

Adaptive Network Configuration Management:  
**Aligning People, Business  
Processes, and Systems**



When information comes together,  
your world moves ahead.

## Executive Summary

Business models are increasingly dynamic. Mergers and acquisitions significantly affect organizational structures. Uncertain economic environments with markets that expand and contract with little warning wreak havoc on traditional long-range planning processes. As a result, enterprises constantly must find ways to adapt quickly and wring efficiencies out of everything they do.

The challenges of this environment force many enterprises to reduce IT costs and control complexity—while ensuring they allocate enough of the right resources to achieve business objectives. To prosper, an enterprise must clearly prioritize its requirements, as well as find innovative ways to conserve its human and material resources while meeting its objectives.

To make matters worse, customer expectations for service have become rigid. Accustomed to the promise of a web-enabled world, customers expect business information and services to remain constantly available, from anywhere, in a way they deem most suitable, and with a guaranteed quality of service. IT organizations must virtually eliminate downtime and have the ability to respond immediately to customer issues.

Sophisticated enterprises now demand an automated, agile, and disciplined approach to network change and configuration management. Imagine a network operations center in which all network documentation is persistently accurate; where you can identify any network change activity instantly; where all network changes are approved, scheduled, and archived. Imagine the increase in operational productivity. Imagine the insight your operations staff will have with a realtime view of network faults and performance that they can immediately correlate with network changes. Imagine the peace of mind you will have when you know that all unauthorized network changes can be rolled back automatically based on your policies. This is all possible with network configuration management within an adaptive management framework.

This document provides a pragmatic, process-oriented roadmap that enterprises can follow to improve network performance, and create an efficient and reliable infrastructure that delivers the service the business demands. It then outlines how EMC® VoyenceControl™ can automate these business processes and how VoyenceControl can be integrated adaptively within an existing network management environment.

## Adaptive Network Configuration Management

Enterprises no longer can afford an unreliable network infrastructure. Rapid restoration and recovery from any network outage is a mandate for all network operations organizations. To accomplish these objectives, operations groups have invested in fault and performance management systems. Fault management platforms have become increasingly sophisticated in identifying the root cause of network faults. Performance management systems work to analyze and report network and application performance metrics to address issues before they turn into problems. To counter increasing security threats, organizations have also deployed intrusion detection and intrusion prevention systems.

In large measure, the discipline in today's network operations that has been neither automated nor optimized is network configuration management. Industry analysts estimate that 50 percent to 70 percent of all network outages are directly attributable to errors introduced during manual change processes.

Further, 90 percent of network fault-, performance-, or security-related events require changes to the network configuration. In the absence of good process and a holistic solution, network configuration management is accomplished through a combination of outdated network diagrams, spreadsheets with network-access information, vendor-specific tools, semi-automated scripts, or by directly logging into the devices.

One of the best ways to address these network management challenges, and improve network reliability, is to implement a network configuration management process and an automated solution. Many organizations consider this business-critical discipline as an essential success factor in mastering today's complex, dynamic, and distributed networks. Network configuration management is the science of organizing, documenting, and controlling continually evolving networks.

The introduction of a network configuration management discipline in an enterprise should be a phased approach that results from an investment in people, processes, and systems within the framework of an adaptive methodology.

From the point of view of business objectives, network configuration management enables an enterprise to:

- Control the full process of network design and modification—continuously
- Identify potential problems before they harm the infrastructure
- Measure the performance of the network change process, which results in:
  - Improved network availability
  - Improved enterprise productivity
  - Lower overall costs

Network configuration management solutions must address:

- Network configuration version management
- Network document generation
- Network change job scheduling
- Change process management
- Distributed device communication and control
- Change auditing and reporting

## Staffing Network Management Resources to Maximize Success

Historically, the staffing of network management personnel was an ad hoc chore resulting in a group of highly skilled, multi-use technicians playing the roles of network administrators, network operators, and network engineers. This staffing model is expensive because expensive network engineers often find themselves performing routine and repetitive tasks that, with proper tools and processes, could be safely delegated to less-skilled (and lower-cost) entry-level network personnel.

With the increasing complexity of network infrastructure and the requirement to design networks that support many specialized service levels, network staffing must become as rigorous as traditional data center staffing.

