

March 2006

**MANAGED SERVICE PROVIDER NETWORK
CONFIGURATION & CHANGE MANAGEMENT
REQUIREMENTS**



Table of Contents

1	MANAGED SERVICE PROVIDER CHALLENGES	3
2	NCCM APPLICABILITY WITHIN THE MSP DOMAIN	4
2.1	OVERVIEW	4
2.2	CONFIGURATION MANAGEMENT	5
2.3	CHANGE MANAGEMENT	6
2.4	NETWORK SECURITY MANAGEMENT	6
2.5	NETWORK ASSET MANAGEMENT	7
3	KEY TECHNICAL REQUIREMENTS	8
3.1	FLEXIBLE, COST-EFFECTIVE DEPLOYMENT OPTIONS	8
3.1.1	HIGHLY SCALABLE, DISTRIBUTED ARCHITECTURE.....	8
3.1.2	SECURE NETWORK AND CUSTOMER PARTITIONING.....	8
3.1.3	ANY-ANY CLIENT-SERVER CONNECTIVITY.....	9
3.2	SUPPORT FOR PRIVATE OVERLAPPING IP DOMAINS.....	9
3.3	COMPONENT REDUNDANCY AND RESILIENCY	10
3.4	REPORTING	10
3.5	MULTIVENDOR DEVICE SUPPORT AND EXTENSIBILITY	11
3.6	INTEGRATION WITHIN AN OSS ARCHITECTURE	11
3.6.1	APPLICATION PROGRAMMING INTERFACE (API).....	11
3.6.2	FAULT MANAGEMENT	12
3.6.3	INVENTORY	12
3.6.4	SERVICE PROVISIONING/ACTIVATION	13
3.6.5	SYSTEM ADMINISTRATION	14
4	REGULATORY COMPLIANCE AND INDUSTRY BEST PRACTICE	15
4.1	INTERNAL STANDARDS.....	15
4.2	INDUSTRY STANDARDS	15
4.3	CUSTOMER DEMANDS	16
4.4	DEMONSTRATING COMPLIANCY	16
4.5	ITIL.....	16
4.6	ENHANCED TELECOM OPERATIONS MAP (ETOM)	17
4.6.1	OVERVIEW	17
4.6.2	NCCM ALIGNMENT WITH ETOM	18
5	NCCM BENEFITS FOR THE MSP	20
5.1	REDUCTION IN OPEX	20
5.2	IMPROVED SERVICE AVAILABILITY AND MTTR.....	21
5.3	REVENUE GENERATION AND COMPETITIVE DIFFERENTIATION.....	21
5.4	STANDARDS AND LEGISLATIVE COMPLIANCE	21
5.5	CONFIGURATION COMPLIANCE VISIBILITY.....	22
6	CONCLUSION	23

1 MANAGED SERVICE PROVIDER CHALLENGES

As part of an overall drive to deliver greater operational efficiencies, reduce costs, implement best practices and ensure regulatory compliance, Managed Service Providers (MSPs) are leveraging new technologies to help improve and streamline their configuration and change management processes.

Emerging ISV companies working with selected value-add systems integration partners are bringing next-generation Network Configuration and Change Management (NCCM) solutions to market. The use of such solutions is helping MSPs ensure that configuration changes made to customer networks are done so in a safe, controlled and approved manner.

Historically, and until comparatively recently, configuration and change management within MSP networks has largely been confined to activities such as backing-up and restoring device configurations for business continuity purposes, bulk configuration changes (such as adding new Access control List or SNMP community strings), OS download/upgrades and rudimentary checking of configurations against pre-defined configuration templates. Many MSPs have often relied upon in-house developed tools and scripts to achieve these tasks. Such tools are often understood by a select number of IT support staff and require frequent updating/maintenance to remain of value. Other MSP organizations utilize Element Management Systems (EMS) provided by network equipment manufacturers - whose support is often limited to particular devices and technologies.

The continued reliance on manual processes and non-optimal tools means that device configuration activities often remain the largest single cost within network operations - the Yankee group has recently estimated this to be as high as 4 5 percent of operational costs in some organizations. In addition to reducing overall operating expenditures, other key challenges faced by MSPs include:

- Improving overall service availability
- Increasing revenues and operating margins
- Competitive differentiation
- Standards and Legislative Compliance

In today's highly complex, heterogeneous networks there is an ever pressing need to maintain the highest level of network availability, performance and security. Furthermore, MSPs are coming under increasing pressure to adhere to industry standards of best practice such as the IT Infrastructure Library (ITIL). ITIL's IT Service Management (ITSM) process guidelines help ensure configurations are deployed as designed, assure service and security of networks, and support regular risk/vulnerability assessments. Furthermore, enterprise customers are increasingly demanding that MSPs demonstrate compliance with the same external regulatory controls that they are subject to, such as Sarbanes Oxley (SOX), HIPPA and Basel II.

Moving forwards, to achieve overall business goals, MSPs will need to treat network device configuration management as a highly structured process framework and deploy next generation technology platforms that help to automate and enforce configuration management workflow. This paper examines the role of network configuration and change management in the MSP today and highlights potential benefits associated with deploying a next generation NCCM platform.

2 NCCM APPLICABILITY WITHIN THE MSP DOMAIN

2.1 OVERVIEW

Network configuration and change management within MSP organizations typically covers a number of different IT management disciplines: Configuration management, Change management, Release Management, Security management and potentially Asset Management are those most directly affected. Other management disciplines such as Fault management and Service Level management may also be impacted and in many cases enhanced by the adoption of a structured approach to configuration management.

Best practice guidelines such as ITIL's ITSM highlight the need to view change and configuration management as part of a broader process lifecycle, with each sub-process supporting the activities undertaken in adjacent sub-processes. Such a lifecycle may encompass a number of distinct phases such as the pre-deployment design and planning activities associated with rolling out new device configurations, authorizing and implementing the changes, updating inventory records, checking compliance and so on.

