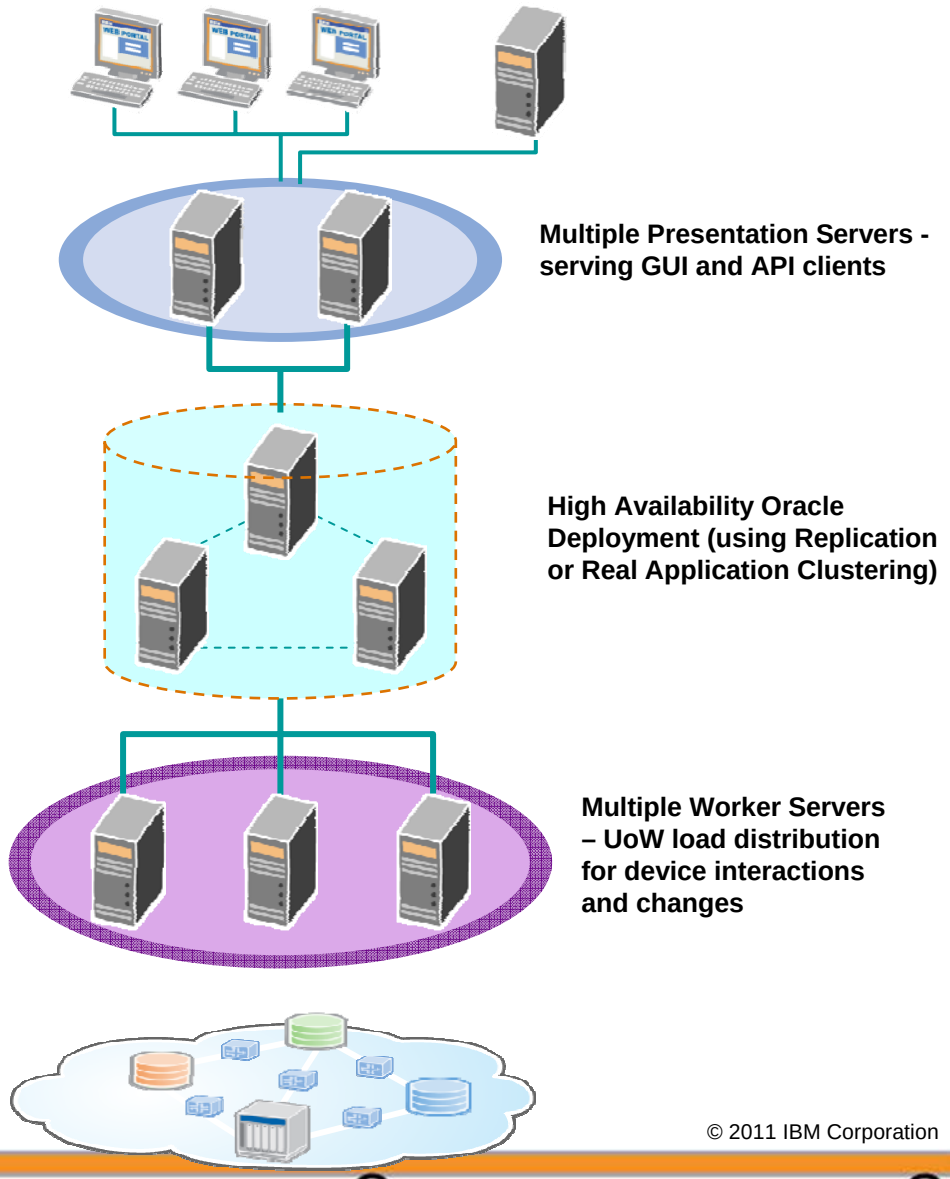
- ***n*** : 100s Users / API sessions
- ***n*** : 10K Change Requests
- ***n*** : 100s Activity Reports

Database Layer (*n* = 1)

- ***n***: 100s Concurrent Transactions
- ***n***: 1000s Transactions per Hour
- ***n:*** 1M Policy Checks
- ***n:*** 10K Device Configurations
- ***n:*** 10K Reads / Writes
- ***n:*** 100s OS / Patch Upgrades

Device Layer (*n* = 4)