To maximize the success of the operation, staff models must recognize several specialized and expert roles for the networking professionals and several levels of required certifications. Some of the key roles that should be included are:

- **Network Architect**—Responsible for developing the key standards and guidelines for the network architecture, this role requires a thorough understanding of the business requirements, current vendor offerings, technology trade-offs, and future strategic-planning abilities. A network architect's responsibility includes:
  - Identifying the impact of current and future business needs on the technology infrastructure
  - Establishing the network availability and performance metrics to meet business objectives
- **Network Security Specialist**—This role is chartered with developing the network security blueprint that acts as the first line of defense against malicious network intrusion and unwanted access. With the increasing threat of security breaches, viruses, and other malicious activity—all of which can have crippling effects on enterprise operations—an absolute requirement exists for establishing and maintaining a proactive security stance. The network security specialist is a key contributor to the overall security blueprint, and must define the security policies for firewalls and routers.
- **Network Design Engineer**—This role is responsible for developing the engineering packages that define the hardware, capacity, and configuration of all planned and deployed network devices. Network design engineers define the routing, access control, and quality-of-service policies for all network devices. They ensure that network uptime and performance meet the metrics defined by the architects. Network design engineers review and approve all planned changes to the network before those changes are deployed. Network design engineers are also responsible for managing the capacity (including utilization and saturation) of wide area networks to ensure that the available bandwidth is meeting business needs.
- **Network Operations Specialist**—This role is responsible for ensuring maximum availability and the highest performance across the entire network infrastructure. The operations staff monitors the network for any fault, identifies adverse performance trends, and watches for any unplanned change activity. The operations specialist should deploy contingency plans and configuration changes in the event of network fault or performance degradations.
- **Network Technician**—This role is responsible for maintaining the configuration of the network (including device configurations, circuits, etc.), coordinating with vendors and service providers on move, add and change activity, and ensuring that the physical infrastructure is built out to the highest professional level.

## Develop a Process to Improve Network Availability

The first step in upgrading the configuration management of networks is to introduce a network configuration management process that instills the discipline and control required to manage the network change process.

In a business-aligned network infrastructure organization, the processes and procedures for network deployment, maintenance, and upgrade activities are well-defined and communicated to the internal staff as well as the external service providers. The processes used are well-documented, readily available, and consistent with the way work actually gets done. The process definitions are updated when necessary, and improvements are developed through controlled pilot tests, cost-benefit analysis, or both. An objective, quantitative basis judges process quality and analyzes problems with the process and operations. When schedules and budgets are based on historical performance, the expected results for management cost, network availability, and reliability are usually achieved. Disciplined organizations follow a process consistently because all participants understand the value of doing so, and the necessary automation infrastructure exists to support the process.

In an adaptive network configuration management process, the organization develops the capabilities to anticipate change events and respond to them systematically.

### Phase 1: Choose a Discrete Project to Start

The first step in getting control of chaos is to establish procedures for managing configuration and change in networks. Establishing basic process management discipline on a project-by-project basis is an excellent way to begin. Over time, network configuration management procedures may be refined, documented, practiced, trained, measured, and improved upon.

The following steps are offered as a best practice for getting started:

1. Capture the current network image
2. Produce up-to-date network documentation
3. Back up all device configurations to a centralized server
4. Capture device access passwords and SNMP read-write strings
5. Integrate a user-, group-, and role-level authorization process around change accounting and auditing
6. Update the device configurations to report all change activity to configuration management system
7. Ensure all user device access requires TACACS+ authentication (or something similar)
8. Create an updated network diagram and keep them synchronized with all network changes
9. Internally publicize your change management process with peer-level reviews and approvals before making changes to the network
10. Implement maintenance windows for all pre-scheduled changes in the off-business hours
11. Implement a change-audit process that reconciles all unauthorized and unreviewed changes to the network configurations

## Phase 2: Baseline, Secure, and Standardize

After the introduction of a change management process, the network operations specialist needs to fortify the network configuration and focus on standardizing on a set of best practices and network-wide configuration and security policies. This is critical to ensuring consistent network performance, as well as eliminating chances of one-off configuration errors and security lapses due to incomplete configuration profiles. The result is proactive management of the network where operators can anticipate and mitigate network downtime.