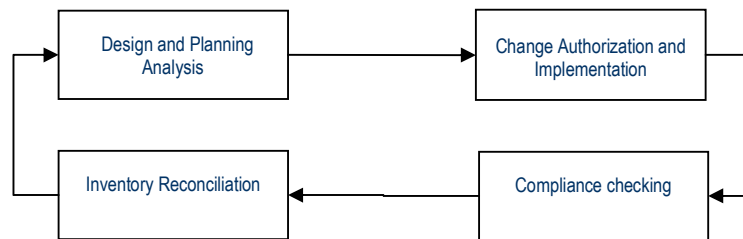


Figure 1 - Network Configuration and Change management – A typical process lifecycle

Of course, in order to implement and operate an ITIL-compliant change and configuration management process, one needs to consider how these processes will be underpinned and enforced by cooperating IT systems. Today, configuration change activities may originate within many different silo-centric processes involved in running customers' network, such as new equipment roll-out, manual and/or unauthorized changes, provisioning requests, security changes, version updates or even customer self-configuration.

The impact of network changes may often be compounded given that these multiple Services/Silos are being supported by the same underlying network infrastructure. Aside from addressing any specific functional requirements of the configuration and change management disciplines (see below), key capabilities that assist in combining together all the disparate elements that comprise the network and its associated operational support systems (OSS) include:

- The ability of the NCCM solution to centralize the management and normalization of configuration data across multivendor, multicustomer network infrastructures.
- The ability of the NCCM solution to automate the flow of information between constituent components of the process framework.

The following sections describe key functional elements within the various management disciplines that constitute configuration and change management:

2.2 CONFIGURATION MANAGEMENT

A key concept within ITIL is the Configuration Management Database (CMDB), a repository of information describing topology, service mappings and other relationships. The CMDB is the facilitator for cooperation between systems involved in the overall change management process such as service level, asset and capacity management. Network Configuration Management solutions typically include provision for population of the CMDB together with configuration back-up/restore and policy management activities. NCCM solutions should be capable of being integrated into leading CMDBs as a Federated portion of those CMDBs.

A NCCM platform may include the ability to automate certain aspects of the above activities in order to perform tasks in alignment with ITIL standards, such as automation of configuration or changes for large number of devices, backing up configurations as per predefined schedules, etc. Other features may include:

- OS/Firmware Release Management
 - Provide an ITIL-compliant Definitive Software Library (DSL)
 - Bulk OS upgrade for hundreds/thousands of devices
 - Managing increasing complexity; Different devices often have multiple operating system (OS) components running, e.g. Cisco 6509 switch chassis with MSFC routing module, each running different firmware
 - Ensuring sufficient memory is available before downloading the OS
- Controlled commissioning/decommissioning of elements of a network
 - Bringing to service new devices, enabling new interfaces, introducing protocols, etc
 - Support for template-based configuration (e.g., ACL's, SNMP, AAA config)
 - Administration: Supporting add/roll back, patches, configuration changes, and scripts
- Intelligent back-up/restore of configurations
 - Versioning of configurations
 - Save the configuration only if it's changed
 - Configurable multiple schedules
 - Intelligence to only send the specific config-let or the delta in the configuration change
 - Restoring the configuration to a known state/revision
- Configuration consistency checking
 - Template checking e.g., is an element configured in the approved manner?
 - Raising an alert when a discrepancy is identified, where a configuration change has been made that breaks configuration rules*
 - *More complex when the majority of high-touch configuration changes are made via a provisioning tool
 - Notification of failure to configure
 - Integrity checking based on sensible configuration rules (e.g., duplicate IP addresses/subnets, etc.)

- Act as a definitive source of configuration and asset data
 - Record configuration/asset information in a searchable form to a central database (CMDB) at some interval, including logical config, hardware, OS etc.
 - Support the publication of configuration data
 - Maintain the Network Inventory e.g., Model logical connectivity, Manage IP address ranges.
 - Data-fill other applications, e.g., network and service inventory

2.3 CHANGE MANAGEMENT

A MSP NCCM platform should enable both the definition and automation of the network device configuration change management processes. For example, the solution should support multilevel workflows to ensure that standard, non-standard, and urgent changes all follow the standard corporate change management process and are also ITIL compliant. The solution should also support tight integrations with any existing change management/workflow, helpdesk, and trouble-ticketing systems to ensure maximum return on investment and minimize disruption to existing working practices. Other change management facilities should include:

- Change management process
 - Planned/Unplanned change notifications
 - Authorization, approval and tracking of change requests
 - Support definition change and authorization levels
 - Change status reporting
- Change audit processes
 - Reports of change activities: Who did what, when
 - Facilitate visibility of network change activity.
 - Perform automatic audits of all proposed changes to device configurations ensure non-compliant change don't enter the operational network.
 - Re-occurring scheduled audits of the infrastructure to automatically detect non-compliant devices and automatically submit suggested remediations (for approval within existing change management/work flow process).
 - Support inventory and asset reporting of network devices, software and configurations
- Compliance
 - Track changes enabling validation of compliance with standards (e.g., ITIL, NGOSS, etc)
 - Track compliance to industry regulations (e.g., Sarbanes-Oxley, HIPAA, Basel II, etc).

