META Group

META Delta

2 December 2002 **File: SMS 1133**

Network Configuration Management

Service Management Strategies

Glenn O'Donnell

Network configuration management has traditionally been a vendor-centric and disorganized activity. However, increased demands for efficiency and operational discipline are forcing IT organizations to pursue structured systems for multivendor environments. Ultimate solutions will require further evolution in management tools, embedded agent technologies, and organizational culture.

Network configuration management (NCM) remains limited to element management tools specific to hardware vendors (e.g., Cisco's CiscoWorks, Nortel's Optivity) and exclusive groups of network engineers. Virtually all NCM is currently accomplished using more restrictive approaches. The evolution of NCM is now accelerating in both technical and cultural aspects, driven by an intensified need for strict governance and smooth execution. By 2003/04, 10% of Global 2000 enterprises will be using broader NCM products. The immaturity of available products will mitigate this progress through 2004, when more comprehensive NCM tools and operational culture will mature. By 2005/06, broad heterogeneous NCM will be popular (50%-60% of G2000). Targeted outsourced services will account for 5%-10% of all G2000 NCM efforts by 2003/04, and 30%-40% by 2006.

Cisco is currently the dominant NCM vendor, mainly because it leverages its dominance in network hardware. It is also leading many developments in embedded agent technologies (e.g., NetFlow, Service Assurance Agent) and auxiliary technologies (e.g., security, appliance-based management). No hardware vendor will effectively provide heterogeneous configuration management; however, they will continue to drive embedded technologies for use by broader management products.

Emerging vendors (e.g., Intelliden, PowerUp Networks, AlterPoint, Goldwire, Rendition Networks, DSET) are attempting to unify NCM by normalizing configuration functions across multivendor device environments. Several of these vendors offer clever technology solutions to insulate users from the idiosyncrasies of each vendor's interfaces. All are early in their life cycles, so additional development is required for truly broad applications. Early versions show promise, though they currently almost exclusively support Cisco configuration, with additional vendor support targeted for future development.

Operational support system vendors have long supported network service providers, performing NCM of circuit-switched and IP carrier networks (e.g., Visionael, NetCracker, MetaSolv, Orchestream). Some are beginning to target the needs of enterprises for NCM (see SMS Delta 1079). Such products tend to be much broader in scope to cover provisioning and other operational support system functions, but enterprises with more advanced operational maturity can benefit.

Traditional enterprise infrastructure and application management (IAM) vendors (e.g., HP OpenView, IBM Tivoli, CA, SMARTS, Aprisma) all offer limited NCM capabilities, though none functions well for broad-based configuration. However, these tools do play a major role in autodiscovery of network devices and mapping the relationships between them. These relationships are as important to the configuration management of networks as device-centric characteristics. Both perspectives must be considered for full NCM, ideally joined by integration hooks in the software to propagate relationships across the two.

META Trend: During 2002/03, real-time reporting tools will remain at element levels, but will evolve additional intelligence (e.g., in-context analysis) through 2004. Although operational metrics will shift from bulk to exception reporting, integration of disparate performance data will still be a manual effort through 2005. Through 2006, service-level "everything" (reporting, verification, management, etc. — SLx) will remain market noise and partial reality.

Through 2004, vendor consolidation will accelerate because enterprise and service provider automation systems are

merging and established IAM vendors will seek features now pioneered by emerging vendors. Acquisitions are certain, because these emerging vendors are unlikely to survive independently.

NCM has several economic benefits to the IT organization, including the following: it ensures integrity of the infrastructure by minimizing mistakes; disaster recovery and incident resolution are faster and easier, reducing operational expenses and adverse business impact; and standardized tasks and processes result in a diminished dependence on high-salary, high-skilled experts and fewer staff members overall (realistically, as low as 25%) to manage the same environment. In addition, much of the operational power is distributed more evenly across personnel instead of a select class of experts. This elite group is more effectively used for architecture development and infrastructure design, not operations.

Primary operational ownership will migrate from network subject-matter experts (SMEs) to the command center (see SMS Delta 1002). As organizations centralize management functions into the command center (see SMS Delta 1056), NCM will need to augment monitoring systems to enable adaptive control functions. SMEs will still require access to NCM systems, but unfettered access is discouraged for all parties. No configuration management system can be effective without a rigorous change management process to ensure stability of the configuration as well as the infrastructure itself.

Meticulous structure is a hallmark of a good configuration management system, which will always work in tandem with strong change management. Operational efficiency benefits from common tasks, consistent interfaces, thorough checks and balances to prevent misconfiguration, and accurate data to assist incident management, capacity planning, and problem management. Tools should be used that track versions to follow configuration changes and enable a retreat if configurations fail to meet expectations.

A popular method of configuring networks is via command line interfaces (CLIs), such as Cisco's IOS. These methods offer extensive freedom and flexibility, but they are also severely error-prone without strong tools to prevent the execution of mistaken or malicious configuration commands. Liberal access to CLI configuration is dangerous and inefficient, even if those given such access possess superior talents. Whenever possible, direct human interaction with network hardware should be avoided.

An enormous benefit of NCM tools is the widespread modification of configuration parameters across the infrastructure. A device-by-device approach is an overwhelming burden. Automation of these tasks is easy, but some SMEs will resist, because automation curtails their perceived value. Such automation is necessary and inevitable; without it, IT organizations will be unnecessarily crippled by inefficient practices.

Communication protocols for NCM are mixed. While almost all equipment vendors support SNMP (Simple Network Management Protocol) for retrieving management information, many avoid or restrict its use for active configuration changes. The significant security vulnerabilities of SNMP Version 1 are to blame. Justifiably, network managers and vendors did not trust SNMPv1 for this sensitive task. The response to this issue manifested itself in the form of the CLI. Although admittedly better than SNMPv1 in some respects, this ubiquitous method is still riddled with security concerns, in addition to its cumbersome use and cryptic syntax. SNMP Version 3 (Version 2 was aborted) solves the majority of security concerns, but XML-based communication is gaining acceptance for management systems. By 2005/06, most NCM traffic will use XML encoding, with SOAP or HTTPS as the underlying transport protocol. Through 2010, SNMP will continue to serve as a supplier of read-only information, very slowly succumbing to the challenge of XML. NCM tool vendors are all adapting to XML and other standard object technologies, but equipment vendors must also comply.

Bottom Line

Organizations should migrate away from dependence on highly manual network configuration management that is costly and error-prone. Broad multivendor solutions are still early in their evolution, but technology will mature quickly. Operational culture will be the most tenuous impediment.

Business Impact: Operational automation yields lower operational expenses, robust IT infrastructure, and more consistent services.