

Military

EMBEDDED SYSTEMS

VOLUME 4 NUMBER 5
JULY/AUG 2008

Mil Tech Trends: Embedded net-centric warfare

Conquering new military network management challenges



Photo courtesy of the U.S. Air Force by Tech. Sgt. Reynaldo Ramon

Advanced military networks require complex provisioning and can no longer be dependent upon manual administration approaches. Methods such as Command-Line Interfaces (CLIs) and Simple Network Management Protocol (SNMP) exist, but their limitations are somewhat prohibitive. Accordingly, a new approach to the problem has recently become an IETF standard called NETCONF, an XML-based protocol specifically designed to configure the most demanding network situations by providing automated configuration management, improved network security, robust configuration changes, and Policy-Based Network Management (PBNM).



Tail-f Systems
XML-based Network Management

Contacts:

Europe and Asia: +46 8 21 37 40
North America (East): 703-777-1936
North America (West): 510-521-2588
info@tail-f.com
www.tail-f.com

Communications networks play an increasingly vital role in modern warfare and defense systems. Emerging network-centric operational doctrines seek to convert an information advantage into a competitive operational advantage through networking and information sharing among dispersed forces. Programs such as the U.S. Navy's Cooperative Engagement Capability (CEC), the U.S. Army's Future Combat Systems (FCS), and the U.S. Department of Defense's Transformation Satellite Communications System (TSAT) are moving to an increasingly network-centric warfare model.

This emerging paradigm creates significant challenges from a network management perspective. Military networks are larger, more diverse, and more central to mission success than ever before. Rapid force deployments and changing operations drive constant network configuration changes.

In this environment, configuration errors can easily cause network outages, and system downtime risks lives. The software that monitors, configures, and controls these networks must be designed for high performance, continuous service, ironclad security, and fast, error-free

Approach	Configuration Challenges
Manual Configuration	Prone to human error Labor intensive, not scalable No transaction and rollback management
CLI Scripting	Maintaining scripts time consuming Device changes risk scripting errors No transaction and rollback management
SNMP	Best for monitoring Security issues No transaction and rollback management

Table 1

adaptation to the rapidly shifting needs of the modern mission. This is best accomplished with a standards-based architecture that provides strong security features, robust operations, and proper architectural support for rapid, error-free, automated configuration.

Current approaches such as Command-Line Interfaces and SNMP – which rely on manual configuration of individual devices or on large libraries of proprietary scripts – will fail to meet the requirements of future forces. However, the NETCONF standard, an XML-based protocol, is specifically designed to support automated configuration management and provide improved network security, robust configuration changes, and policy-based network management. These capabilities make it an

elegant and efficient solution to next-generation military network management challenges.

Limitations of current approaches

As mentioned previously, different approaches exist for managing network devices, including CLI and SNMP, but each has its own limitations (see Table 1).

Traditional CLI approach

The traditional approach to managing network devices has been to use manual configuration interfaces, such as CLIs. However, using unique management interfaces for each networking device can result in a lack of consistency between devices as well as a lack of integration with other applications. Further, configuring individual devices by hand, even aided by a central management console, is not a scalable approach due to low productivity levels and the likelihood of human error.

One approach to automating network management activity is to develop CLI scripts for the devices in the network, send textual commands to each individual device, and analyze its textual output. Fresh scripts are written and tested as new equipment is added. The library of scripts comes to implicitly embody all knowledge of the network. Maintaining the scripts becomes an ongoing challenge and another opportunity to introduce human error.

To interface *ad hoc* scripts to consolidated management servers, such as Network Management Systems or Operations Support