The major tasks that need to be accomplished in this phase include:

- Conduct a security audit of all network configuration files including a detailed review of all access control lists
- Review the device configurations against the NSA security guidelines (see Report Number C4-040R-02, available at [http://www.nsa.gov/snac/routers/cisco\\_scg-1.1b.pdf](http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf))
  - Router security policy written, approved, distributed
  - Router IOS version checked and up to date
  - Router configuration kept offline, backed up, access to it limited
  - Router configuration is well-documented, commented
  - Router users and passwords configured and maintained
  - Password encryption in use, enable secret in use
  - Enable secret difficult to guess, knowledge of it strictly limited
  - Access restrictions imposed on Console, Aux, VTYs
  - Unneeded network servers and facilities disabled
  - Necessary network services configured correctly (e.g., DNS)
  - Unused interfaces and VTYs shut down or disabled
  - Risky interface services disabled
  - Port and protocol needs of the network identified and checked
  - Access lists limit traffic to identified ports and protocols
  - Access lists block reserved and inappropriate addresses
  - Static routes configured where necessary
  - Routing protocols configured to use integrity mechanisms
  - Logging enabled and log recipient hosts identified and configured
  - Router's time of day set accurately, maintained with NTP
  - Logging set to include consistent time information
  - Logs checked, reviewed, archived in accordance with local policy
  - SNMP disabled or enabled with good community strings and ACLs
- Develop enterprise-wide network security policies and manifest them as network device configuration templates
- Review routing protocols to ensure implementation with restoration and recovery parameters
- Review the applicability of BGP and MPLS to the environment to enhance resilience
- Ensure that quality-of-service policies are consistently configured in all routers
- Develop and implement quality-of-service policy configuration templates to standardize quality of service across routers

### Phase 3: Analyze and Optimize

With the baselining of network configurations, an opportunity exists to optimize the network architecture and performance against key business metrics. This ensures appropriate sizing and configuration of network assets to meet current and predicted business needs. This requires capturing of utilization and saturation metrics, as well as simulating future business scenarios.

### Phase 4: Integrate and Leverage

Integration of network configuration management solutions with problem, fault, performance, and security management solutions is the capstone leading to adaptive management of networks. Sharing of key configuration management data and events with the fault management system, for instance, provides new insights into root-cause analysis. Trending in performance management systems is more meaningful when correlated with network change activities.

Figure 1 illustrates and visually summarizes the aforementioned four phases of bootstrapping a rigorous network configuration management process.

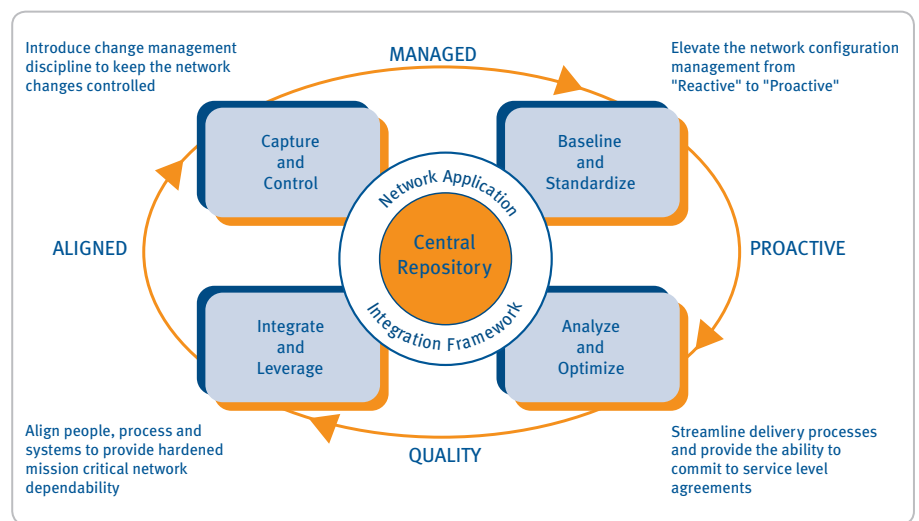


Figure 1: A four-phased approach to establishing a best-practice change control process.

