FLEXTRONICS®
Software Systems

FCAPS

White Paper

FLEXTRONICS®
Software Systems

FLEXTRONICS®
Software Systems

1. Overview

For the convenience of standardizing management, network management activities are subdivided into different functional areas. The network management functional areas are

1. Fault management
2. Configuration management
3. Accounting management
4. Performance management
5. Security management

Today, most network management systems address FCAPS (FCAPS is an acronym of these functional areas). It also provides an indication of the measurement of the capability of network management systems. This white paper describes FCAPS in general and the Future Software framework for FCAPS, applicable for any network equipment.

2. Introduction

Since early 1980s computer networks began to grow and more mission-critical applications are being built on the network infrastructure. It becomes increasingly important to keep the network downtime to a minimum because it results in lost opportunities, revenues and productivity. In this environment, scalable, high-performance network management has become a critical differentiator for network service providers.

Network management systems employ a variety of tools, applications, and devices to assist network managers in monitoring and maintaining networks. The most commonly used framework is centered around "**FCAPS**" model, standardized by ISO. Though ITU-T initially defined the FCAPS specifications for telecom networks, the same concepts can be applied to data networks.

The basic idea behind FCAPS is very simple – it categorizes the plethora of information handled by a management system into five key functional areas: **F**ault Management, **C**onfiguration Management, **A**ccounting Management, **P**erformance Management and **S**ecurity Management. FCAPS is an acronym of these functional areas.

The paper is organized as follows: Overview of FCAPS functionalities, Future Software Framework for FCAPS, ACE, Use of Future Software Framework, and Planned Enhancements.

3. Overview of FCAPS Functionalities

The following table (from the International Engineering Consortium WebPro Forum Tutorial) lists the management features supported by each of the components in FCAPS.

FM	CM	AM	PM	SM
Fault detection	Resource Initialization	Track service/ resource usage	Utilization and error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault Isolation	Auto and Sub rack Discovery	Accounting limit	Performance Data collection	Access logs
Network recovery	Back up and restore Database handling	Combine costs for multiple resources	Performance Report generation	Security Alarm/Event Reporting
Alarm handling	Resource Shut down	Set quotas for usage.	Performance Data analysis	Data privacy
Alarm Filtering	Change Management	Audits	Problem Reporting	User access rights checking
Alarm Generation	Support for pre-provisioning	Toll fraud reporting	Capacity planning	Take care of security breaches and attempts

Clear Correlation	Inventory/ Asset Management	Support for different modes of accounting	Performance data/statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining and examining historical logs	Security related information distribution
Error logging	Remote configuration			
Error Handling	Initiation of jobs and tracking their execution			
Error statistics	Support for automated software installation and information distribution			

3.1 Fault Management (FM) Module

Faults manifest themselves as either persistent or transient events. However, certain types of errors (such as dropped packets and erroneous frames in a LAN) are typical even in a well-functioning network. These types of errors and transient events have to be logged and do not require any correction whereas persistent faults require correction. Some types of persistent faults can be corrected automatically at the network equipment level without the intervention of administrator whereas some types of faults can be corrected only at the administrator level. Any fault management entity at the network equipment level should have at least some support for detection of persistent faults and automatic correction of faults.

This support could be as simple as responding to requests, from managers, for attributes of managed objects at periodic intervals (i.e., polling). For advanced systems, this could be generating messages on its own after detecting faults on a resource (event notification) and performing polling on behalf of manager (indirect polling). For managing a large number of network equipment, the fault management strategies that rely on event notifications and indirect polling are considered most efficient - as it minimizes network traffic and processing load on the manager.

Generally occurrence of one fault can lead to occurrence of one or more related faults. In this case, the occurrence of the fault that is the root cause should be reported while suppressing the reporting of all other related faults. To support this feature, the relation between the faults is generally maintained as a uni-directional tree (with no cyclical dependencies). This tree is referred to as *dependency tree* in this document. Once a fault occurs, all the child faults of this fault in the dependency tree are masked so that no fault is reported for the child faults. Any fault management strategy should have support for this feature in order to avoid overwhelming the manager with reports of all related faults.

3.2 Configuration Management (CM) Module

Configuration management is used to locate the resources, including the failed ones, and also to keep track of the types of resources and their details. The managed objects can be stored in directories. The data on managed objects is collected on a regular basis and where there are changes, can be collected in the manager, using unsolicited messages such as traps. CM standardizes activation and deactivation of the managed objects in a controlled manner and updation of configuration information. It provides support services (software management) to keep the system and the resources operational. Change management, which is a part of CM, keeps track of changes in computer networks and the resources associated with them.

