# Cisco Advanced Services Network Management Systems Architectural Leading Practice

## Contents



## Introduction

### Preface

This document is intended to provide the reader with a high-level guide to help establish a network management architecture that can be implemented as one the goals toward providing a world-class network and support infrastructure.

The document will detail the Advanced Services network management proposed strategy and how it relates to the ISO and IT Information Library (ITIL) management models.

Cisco® uses both the functional fault, configuration, accounting, performance, and security (FCAPS) model as defined by the ITU standards and the ITIL framework to assess network

management areas. ITIL references and terminology are used in this document. Specifically, this document incorporates several of the ITIL service management concepts. This document contains strategies regarding incident and problem management as they relate to the ITIL framework..

This document should help you focus on requirements based on the documented network management philosophy and an existing understanding of your network management objectives. It is a document intended to generate discussion between you and your team as to the most appropriate network management architecture for your company.

A viable network management solution must provide reliable, scalable support and effective visibility into your infrastructure. This document provides strategies and recommendations on the architecture and design for the network management systems that should support your business goals and objectives.

The completed product of the process started by this document should then act as the architecture guidelines for future network management system (NMS) tool selection, thus helping to ensure that independent implementations will not result in system incompatibilities and that critical network management integration will occur.

### Intent

This document outlines a proposed high-level strategy of the key areas of network management architectures. The intent is to jointly review each section and create a final strategy that meets all listed requirements and supports your company's business goals. Once an area has been finalized through a joint review process, an associated set of lower-level documents may be created by your company's various stakeholders that will provide detailed designs and implementation plans as required.

## Network Management Goals and Requirements

### Operational Goals

The functional requirements for the architecture outlined in this document are intended to allow your company to achieve the following operations goals:

- Proactive monitoring of network infrastructure and service levels
- Streamline network operations functions through NMS tools optimization
- Scalability of NMS architecture to support new network technologies such as Multiprotocol Label Switching (MPLS), wireless, quality of service (QoS), and others
- Increase the ability to detect soft failures at the protocol, hardware, system software, and interface levels
- Help enable proactive maintenance to be performed by the network operations center (NOC) support team upon detecting faults or performance degradation
- Help enable intelligent forwarding of network events to the NOC

### Functional Requirements

Given the high-level manageability goals outlined above, the following sections highlight the functional requirements in specific network management functional areas.

Fault Management

Fault management encompasses the discipline of identifying faults in a network environment. Faults are identified by receiving events such as syslog and Simple Network Management Protocol

(SNMP) traps from network devices, polling network device MIBs, and identifying real or potential error conditions and setting thresholds that trigger events. In addition, the NMS should be able to provide event correlation as well as reporting and tracking. The NMS used should also provide a northbound interface for exporting critical messages to a higher level manager or MoM (manager of managers).

In an ideal environment, the fault manager would collect both syslog and SNMP information, filter that information, and pass the filtered data to a MoM for further processing. This method helps decrease the amount of data that an end user needs to see or react upon. The MoM, in turn, can provide further analysis and automation based on the incoming event streams such as verifying down circuits, testing connectivity, and opening trouble tickets based on those findings.

### Unmanaged Events

Stand-alone fault managers are used to gather event data from devices throughout the network and report their findings. They have little to no capability of automating reactions based on gathered data. When a message comes into the fault manager, the typical course of action is simply to report the fault to a screen being monitored by operations personnel.

### Managed Events

By employing the use of a MoM, your system can react to these events automatically, which can drastically reduce downtime in mission-critical networks. For example, when an event comes in from the fault manager, the MoM can:

- Verify connectivity to the reported down device/interface by ping/Telnet or other means
- Gather information about the device such as vendor, serial number, location, contact information, circuit IDs, site IDs, and so on from a device inventory database
- Attach historical reports gathered from other NMSs such as bandwidth, CPU, memory, and so on
- Open a trouble ticket automatically and have that ticket prepopulated with important information from the device information database

This method would not only relieve operations personnel from having to look up the information for an outage, but would save critical time in bringing the fault to a resolution.

### Event Correlation

Event management encompasses event-correlation and root-cause analysis. It allows for multiple input streams from various network devices and environments and, using knowledge of the network topology and a sophisticated rule set, attempts to identify the source or root cause of a network fault or problem.

- At the top level (MoM), event correlation features should be supported to aggregate and correlate incoming alarms. The system needs to have the intelligence to correlate event types (SNMP, syslog, and so on) as well as to provide automation of tasks based on event criteria.
- Filtering capability should be supported to selectively display relevant alarms.
- The system should be capable of escalating critical alarms based on the number of occurrences and time delays in acknowledgement.
- Alarm severity should be customizable based on end-user or operational needs.
- Alarm properties and escalation should be policy based, dependent on the role of the

device in the network.