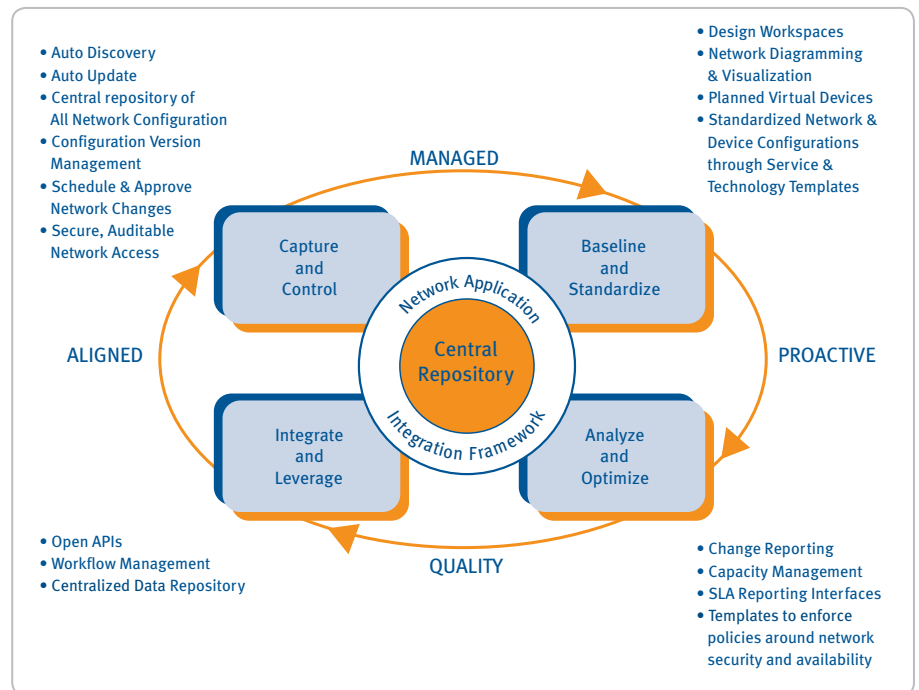
## Automating the Process with EMC VoyenceControl

EMC VoyenceControl masters the complexities of large, distributed, multi-vendor networks by managing network planning, design, deployment, and change. This solution provides a comprehensive, historical, and versioned record of all network device configuration data, which provides customers with an adaptable and reliable approach that will accommodate their ever-changing network environments.

VoyenceControl allows network architects, security specialists, design engineers, operations specialists, and technicians to collaboratively define, control, and optimize every phase of the network resource lifecycle. It delivers the flexibility and functionality required by the most complex network environments.

Figure 2 maps the features provided by VoyenceControl in the context of the phased approach to establishing the process.

Figure 2. VoyenceControl automates the process.



## Integrating VoyenceControl into a Network Management Ecosystem

Undisciplined network operation centers usually use a set of independent, loosely associated, functional components—with minimal data, information, or knowledge sharing through automated interfaces. The operator represents the only means of correlating the information gleaned from various applications. With the increasing complexity of network architectures, protocols and services, network management heuristics are becoming more complex and the decision windows for network operators are shrinking. This leads to absolute chaos whenever a significant network event occurs. In this environment, recovery times range from several minutes to days. Adding new network management applications without a well-considered interoperability framework only adds to the problem.

This situation requires an architectural framework that provides the context for the addition of new systems while ensuring maximum value from the legacy investments. The framework identifies primary functional components, integration points, and a roadmap for acquisition of new components to fully complete the management environment. Judicious vendor choices and close integration of these components will ensure improved network management processes and will significantly reduce operational overhead.

VoyenceControl provides many of the critical functional components in a network operations center. It additionally provides the critical integration capabilities and valuable operational repository that allows a network operations center ecosystem to function cohesively.