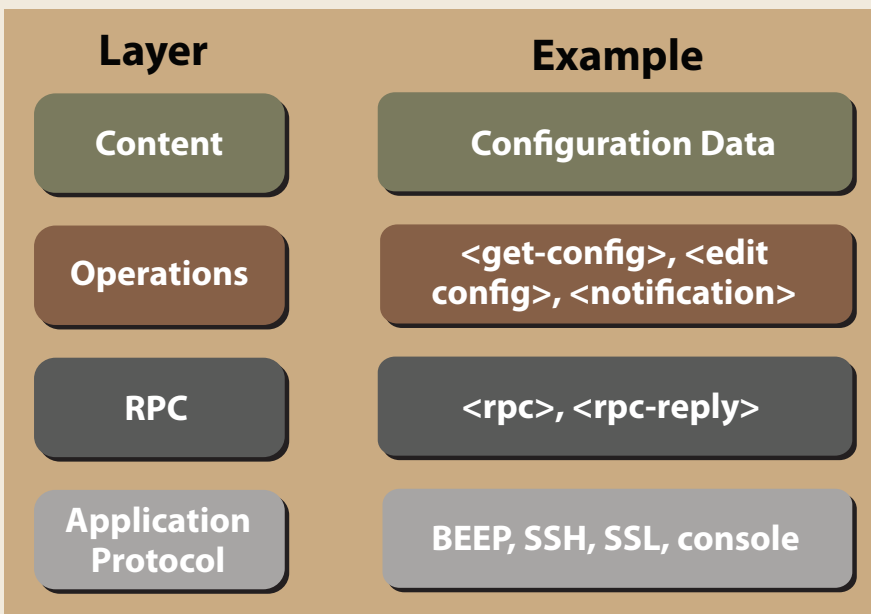


Figure 1

Systems, requires a “mediation layer” of adaptations. This is expensive to develop and maintain. In addition, multi-box transactions are rendered difficult by the lack of a standardized scripting model for equipment from multiple vendors and the absence of locking and other semantics needed to ensure consistency and correctness of changes across the network. A preferable method is to formalize the network architecture and network elements into a complete and cohesive data model that is used by both the management system and system administrators.

SNMP poorly suited to configuration management

While SNMP is well established and works well for monitoring network devices, it is not a good solution for configuration management. First, SNMP operates over User Datagram Protocol (UDP), an unreliable datagram protocol. Second, SNMP uses a protocol-specific security mechanism rather than a standard method, increasing administrator workload and complicating network architecture. Third, because UDP limits the maximum message size, large configurations cannot be sent in a single datagram. Finally, although some vendors provide proprietary mechanisms, SNMP lacks a standard method to allow the network to revert automatically to a working configuration in the event of a configuration error. For these reasons, SNMP is rarely used in practice for writing configurations.

IETF and automated configuration management

The IETF has acknowledged the need for an improved standard for automated network configuration. Therefore, in December 2006 an XML-based protocol called *NETCONF* was finalized (RFCs 4741-4744). Equipment vendors and network operators are taking advantage of NETCONF to facilitate scalable deployments of networks without the risks of disruptive configuration errors. Figure 1 shows the structure and layers of the NETCONF protocol.