2.4 NETWORK SECURITY MANAGEMENT

NCCM should support the management of network security:

- Management of Security Components
 - IDS management
 - Firewall management
 - PKI management
 - AAA management

-
- Logging
 - Support security logging, e.g., who made what changes and when
 - Authentication/Authorization
 - Support interworking with third-party network authentication and authorization mechanisms, e.g., TACACS+, Radius and LDAP
 - Software updates
 - CERT-driven OS and application security updates
 - Virus management
 - Identification of virus-related network events, impact management and associated rectification, e.g., rapid application of ACLs to contain virus/worm propagation.
 - Security audits
 - Assess security on network devices
 - Support routine hardening of all devices

2.5 NETWORK ASSET MANAGEMENT

NCCM platforms may also support an element of Network Asset Management via integration with inventory and financial tracking platforms:

- Inventory/asset repository
 - Database storing inventory-related information
 - Support for all network devices
 - Categorize assets according to various criteria
 - Support for asset audit
- Tracking
 - Track location, usage, costs, EOL date, etc.
 - Track into resource spend
 - Provide information to base spares planning and purchase
 - Provide reports/Support data querying

3 KEY TECHNICAL REQUIREMENTS

3.1 FLEXIBLE, COST-EFFECTIVE DEPLOYMENT OPTIONS

A MSP NCCM solution will clearly need to be capable of scaling to tens of thousands of devices, often comprising many disparate enterprise customer networks. To this end, the solution must:

- Be architected to allow its constituent management components to be distributed across multiple cooperating hardware platforms, possibly with device data collection activities separated from centralized management server activities.
- Be capable of accommodating features and functions of managed network environments such as private, overlapping IP domains
- Maintain close alignment with the SP operational/security model.

3.1.1 HIGHLY SCALABLE, DISTRIBUTED ARCHITECTURE

NCCM tools used within a MSP environment should ideally be based around a multi-tiered architecture that is capable of scaling to tens of thousands of devices, from a multitude of manufacturers, across hundreds of heterogeneous networks.

The components of such a multi-tiered architecture would typically include Web/Java-based clients, one or many centralized management servers acting as the principal ingress points into the application suite and one or many distributed device data collections agents.

The principal benefits of such a distributed architecture are:

- Scalability: By separating platform management and administrative functions from the underlying data collection activities, larger networks would typically be accommodated by simply deploying more data collection agents.
- The organization of the data within the management layer can be reorganized at will for presentation and access purposes with only limited changes being required to device ACLs (given the same data collection agents could remain in situ).
- Data collection agents could send data to many management servers allowing for operational flexibility or 'follow the sun' type deployments

All inter-component communication in the above architecture should also typically be capable of being transmitted via encrypted SSL sessions for security purposes.

3.1.2 SECURE NETWORK AND CUSTOMER PARTITIONING

MSP networks often comprise many different customer network environments and when viewed as a whole, may appear comparatively large and somewhat unwieldy from a management perspective. Therefore, MSP networks will typically require secure segmentation to be put in place between customers, geographical and/or organizational domains.

The capability to 'partition' the network into smaller sub-domains necessarily extends to the OSS tools - including the NCCM platform. While running separate instances of management platforms

(e.g., one per customer/region) may provide one way of addressing this requirement, a more cost-effective approach will typically involve the use of a smaller number of hardware platforms running applications that allow the managed network to be partitioned into logical/physical containers, e.g., one per container per customer, location, region etc.

Given that such containers will typically map to network, customer, geographical or organizational boundaries, the use of security access control will also be necessary to prevent certain users/operators from viewing or manipulating the entities within these containers. By taking advantage of access controls, it should be possible to dictate who is able to access devices and how networks are accessed. While access to networks may be provided by assigning users or groups to networks, other enhancements could allow security to be provided at not only the network level, but also the device level.

The use of such partitioning features should ideally allow the creation of hierarchical site constructs such as location/building and perhaps even floors within that building, or for the creation of user-defined views of specific devices or network vendors. Ideally, these groups should be capable of being automatically populated using criteria that map to device attributes, e.g., standardized naming conventions or via importation from third party systems and tools using the NCCM platform API. It should also be possible for devices to reside in more than one group e.g., a device can simultaneously belong to both the 'Cisco routers' and 'Asia-PAC Core network' groups/partitions.

3.1.3 ANY-ANY CLIENT-SERVER CONNECTIVITY

It should be possible for a NCCM console application to simultaneously connect to one or many servers, depending on the operator's specific role and access permissions. It may also be advantageous for the NCCM platform to be capable of abstracting/hiding some of the underlying complexity of the actual architecture from operators. This will be of particular relevance where users of the tool are responsible for managing devices belonging to a particular customer or in a specific service context, for example. In this scenario, the entirety of the network may actually be being managed by many distributed NCCM components. It should therefore be possible to employ additional management components in a seamless fashion as the network grows, without significantly impacting the way in which the console tool is used. The management architecture should also not prevent servers from connecting to a potentially large number of distributed consoles located in many geographical locations.

3.2 SUPPORT FOR PRIVATE OVERLAPPING IP DOMAINS

MSPs offering Managed IP Network Services need to manage the networks of customers that deploy identically-numbered private IP address spaces. This is a problem because network management applications and the IP protocol stacks on which they run operate under the assumption that IP addresses are unique. Common solutions that eliminate (or at least minimize) this problem are to either employ multiple NCCM platforms, the use of Address Translation Gateways, the use of a Management overlay network or the selection of a NCCM platform that is able to cope with private addresses without recourse to the other solutions.

(1) Multiple Hardware Platforms - The MSP deploys multiple hardware platforms each running a separate copy of the management application. Customer A's network is managed from one platform, customer B's network from another, and so on. Static routes are configured on each platform so that packets from the first go to customer A's network and packets from the second go to customer B's network. This approach may solve the immediate problem; however, the disadvantages are that each new customer requires a dedicated hardware platform making the

solution cost prohibitive and resulting in multiple isolated management applications. This makes it difficult for the MSP to consolidate its operations management.

2) NAT – Network devices could reside in environments accessed by the MSP using Network Address Translation (NAT) . In this scenario, the overlapping IPs would effectively be hidden from the NCCM solution data collection agent. The possible disadvantages to this approach are those of network/processing overhead and problems associated with effective diagnostic troubleshooting.