3.3 Accounting Management (AM) Module

Accounting management involves tracking service usage and informing relevant users and authorities about the usage of resources and the costs associated with their usage. When computing resources are scarce, it may be necessary to set limits on the usage of the resources. Automatic corrective actions should be taken on exceeding thresholds. Costs on resource usage may sometimes need to be combined and consolidated.

3.4 Performance Management (PM) Module

PM comprises of gathering network statistics, evaluating system performance under both normal and degraded conditions and altering system mode of operation. Any performance management entity at the network equipment level should have support for data collection. This support could be based on direct polling or indirect polling. In advanced systems, there can be support for monitoring critical parameters and raising faults on parameter values exceeding configured threshold levels.

3.5 Security Management (SM) Module

Security management system should minimize unauthorized or accidental access to network control functions. Security management function deals with ensuring legitimate use, maintaining confidentiality, data integrity and auditability. It should provide access control for association, operation and notifications (security alarms). Based on the access rights, it should enable/disable functionalities of network elements. It should continuously monitor the system for any security breaches and should automatically take corrective action like denying access to some portions of network or usage of functionalities.

3.6 FCAPS Framework

There are many network management systems available in market today, which provide these functionalities targeting a particular type of network device and platform. There is a requirement for a generalized framework solution providing a set of common/default management functionalities in a vendor, device and platform independent manner. This framework solution has an easy plug in and plug out facilities for interfacing with the management applications on one side and with the device on the other side. There are number of advantages based on a generalized approach which is covered in the next section.

4. Framework Advantages

Reusability and Reliability

A framework provides reusability both in terms of code and design. The Framework implements a set of core functionalities that can be used for managing variety of devices from multiple vendors, multiple domains and supporting multiple technologies. Vendors can use the framework for managing any type of network element and need not develop applications from scratch. Greater reliability is achieved as the common base is reused.

Easy of use and thin client

The vendor's programming effort is minimized and simplified to a great extent. The vendor has to write just a few lines of code in the management application, to provide (graphical) user interface based on the specific needs. The framework is already written, debugged and tested.

Cost Effective

The vendor does not have to manage its network solely at the level of hardware devices. A Framework provides them the ability to manage at much higher levels of abstraction, minimizing the development time.

Generic Management and Flexibility

A generic framework providing core functionalities provides the ability to vendor to manage most of the parts of their networks in as generic a manner as possible. This also provides flexibility by allowing specific customizations to be done by vendors wherever applicable.

Object Oriented Approach

With a framework based on an Object Oriented approach, advantages are modularity, ability to model generalized/specialized hierarchies and modularity. Modularity provides increased ability for abstraction and reliability.

Increased portability

The framework components make it easy to write concurrent networked applications on one OS platform and quickly port them to many other OS platforms. The cost of porting is less than the cost of redevelopment on the new environment. Framework and applications exhibit uniform behaviors irrespective of the underlying platform.

Scalability

The framework is highly scalable. This means irrespective of the load (number of elements being monitoring) on the system, the response reliability from the system is the same.

As the framework components are designed using the above features there is an increase in software quality, efficiency and predictability.

5. Future Software Framework for FCAPS

Future Software has developed a FCAPS framework that can be used for managing any networking equipment i.e., managed element. Current version of the framework supports Fault and Performance Management components. The implementation uses ACE (Adaptive Communication Environment) wrapper classes.

References

1. 1. Network Management System Essentials by Diwakara K Udupa McGraw-Hill Series on Computer Communications
2. International Engineering Consortium WebPro Forum Tutorial
3. ADAPTIVE Communication Environment (ACE) Website. http://www.cs.wustl.edu/~schmidt/ACE.html

Abbreviations and Acronyms

ACE	Adaptive Communication Environment
FCAPS	Fault, Configuration, Accounting, Performance, Security
ISO	International Standards Organization
OS	Operating System

FLEXTRONICS®
Software Systems

For More Information

FutureSoft, an ISO 9001:2000 certified, SEI-CMM-Level 5 company, is a leading provider of communications software solutions, protocol stacks and services to the global communications industry in areas like IP Switching/Routing, Broadband Access, Wireless and Wireline applications. The company also offers a range of embedded software solutions and services that span across multiple domains including automotive, process control, mobile handheld and building automation. The company has wholly owned subsidiaries in US, UK and Taiwan for addressing the North American, European and Asian markets.

For more information, contact us at:

Flextronics Software Systems Ltd.,
Plot 31, Electronic City, Sector 18,
Gurgaon – 122015, Haryana (INDIA)
Tel: +91-124-2346666/2455555,
Fax: +91-124-2455100/2455101
E-mail: info@flextronicssoftware.com
Visit us at: http://www.flextronicssoftware.com