- The system should be able to virtually partition the managed network into multiple logical entities based on geographical locations.
- The fault management system should support role-based access to fault events based on job responsibilities.
- A knowledge base consisting of troubleshooting guidelines or methodologies should be part of the fault management system. This is to facilitate rapid problem isolation on network-related issues.
- The system should provide integration between the fault and the inventory management system to support autopopulation of information.
- Integrate between the inventory system and the trouble-ticketing system for autopopulation of relevant trouble ticket fields.
- The system should provide the flexibility to forward traps and alarms to a different location/system for after-hours monitoring.

Log Management (Syslog)

Logging is a critical part of network management. Good logs can help you find configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of your network. Cisco devices have the ability to log a great deal of their status.

Syslog is also a great resource for network compliance, allowing companies to adapt quickly to changing regulations such as Sarbanes Oxley (SOX), Control Objectives for Information and related Technology (COBIT), IT Infrastructure Library (ITIL), Gramm-Leach-Bliley Financial Modernization Act (GLBA), Visa Card Holder Information Security Program (Visa CISP), Payment Card Industry (PCI) Data Security Standards, Health Insurance Portability and Accountability Act (HIPAA), Committee of Sponsoring Organizations (COSO) of the Treadway Commission, and custom regulations.

Defining all aspects of a syslog server is outside the scope of this document.

NMS North and Southbound API Interfaces

Communication between multiple network management systems is extremely important for event correlation and data aggregation. Most, if not all, NMSs should be able to communicate bidirectionally. This helps ensure the ability to provide correlated events as well as the coordination of data sources throughout the network such as inventory, access, performance data, and so on.

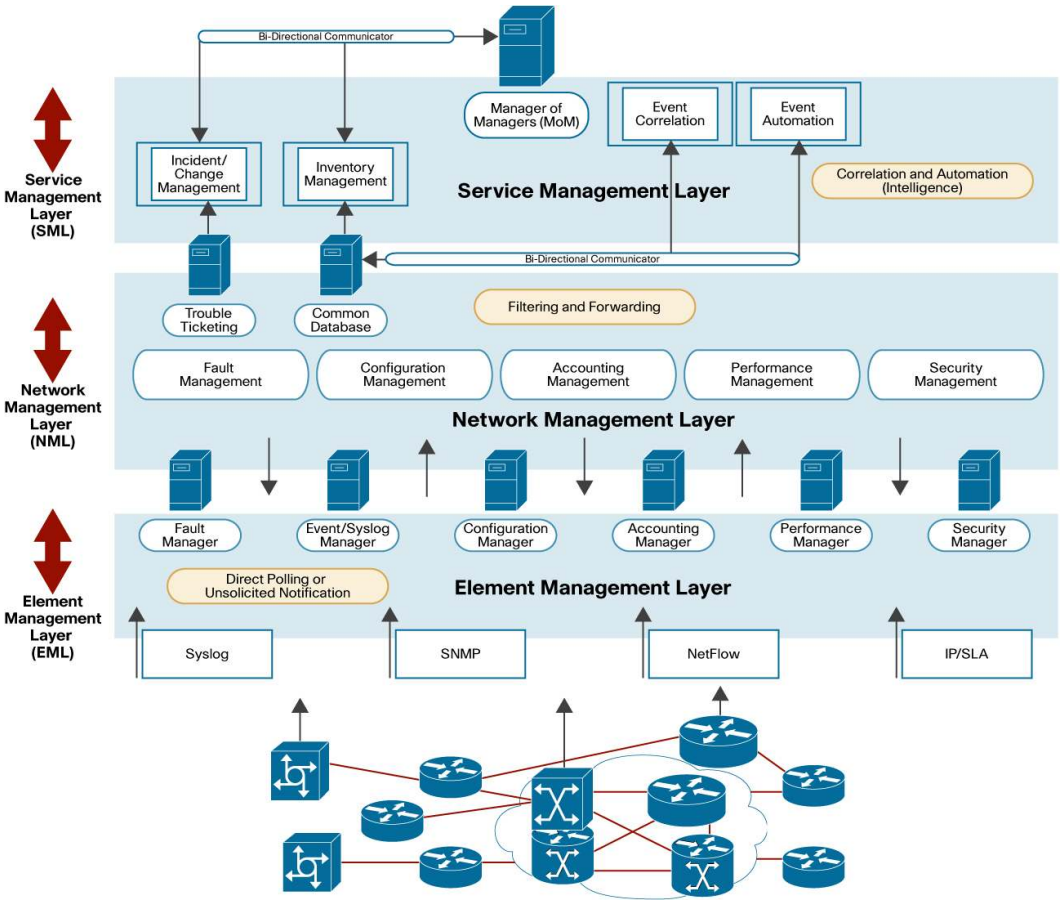
## Network Management Architectural Model

### Hierarchical Approach to Network Management

Layering of network management not only allows NMS systems to communicate better, it reduces the amount of alerts seen by network operations support staff. At the lowest layer, it is nearly impossible to keep up with events displayed from each network element reported in the NMS architecture. For example, it is not feasible to have someone watching every syslog event that occurs on the network. Instead, you rely on systems at the Network Management Layer (NML) to filter through all events and show only those events deemed as most important. The Service Management Layer (SML), meanwhile, is used to further summarize events from the NML and tie multiple network management systems together. A good NMS system will also provide deduplication of these network events in order to further reduce the amount of unnecessary messages seen by operations personnel.