3) Management Overlay – The MSP may elect to utilize its own unique management IP addresses (Management Overlay network) while the customer retains its own IP addresses for internal use. In this scenario where multiple customer networks are being managed within a single MSP management architecture, a single data collection agent would communicate with each device using a unique address. There remains however the requirement for the NCCM solution to be able to logically distinguish overlapping IPs on multiple devices (and also to report on them) and the need for a separate network to be maintained.

4) Multi-tier architecture and Intelligent Data Collection Agents – Generally a MSP environment will use more than one data collection agent on grounds of scalability and security alone. Ideally the NCCM solution will support the use of multiple data collection agents (logical server), and allow each overlapping IP domain to be treated as unique as long as they are served by these different agents. In this scenario, the MSP is granted a high degree of flexibility with each customer being managed by its own logical data collection agent operating in the customer address space. Multiple agents can then feed a centralized data repository and higher-level management NCCM component located in the MSP address space.

3.3 COMPONENT REDUNDANCY AND RESILIENCY

The NCCM solution may offer its own built-in high-availability functionality with standby-by components monitoring primary components (using heartbeat detection mechanisms), ready to takeover the primary’s function in the event of component failure. Alternatively the NCCM solution may rely on underlying resiliency offered by hardware clustering solutions.

3.4 REPORTING

The NCCM platform should ideally provide sophisticated change reporting and include network asset/inventory and resource-level reporting capabilities. The NCCM platform may also offer real-time updated diagrammatic views of network infrastructure in order to assist with user orientation and familiarization, although this functionality is more likely to be available or be replicated within other components of the OSS framework, particularly fault management tools. Appropriate NCCM reporting capabilities are available in a variety of common formats such as PDF, HTML, XML, etc. would include:

Compliance Audit Reports	IP Address Reports
Credential/Device Change Reports	OS and User Reports
Device Connection Reports	Job Reports
Device Duplicate IP Address Reports	Inventory Reports

Reports should also be capable of being scheduled or created in an ad-hoc manner. They should be completely user-defined in terms of content, organization and the network(s) or devices(s) the reports are run against. Once a report is created, it should be capable of being saved and run on a recurring basis. Ideally, all core NCCM tool data should also be made available via the tool API, allowing MSPs to leverage their existing reporting capabilities by simply querying the data from the tools and importing into existing reporting systems.

Of particular importance for communicating the value of the NCCM solution will be an ability to produce Executive-level reports that summarize overall compliance status across all managed networks and all tracked policies, standards and government and other regulatory requirements. Such reports will typically comprise presentation-quality graphics and may be automatically e-mailed as PDF/HTML to designated recipients on a reoccurring basis.

3.5 MULTIVENDOR DEVICE SUPPORT AND EXTENSIBILITY

The NCCM solution should ideally offer standard support for a wide range of network devices, including Cisco, Juniper, Alcatel, Nortel, Extreme, Marconi, Checkpoint, Netscreen and others. It should also enable the management of network devices that use SNMP, Telnet, TFTP, SSH, SCP, XML, HTTP and other leading protocols to transmit configuration data.

In addition, the NCCM solution should offer an extensible device mediation architecture, which enables customer support staff or systems integrators to rapidly support or 'certify' new/additional devices.

In cases where a network device vendor-supplied Element Management System (EMS) is deployed as the principal management interface to network devices, the NCCM should possess the capability to integrate tightly with the Vendor EMS. Integration in such a scenario could combine the structured workflow and approval-control framework of the NCCM platform with use of the EMS as a proxy device configuration push/pull agent. The advantages to such a means of operation are:

- No changes would be required to device access control lists (ACLs), minimizing disruption and device reconfiguration.
- Network operators could continue to utilize the vendor EMS for ad-hoc configuration/diagnostic activities and would not necessarily have to learn how to use a new user interface.

3.6 INTEGRATION WITHIN AN OSS ARCHITECTURE

3.6.1 APPLICATION PROGRAMMING INTERFACE (API)

In order to maximise the benefit of an NCCM platform, many MSPs will wish to integrate it with other components of their OSS architecture. To this end, it will typically be necessary for the NCCM vendor to provide a comprehensive and well documented application programming interface (API) for allowing its customers and partners to programmatically gain access to core platform data and functionality. Ideally the API will be completely described through a comprehensive Web Services Definition Language (WSDL) allowing a variety of available Web Services tool kits to generate client-side proxies, in a variety of languages (e.g. SOAP/XML, etc.) offering portability to application developers.

3.6.2 FAULT MANAGEMENT

Integrating an NCCM platform with an OSS fault management platform can be of considerable benefit to a MSP. The functionality likely to be required by a MSP would typically include the following:

- Depending upon the configuration-related event, the NCCM platform can send an event to the fault platform, flagging the issue to operations staff. Operators may then drill down in context from the fault management system GUI and view an audit trail of appropriate configuration changes. If necessary, the operator could instigate a roll-back from the NCCM platform.
- Change related events can also be highlighted, e.g., flagging configuration change maintenance windows, highlighting unauthorized changes, highlighting repeated log-in failure.
- Depending upon the particular fault management system deployed, if a configuration change occurs within an agreed maintenance window, the severity or impact of the alarm could be weighted appropriately. Further, if a config change happens in a freeze period/business day then a higher impact can be added.
- Implementing an NCCM tool on the network and enforcing policy and control over configuration changes should have the impact of both reducing the number of “Root Cause” events associated with configuration problems and by association reducing the number of service trouble tickets created by the level 1 customer support desk. Those operators that have already implemented a degree of RCA from vendors such a MicroMuse, EMC Smarts and HP will probably already be aware of the fact that most service-impacting problems are configuration related. The cost improvement from an end-to-end processes perspective can be significant as one configuration problem on a single device can result in multiple service ticket requests generated at the level 1 help desk.

3.6.3 INVENTORY

Many MSPs prefer not to “discover” network devices (via wide discovery address ranges) but to data fill their OSS tools to discover specific devices via a seed file. Consequently, a NCCM platform would typically be seeded by an inventory platform (or other component) of the OSS architecture.