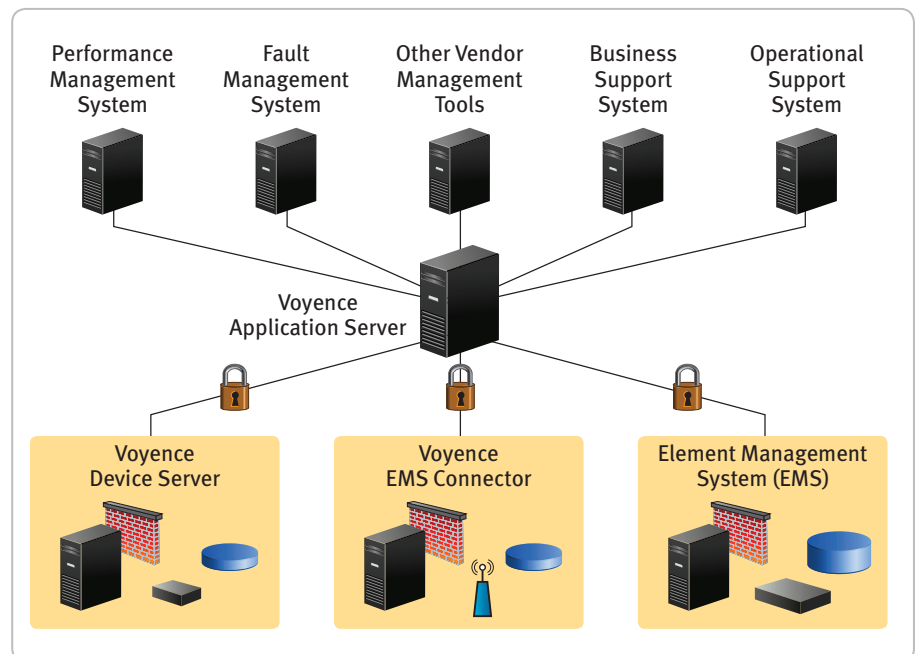


Figure 3. VoyenceControl's distributed architecture delivers efficiency and scalability.

VoyenceControl captures and maintains realtime and historical views of network devices. This information enables IT professionals to determine the source of errors to the exact time and user. It then allows them to roll back or recover the desired network configuration and adjust change processes to reduce the risk of repeating the error in the future.

VoyenceControl also provides the definitive source of network configuration information when investigating a breach in security. This helps to pinpoint the exact cause and preceding events that enabled the breach. With automatic configuration audit tracking, IT professionals have access to more-timely diagnosis and disaster recovery data. With access to realtime and historical views of the network, IT professionals have everything they need to reset the network and make network configuration changes in a more cost-effective, intelligent, and timely manner.

The VoyenceControl Event Framework provides a listener registry and a dispatcher. “Event listeners”—such as the fault management systems, performance management systems, business support systems, and operational support systems shown in Figure 3—use the listener registry to declare interest in events. The dispatcher then collaborates with the listener registry when an event is fired by the core service to determine if there are any “interested” listeners for a particular event. If so, the dispatcher forwards the event to those “interested” listeners. If there are no “interested” listeners, the event is discarded.

The integration framework provides a set of event handlers, event transformers, and event transports. Despite the wide array of events that can be fired and the even wider array of target systems that may be interested in the events, the workflow for dealing with an event is extremely simple:

- Receive event
- Transform event, if necessary, based upon any unique constraints of the target system
- Transport the event (possibly transformed) to the target system using the transport mechanism (e.g., SNMP, CORBA, etc.) sanctioned by the target system

By assembling these integration components, a fully functional network management ecosystem evolves. A benefit to the component approach is that the integration module can be augmented after deployment to listen for additional events or reduce the number of events listened for.

## Conclusion

Although network management solutions play a critical role in automating network operations, configuration management solutions deliver significant additional functionality that make these offerings even more effective.

The benefits of leveraging automated configuration management solutions are far reaching. Automated network configuration management solutions also enable organizations to significantly:

- Maximize return on network investments
- Reduce the total cost of ownership
- Reduce the mean time to repair
- Reduce over-expansion of bandwidth

As challenged as your network environment may seem, there is good news. By following the roadmap outlined in this document, the reliability and performance of your network can improve significantly. Excellent solutions exist to automate the many components in the overall operations fabric. Furthermore, many other sources of best practices are available to help create discipline in your network operations center.



**EMC Corporation**  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America 1-866-464-7381  
[www.EMC.com](http://www.EMC.com)