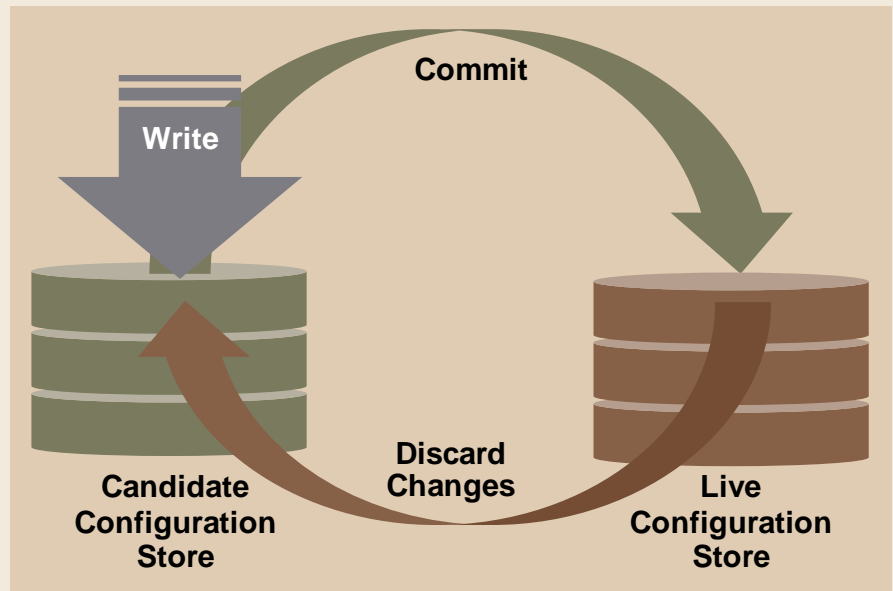


Figure 2

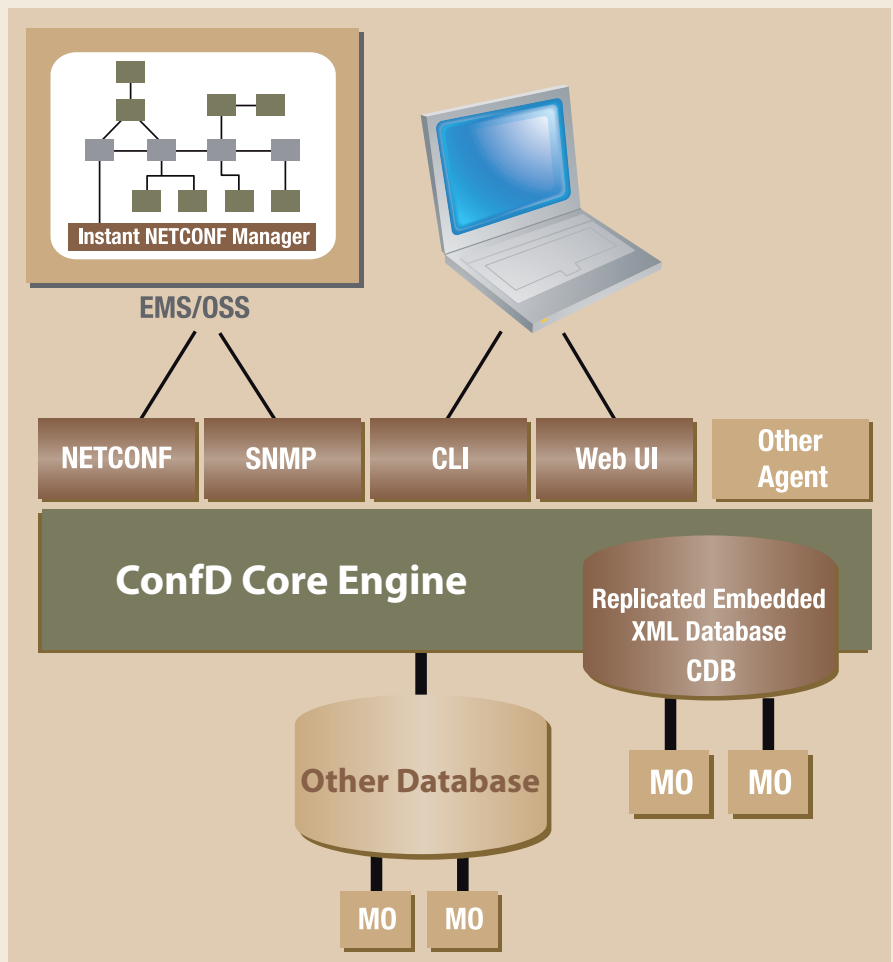


Figure 3

NETCONF offers a number of compelling features that lend themselves well to the particular requirement of next-generation military networks for a management solution that is secure, robust, facilitates a high degree of automation, and is standards-based and commercially supported.

Improved network security

NETCONF is a Remote Procedure Call (RPC)-based protocol that uses XML encoding for protocol messages and configuration data exchanged between managers and agents. XML requests and responses are sent over Secure Shell (SSH), a persistent, secure, authenticated transport protocol. Encryption ensures that the requests and responses are confidential and tamper-proof. In addition to a secure communication system, NETCONF requires devices to track client identities and enforce permissions associated with identities. This means that devices can be managed over an untrusted wide area network, a distinct advantage compared to other approaches. Configuration over a WAN has the further advantage that network management can be centralized through consolidation of all management to a single site, but also decentralized as multiple sites can share device management work.

Robust configuration changes

NETCONF increases the robustness of dynamic networks by providing built-in safeguards to ensure that configuration changes are made in a valid and consistent manner across all network devices. As

depicted in Figure 2, a configuration change will be initially written as a candidate and will only be enacted or committed if no errors occur. After a configured interval, devices automatically revert to their original configuration, unless the change has been confirmed by a second, confirming commit. Administrators can use this capability to test configurations that might potentially degrade or disable connectivity. If such an error occurs, the confirming commit does not reach the misconfigured devices and, after a timeout, the network automatically reverts to the original working configuration.

Policy-Based Network Management

NETCONF's strength in transaction management also lends itself to Policy-Based Network Management, an approach that promises to push the science of network administration to even greater levels of automation and efficiency in reacting to dynamic network conditions, but tends to trigger frequent configuration changes and complex multi-step transactions. For example, NETCONF provides protocol mechanisms for locking configurations and manipulating configurations in bulk. By locking and working on multiple devices

simultaneously, a management system built on NETCONF can implement network-wide policies as logical management operations.

Tail-f Systems provides XML-based network management software for enterprise-class and carrier-grade networking equipment and plays an active role in the IETF Working Group on NETCONF. Tail-f's ConfD software (see Figure 3) enables equipment suppliers to rapidly implement key management interfaces including CLI, Web UI, SNMP, and NETCONF with a robust infrastructure to meet rigorous requirements for high availability and security. ConfD implements the same transaction model used by the NETCONF standard for automated configuration management across all management interfaces.

Making the connection

Military networks are larger and more complex than ever before and are becoming increasingly mission-critical under the emerging doctrine of network-centric operations. Enter NETCONF, which supports automated configuration management and provides improved network security, robust configuration changes, and Policy-Based Network Management to help conquer the challenge. †



Carl Moberg is vice president of engineering at Tail-f Systems. Prior to joining Tail-f, he was the cofounder and director of product management at ServiceFactory. Before joining ServiceFactory, he worked at Telia, where he was one of the principal architects of the company's Internet service platform. He can be reached at carl.moberg@tail-f.com.

Tail-f Systems • +46-8-21-37-40 • www.tail-f.com