That being said, NCCM platforms could also be used to seed the inventory platform with device and interface-related information. While an NCCM platform is less likely to model service-related information, it could be used to seed the configuration status of a device or interface into the inventory (e.g., Whether a VPN Route Forwarding (VRF) instance is applied to a particular interface)

There is also typically a requirement to synchronize all configuration changes to the incumbent inventory management platform. Integration between the NCCM solution and incumbent inventory tools would mean that any requests that rely on accuracy of data within the inventory management system, such as change planning, modelling, provisioning, etc., would be referencing accurate real-time configuration data. The NCCM solution could notify the inventory system whenever a new device has been added to the application, or periodically import or export inventory information. In doing so the inventory system could be brought ‘closer to the network’ by providing real-time network information and manual system input significantly reduced. This could conceivably deliver great value to those operators that integrate their inventory management platform to their

provisioning system; ensuring that all configuration changes are synchronized would reduce the risk of failed service activation requests.

3.6.4 SERVICE PROVISIONING/ACTIVATION

The interaction of a service provisioning/activation tool, and an NCCM platform can be complex:

(i) *Service Provisioning/Activation Tools*

A MSP will usually deploy a service provisioning/activation tool to support the following business needs:

- Support services and service volumes, in-line with service rollout requirements
- Reduce activation time for existing services
- Support the deployment of multivendor equipment within the network
- Support increased levels of integration across OSS systems

Furthermore, operationally, such tools can provide the following benefits:

- Control over application of pre-designed/approved service-related configurations to the network
- Support for repetitive but complex configurations (e.g., QoS configurations)
- Resulting reduction in headcount and thus OPEX

The ability to realize these benefits depends heavily on the nature of the services being deployed. An MSP deploying a large volume of similar IP VPN services will gain a lot of benefit. A smaller network with a small number of services, a low service turnover or significant variance between deployed services is less likely to.

The level of benefit achieved also depends on the Operational Model and operating environment. If a provisioning tool is deployed as part of an end-to-end automated delivery process and is highly integrated into other systems, such as the sales order processing system, and other OSS tools, a significant benefit can be achieved.

Service activation tools vary in their capabilities. Some will hold a detailed model of the service and the supporting network topology and services will be represented as managed objects within this model. Others will hold a much simpler network view and are little more than configuration “wizards” with a basic service registry.

Some may perform much of the resource assignments, while some rely on other systems to perform this function, and require the assignments to be passed to them. Some Service Activation tools include basic workflow capability to manage and coordinate the configuration activity and to perform rollbacks if any device configuration fails.

Most service activation tools have a limited set of services that they support. Such tools will have a very close coupling to the underlying network and may only support specific vendors models, or OS versions. They may also have a relatively restricted model of a “service.” In general, tools with very detailed service knowledge and capability suffer from being less flexible. Conversely, tools with

greater flexibility tend to have restricted domain knowledge, and require more development and maintenance.

It is also important to note that any Service Activation tool will only manage a small proportion of the configuration activities on the network; those associated with service configurations. Any other activities are normally outside the capabilities of these systems. This can present a quandary as there can be major dependencies between the service configuration and the underlying network configuration.

In conclusion, while a service activation tool provides a good environment for managing, recording and constraining service configuration, it cannot necessarily enforce or verify the underlying network configuration and prevent changes to it which may have service impacts.

(ii) *NCCM Platforms*

NCCM platforms can focus on the underlying network configuration of a device configuration, which can often be the majority of the overall device configuration.

It is important that the MSPs operational model supports the careful management of configuration as distinct from service activation.

However, the interaction between a service activation tool and an NCCM platform must be carefully implemented such that they do not conflict.

For example, when a Service Provisioning/Activation tool activates service on a network devices (e.g., attaching a QoS policy to an interface), the NCCM platform must be aware that this is a legitimate change to the overall configuration of the device and not attempt to reverse the change. Similarly, highlighting such a configuration change via a fault management tool would be operationally counter productive.

In this scenario, the NCCM tool functionality must be carefully configured to de-conflict with the Service Provisioning/Activation tool, and it may be that not all NCCM functionality is used to its fullest extent; for example the NCCM tool does not proactively highlight or reverse specific configuration changes, but could still be configured to periodically audit the device to ensure that all ACL, SNMP and AAA configuration is appropriately implemented.

3.6.5 SYSTEM ADMINISTRATION

A key role of an NCCM platform is to intelligently back-up device configurations. Many MSPs may elect to protect these back-up files by integrating NCCM functionality with industry-standard back-up software and practices (e.g. use of SAN)

4 REGULATORY COMPLIANCE AND INDUSTRY BEST PRACTICE

Emerging challenges for MSPs exist in the form of compliance to technical and financial standards and legislation. Key Enterprise clients, many of whom form part of the highly regulated Financial Services sector are increasingly subject to governmental regulation such as Sarbanes Oxley (SOX) and Basel II.

Compliance legislation requires management and network professionals to attest to documented and auditable internal controls that hold the company accountable for the most important business functions.

Telecommunications Companies are not immune to this legislation; severe financial and legal penalties are being implemented for companies that do not adhere to compliance laws. Furthermore, the ability to demonstrate adherence to such codes of best practice is also increasingly becoming a competitive differentiator for MSPs in an already competitive marketplace.

4.1 INTERNAL STANDARDS

This may involve ensuring networks are configured as designed and approved by the MSP design authority, therefore underwriting service quality. The maxim that “the majority of faults are down to mis-configurations” can be addressed by pro-actively checking for configuration compliancy in network devices.

Similarly, in order to secure their networks, MSPs must ensure that devices are configured to comply with agreed security policies. For example, an NCCM tool may regularly check that all devices have the appropriate ACL, SNMP and AAA configurations applied, and where inconsistencies are found, potentially automatically apply the relevant configuration.