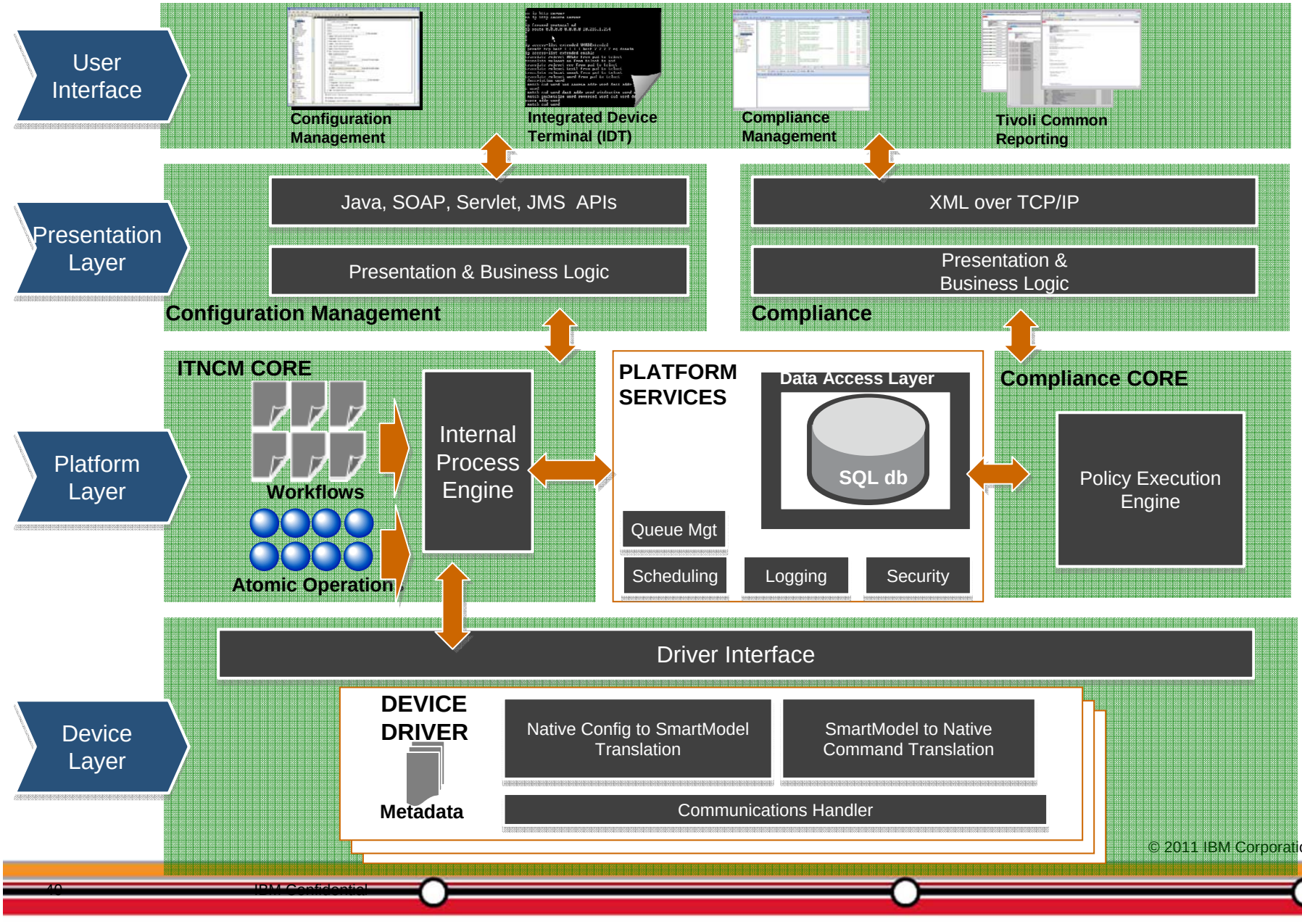
- ***n:*** 100K Number of Devices
- ***n:*** 1M Device Configuration Lines
- ***n:*** 10K Device Changes
- ***n:*** 10K Discovered Device



*n = number of dual-CPU dual-core Linux (2.33GHz, 4GB RAM) servers

© 2011 IBM Corporation

ITNCM's Architecture



© 2011 IBM Corporation

Trademarks and disclaimers

© Copyright IBM Australia Limited 2011 ABN 79 000 024 733 © Copyright IBM Corporation 2011 All Rights Reserved.
TRADEMARKS: IBM, the IBM logos, ibm.com, Smarter Planet and the planet icon are trademarks of IBM Corp registered in many jurisdictions worldwide. Other company, product and services marks may be trademarks or services marks of others. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list pricesand performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© 2011 IBM Corporation