The hierarchical model in Figure 1 shows the major components that make up a comprehensive NMS system and provides a high-level integration scenario. Cisco Advanced Services encourages the adoption of a layered, hierarchical network management system. This type of architecture involves data flow and integration of multiple NMS tools to be effective. Figure 1 depicts those tool and data relationships.

**Figure 1.** Hierarchical Model Overview




The underlying hierarchical philosophy is to get the organization to a basic level of integrated network management. The foundation for this architecture comes from the Telecommunications Management Network (TMN) (M.3000) model. “TMN provides a framework for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks. To achieve this, TMN defines a set of interface points for elements which perform the actual communications processing (such as a call processing switch) to be accessed by elements, such as management workstations, to monitor and control them. The standard interface allows elements from different manufacturers to be incorporated into a network under a single management control.” (http://en.wikipedia.org/wiki/Telecommunications_Management_Network).

### Element Management Layer

The first level, the Element Management Layer, defines individual network elements used in deployment. In defining this layer, for each anomaly that occurs in the network, potentially multiple devices can be affected by the event and can independently alert network management systems that an event has occurred resulting in multiple instances of the same problem.

Network Management Layer

In the middle of the diagram is the Network Management Layer. This function takes input from multiple elements (which in reality might be different applications), correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that has occurred. The NML provides a level of abstraction above the Element Management Layer in that operations personnel are not “weeding” through potentially hundreds of Unreachable or Node Down alerts but instead are focusing on the actual event such as, "an area-border router has failed."

Service Management Layer

At the top of the diagram is the Service Management Layer. This layer is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems. The goal is to move traditional network management environments and the operations personnel from element management (managing individual alerts) to network management (managing network events) to service management (managing identified problems).

Benefits of Hierarchical Layers

From a practical perspective, integrating these elements involves:

- Assembling a robust set of event correlation rules that consistently and accurately identify the source of an event
- Opening a trouble ticket in an incident management application that operational personnel begin working on

This helps enable an operations organization to:

- Proactively manage the network
- Identify and correct potential network issues before they become problems
- Prevent a loss of network connectivity, thus ensuring organizational productivity
- Focus on the solution instead of the problem

## Reducing Downtime (MTTR)

### Silos

Most of the tools deployed in traditional NMS environments act as “silos” meaning they are not aware of any other tools available within the environment. Some of the issues resulting from this design include seeing multiple alarms for single events, looking too many places for event information and creating a disconnect of information between network events and support personnel resulting in lost information and Mean Time to Repair (MTTR).

### Manager of Managers

A MoM is instrumental in providing the intelligent network management services at the top layer of this hierarchical model. Among other things, MoMs are used to provide a final filter between the network operations personnel and events seen on the network. The MoM can correlate events to other sources of information (such as inventory, performance, contacts, and so on) and provide automation for operational tasks that can greatly decrease MTTR.

### Automation

Automations should be implemented for common events and tasks. These automations should be triggered by the MoM and are designed to reduce MTTR.

For example, when an event comes in, most operations personnel are trained to perform certain tasks before ever actually working on the event. These tasks may include verification of the outage (by manually pinging, and so on), looking up contact information (who owns that device), deciding how important the device is according to when the event happened (3 a.m. on Sunday, nonessential device, versus 1 p.m. on Monday, and so on).

All of these procedures can be automated so that when an event comes in, operations personnel are presented with final results of gathered information instead of the simple event. Tables 1 and 2 show a simplified example of such an event stream. Note that this is merely an example; there are many other items that can be prepopulated to event lists.

**AUTOMATION EXAMPLE**

**Table 1.** Event Automation: Simple Event

| Device IP | Device Name | Time Stamp | Event Information |
|---|---|---|---|
| **1.1.1.1** | router-1 | 04/25/2006 00:01:00 | Interface down |
| **2.2.2.2** | router-2 | 04/25/2006 00:01:00 | SYS-5 configuration change |

**Table 2.** Event Automation: Enhanced Event

| Device IP | Device Name | Time Stamp | Circuit ID | Customer | SLA | Event Information |
|---|---|---|---|---|---|---|
| **1.1.1.1** | router-1 | 04/25/2006 00:01:00 | Sprint: 1002983 | RTP | Site closed from 8 p.m. to 6 a.m. | Interface down |
| **2.2.2.2** | router-2 | 04/25/2006 00:01:00 | AT&T: 33884 | FLC | 24 hour | SYS-5 configuration change |

### Inventory Management

Network inventory management is an essential component of robust network management architectures. Tools that provide planning, design, and lifecycle management for network assets should be the primary focus of any well-managed network. Network inventory systems should be implemented that provide actionable information that administrators can use to improve network management performance and help develop effective network asset control processes.