The use of NCCM platforms in this manner can support vulnerability assessments and prove compliance to security components of industry standards.

4.2 INDUSTRY STANDARDS

Many MSPs have embraced the eTOM and NGOSS initiatives, driven by the TeleManagement Forum (TMF). Equally, ITIL is being increasingly adopted as the standard for best practice in the provision of IT Service, and will soon be an ISO standard.

However, the impact of the requirements of such legislation as Sarbanes Oxley and European equivalents such as Basel II are starting to be felt by MSPs.

Although MSPs not listed in US exchanges are not strictly subject to Sarbanes Oxley, even those that are not may consider adherence with its principals in terms of good corporate governance. Similarly, although Sarbanes Oxley and Basel II focus on financial activities, there are security-related requirements; further, information held within configuration databases or inventories may have a financial aspect (e.g., rent and revenue of mobile phone masts)

4.3 CUSTOMER DEMANDS

Increasingly, MSPs are being asked to demonstrate compliancy with their customers' requirements in terms of standards. This particularly includes customers insisting that MSPs are ITIL compliant.

It is considered that customers, particularly those in the financial sector, will increasingly require MSPs to demonstrate how their networks and services comply with supporting the customers' adherence to legislation such as Sarbanes Oxley and Basel II.

Further, in order to support service levels, MSPs must be able to demonstrate to customers that services were correctly configured and delivered.

4.4 DEMONSTRATING COMPLIANCY

There is an associated cost with supporting and being able to demonstrate compliancy to the standards, initiatives and legislation discussed above.

Historically, many MSPs with IP networks have operated with limited formal configuration and change management tools and processes. Although some have deployed expensive service provisioning/activation platforms, the complexity in terms of the requirements regarding the demonstration of compliancy have increased significantly.

Further, in an MSP environment, compliancy to standards may have previously been considered to be meeting OSS standards, e.g., NGOSS. For Managed MSPs, where many of the services provided are application based (eg: DNS management, etc), ITIL becomes increasingly if not more pertinent.

Demonstrating ITIL compliancy may involve being independently audited to show that the MSPs processes are ITIL compliant. NCCM platforms can support in terms change/release and configuration management.

4.5 ITIL

Although the UK Government originally created the IT Infrastructure Library (ITIL), it has rapidly been adopted across the world as the standard for best practice in the provision of IT Service.

Historically, MSPs provided network connectivity and management of that network to customers; however the network has increasingly become transparent as customers look to MSPs to provide access, connectivity, security and IT services such as hosting and content delivery. Whereas service delivery once concerned the delivery and management of networks, it can now also include the management of IT services themselves, and involves a number of management practices to ensure that IT services are provided as agreed upon between the MSP and the Customer.

ITIL comprises a series of documents that are used to aid the implementation of a framework for IT Service Management. ITSM is itself generally divided into two main areas: service support and service delivery. Service Support is the practice of those disciplines that enable IT Services to be provided effectively. The six Service Support disciplines are:

- Configuration Management - Pertaining to the implementation of a database (Configuration Management Database – CMDB) that contains details of the organization's elements that are used in the provision and management of its IT services. This is more than just an

'asset register,' as it will contain information that relates to the maintenance, movement, and problems experienced with the Configuration Items.

- Incident Management - Pertaining to the resolution and prevention of incidents that affect the normal running of an organization's IT services.
- Problem Management: - See Incident Management above.
- Change Management - Pertaining to the practice of ensuring all changes to Configuration Items are carried out in a planned and authorized manner. This includes identifying the specific Configuration Items and IT Services affected by the change, planning and testing the change, and having a back-out plan should the change result in an unexpected state.
- Service/Helpdesk - This plays an important part in the provision of IT Services. It is very often the first contact the business users have in their use of IT Services when something does not work as expected.
- Release Management - Pertaining to the management of all software configuration items within the organization. It is responsible for the management of software development, installation and support of an organization's software products.

NCCM platforms can support the implementation ITIL, particularly in terms of Configuration, Change and Release Management. For example, Configuration Management essentially consists of four main tasks:

- Identification – the specification, identification of all IT components and their inclusion in the CMDB.
- Control – the management of each Configuration Item, specifying who is authorized to 'change' it.
- Status – the recording of the status of all Configuration Items in the CMDB, and the maintenance of this information.
- Verification – reviews and audits to ensure the information contained in the CMDB is accurate.

There is growing evidence of Enterprise customers insisting that MSPs be in a position to demonstrate the degree to which delivered IT services are ITIL compliant.

4.6 ENHANCED TELECOM OPERATIONS MAP (eTOM)

4.6.1 OVERVIEW

The *Enhanced Telecom Operations Map* is the most widely used and accepted standard for business process in the telecom industry. The eTOM describes the full scope of business processes required by an MSP and defines the key elements and how they interact, creating a guidebook that is becoming the common business language of the telecom industry.

At the conceptual level, eTOM can be viewed as having the following three major process areas:

- Strategy, Infrastructure and Product covering planning and lifecycle management

-
- Operations covering the core of operational management
 - Enterprise management covering corporate or business support management

The process structure in eTOM uses hierarchical decomposition, so that the business processes of the enterprise are successively decomposed in a series of levels. Process descriptions, inputs and outputs, as well as other key elements are defined. The Framework also includes views of functionality as they span horizontally across an enterprise's internal organizations.

A particular strength of eTOM as a business process framework is that it is positioned within the next-generation operational support systems (NGOSS) program and links with other work underway in NGOSS. In particular, eTOM provides the Business Map for NGOSS and is a prime driver for business requirements to feed through from the NGOS Business View to the System View and eventually into the NGOSS Implementation and Deployment Views.

The focus of eTOM is on the business processes used by MSPs, the linkages between these processes, the identification of interfaces, and the use of customer, service, resource, supplier/partner and other information by multiple processes.

4.6.2 NCCM ALIGNMENT WITH ETOM

Depending upon how an NCCM platform is implemented at an MSP, it may support multiple eTOM Business Process Groupings, particularly including the service and resource management and operations horizontal groupings that span the operations vertical grouping

The eTOM diagram below provides some indicative areas where the NCCM would directly support key business processes.

The mappings shown in the diagram below will clearly depend upon the specific NCCM platform employed and the nature of the deployment and integration, and consequently are purely illustrative.

However, it is important to note that a well implemented and integrated NCCM platform can provide key support to more than the just the resource provisioning or service configuration and activation processes. NCCM may also support Service Problem and Service Quality Management processes, as well as problem handling and, more importantly, customer QoS/SLA Management

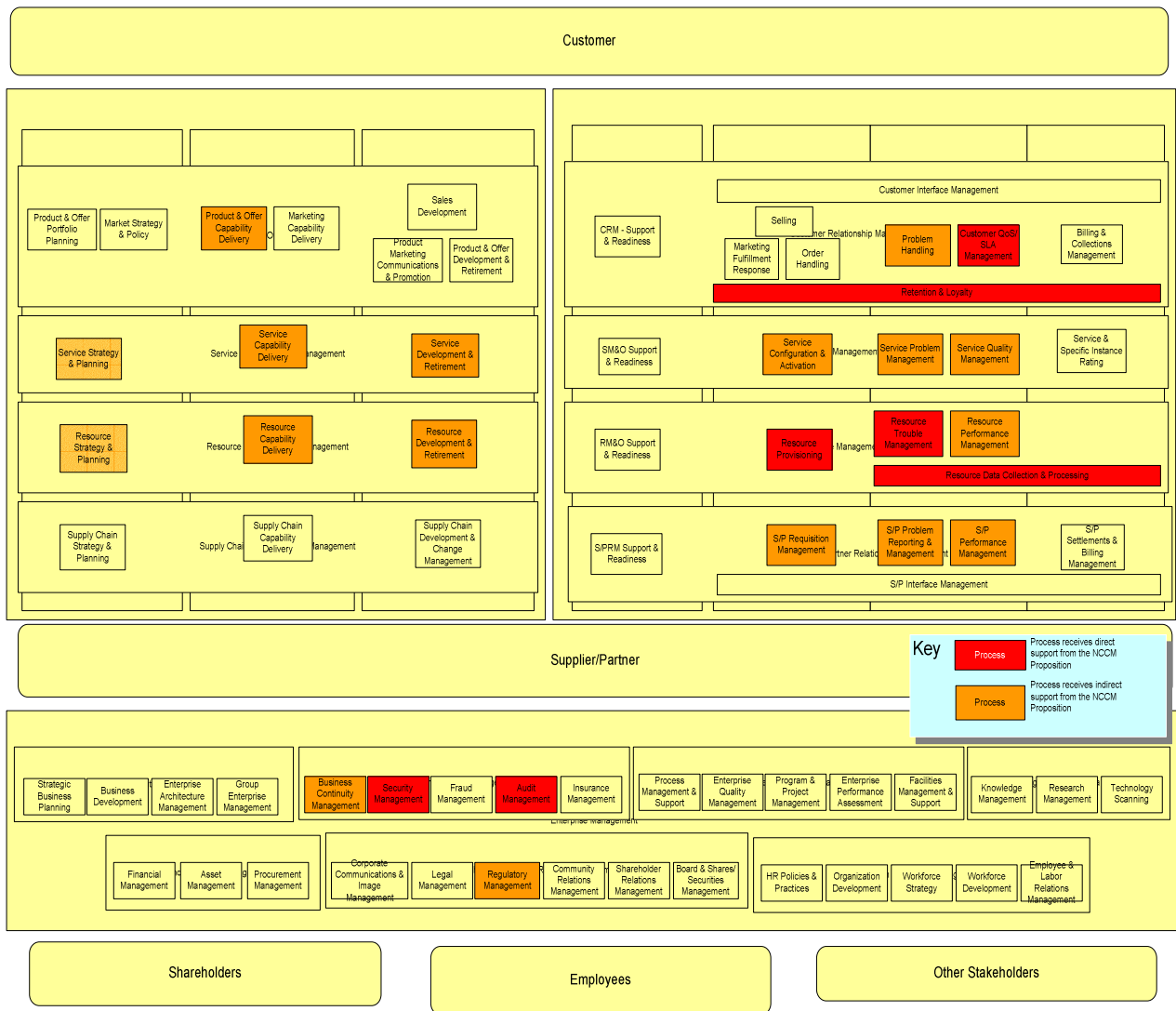


Figure 2 - ETOM Alignment with NCCM

Indeed, there may be other areas in which the deployment of an NCCM platform could indirectly assist with business processes, including:

- *Service strategy and planning*; does the MSP have the correct resources available to deliver the service, how configurations need to be changed/modified to support new planned services, etc.
- *Business continuity management* with Configuration Backups
- *Security management* via enforcement of security config policy, ACL bulk changes, etc.

In terms of the overall business activities of the MSP, the NCCM solution may also support Audit and Regulatory Management, and depending upon how the platform is utilized it may also be possible for it to support processes in the Infrastructure and Service Lifecycle Management horizontal groupings.

5 NCCM BENEFITS FOR THE MSP

The deployment of an NCCM platform brings a variety of benefits to a number of areas of a MSPs business.

While all MSP networks require some level of NCCM functionality, ranging simply from intelligent device configuration back-up to compliancy checking and automatic re-configuration, the degree of implementation and integration should be appropriate for the individual MSP.

As discussed above, the most challenging issues will typically be the interaction and/or integration with a service provisioning/activation tool. An operator without a Service Provisioning/Activation tool can certainly expect to derive significant benefit from deploying an NCCM tool. Operators with a service provisioning/activation tool in place could still benefit from an NCCM implementation, especially if they operate a large and vendor-diverse network, or if the inventory management platform is used as the prime reference for activation or if they are subject to internal compliance regulations.

MSPs with Service Provisioning/Activation tools should evaluate how applicable their existing platforms are in the context of the above requirements and also consider the operational benefits of integrating Service Provisioning/Activation with a next-generation NCCM management platform. The extent of the MSPs existing OSS architecture will dictate to what degree integration is required. An operator with a 'green field' OSS environment may rapidly deploy an NCCM platform, realizing immediate value of its functionality. Integration with the broader range of OSS tools can then be addressed.

5.1 REDUCTION IN OPEX

Historically many MSPs running IP networks have developed change processes that are somewhat non-optimal. Often this is because such processes were leveraged from non-IP legacy networks. Many MSPs have yet to implement effective and robust processes and tools to manage change within their networks. Increasingly, NCCM platforms support sophisticated workflow functionality, and can integrate more easily into a MSPs overall change management process. Indeed, these tools can dramatically improve the effectiveness of such processes if they are fully embraced by the organization.

Automation provided by next-generation NCCM solutions can reduce time spent on configuration tasks from minutes per device to minutes for an entire network. Periodically performed tasks such as credential rolls, ACL updates and OS updates can frequently be executed in a fraction of the time it would take to do the same tasks manually. This means that staffing levels can be maintained at their current levels or even reduced, while enabling the management of much larger networks.

Other improvements in operational efficiency that can be anticipated from the adoption of next-generation NCCM platforms include:

- Speed, predictability and efficiency of configuring new and existing services
- Reduction in numbers of trouble-tickets
- Inventory reconciliation and improved accuracy

-
- Consistent application of business policies
 - New service enablement- CoS/QoS lowest cost, best path selection of route– by providing “as is” vs “as planned” network information to upstream provisioning systems.

IT departments also incur large recurring operating costs in the form of vendor maintenance contracts – these contracts. These are typically based on the number of devices deployed in production. Organizations are left with few choices: they can elect to simply pay the vendor invoice or to try to reduce these costs by undertaking a manual (and hence costly) inventory-reconciliation exercise. NCCM solutions would assist with this task via the automatic creation of a more definitive picture of network inventory in the form of a report using appropriate filters for specific vendor/model types.

5.2 IMPROVED SERVICE AVAILABILITY AND MTTR

According to Enterprise Management Associates, a leading industry analyst firm, between 60 to 80 percent of network outages and service-affecting network problems are caused by change. Improved network service availability can be achieved by consolidating and enhancing fault management/root cause analysis activities via tight integration with a NCCM solution. Such integrations would allow network operation staff to quickly view a history of device changes in configuration, hardware or operating system. Network operators could even be allowed to ‘roll back’ the offending change and quickly return the network to a known state - resolving the problem quickly and efficiently. In summary, such integrations can help identify configuration-related faults more quickly. This in turn can result in decreased MTTR, increased levels of configuration accuracy and improved service levels.

5.3 REVENUE GENERATION AND COMPETITIVE DIFFERENTIATION

Managed MSPs will likely be able to charge a premium for a subset of the NCCM functionality back to their customers, which should result in an NCCM implementation delivering bottom line revenue.

- Delivery of Compliance Reports for the customer environment
- Delivery of configuration changes based on the customer requirements
- Delivery of per-device software changes, updates and password rotations
- Delivery of web-based, per-user views relating to configuration, compliance and change

A Managed Services operator with advanced NCCM technology will likely be able to create a business case based on the reduction in manual processes and time for key configuration changes that are required by the majority of network operations departments today.

5.4 STANDARDS AND LEGISLATIVE COMPLIANCE

Enterprise customers are now frequently required to comply with legislation such as Sarbanes Oxley (SOX) and are looking for their MSPs to demonstrate how they support this legislation. Equally, MSPs are being pressed to prove compliancy to industry standards and initiatives such as ITIL. MSPs are increasingly looking to align with such initiatives in the interest of good corporate governance.

All of the above are important to maintaining existing customers and well as winning new business. An NCCM platform is a key tool in supporting this capability, and even if not viewed as an immediate requirement will, in the medium to long term, position and prepare the MSP for the broader industry drive for compliance.

For example, an NCCM platform may support the controlled authorization of network changes, making such changes visible to staff throughout the organization and allowing centralized sign-off on proposed changes. In the event that a change is made which negatively impacts the network, the NCCM platform can make it easy to see what change was applied where, when, by whom and whether the proper process was followed. It could also easily support 'roll-back' to a previously known state.

This level of change management is often somewhat lacking, even though the importance of change management is increasingly recognized as critical at both customer and senior management level.

5.5 CONFIGURATION COMPLIANCE VISIBILITY

It is widely accepted that the majority of network faults are caused by mis-configuration as opposed to equipment or network component failure. This being the case, the ability to ensure that a configuration applied to a network device is 'as designed' and approved by an MSPs design authority has never been more critical. Not only can an NCCM platform identify compliance to approved configurations/templates, but it can also highlight inconsistencies to operators, and if required, automatically impose the correct configuration components on a device. This provides increased visibility of the configuration status of the entire network to operations

6 CONCLUSION

Long-term business growth and a sustainable operational model will only be achieved once MSPs have been able to overcome the complex mix of operational and technology challenges associated with network configuration and change management.

MSPs seeking to grow service revenues, improve customer satisfaction and reduce operational costs will increasingly adopt a highly integrated approach to network configuration and change management. To ensure a high degree of consistency, this discipline must be underpinned by next-generation solutions that are tightly coupled to existing tools, leveraging investment and facilitating automated information workflow.

Applicable solutions are best selected via a detailed comparison of the architectural features and capabilities detailed above, and extensive evaluation testing within a representative environment, mirroring the size, complexity and transience of the real-world infrastructures which underpin today's managed services.