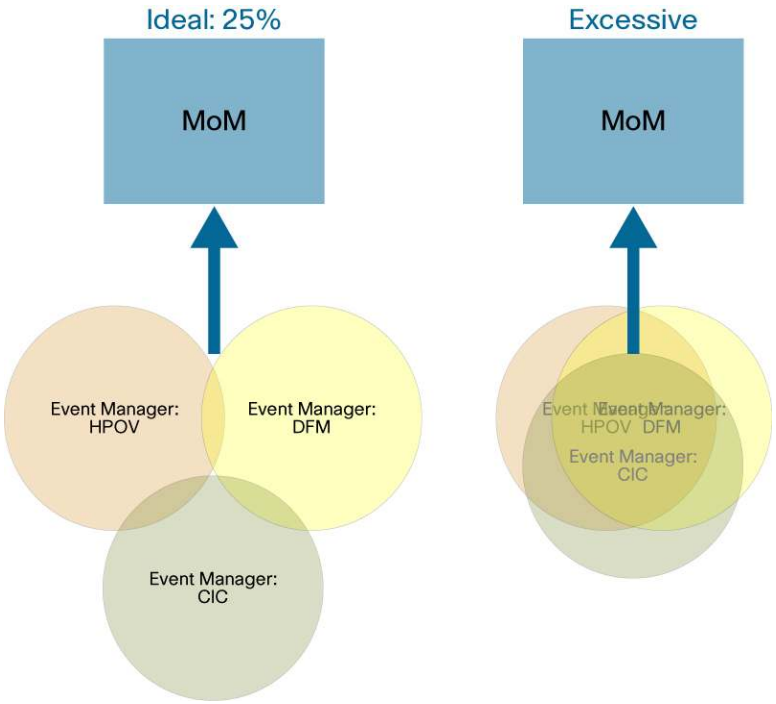
Providing an inventory management strategy is outside the scope of this document, but an effort should be made to create a process that provides strategies and recommendations on the architecture and design for the flow of information within the NMS architecture.

### Overlapping Managers

Systems that provide some redundancy are useful for verifying event data, but care should be taken to ensure that these systems aren't completely duplicating efforts and doubling the amount of system administration needed (Figure 2).

Overlapping managers should be used to validate that an event has indeed occurred. Once verified, a single, filtered event should then be forwarded to the MoM for further processing.

**Figure 2.** NMS Architecture Gaps




## NMS Operational Dependencies

This section details network management leading practices that apply to the majority of the area strategies provided in the previous sections.

### Auditing

It is extremely important that a process be put in place that provides a monthly (or more often) procedure for auditing all NMS systems. These audits should verify, at a minimum:

- Device inventory
- SNMP passwords
- Reachability

### Remediation

A process needs to be developed to provide remediation of events. The tools being implemented are successfully reporting errors, but the errors continue to occur. An immediate effort should be made to resolve the problems being reported.

### NMS Collection Stations

The location of collection systems relative to the managed network devices can impact the efficiency and effectiveness of the network management environment. Active network monitoring systems should be located as close to the managed devices as possible to minimize the impact due to loss of connectivity to a higher NMS layer as well as to reduce unnecessary network traffic.

### Hardware Redundancy

Redundancy of network management systems should be considered at various levels. Systems can fail due to power supply problems, CPU problems, or hard drive failures. In such an event,

another system should be available to quickly take over, at least, fault management functions.

**System Backup**

When a system fails, it is possible that the operating system or software configuration data will be lost. Implementation of a system backup strategy for network management systems should be implemented to minimize the recovery time in the event of a storage failure.

**Uninterruptible Power Supply**

Most network management systems utilize sophisticated operating systems and database management systems that can be seriously corrupted if a sudden power loss is encountered. To prevent against such data corruption, a UPS (uninterruptible power supply) system should be employed where network management systems are installed.

**SNMP Community Strings**

A standardized set of read-only and read-write community strings must be agreed upon and configured accordingly across the network. Disparate community string configuration can often lead to mismanaged devices, false alarms, and unauthorized access. SNMP access control lists (ACLs) should be applied throughout the network to mitigate unauthorized access. Read-write communities should be locked down to specific servers while read-only communities should be open to the NMS subnet and authorized stations only. In addition to ACL deployment, it is recommended that each device be configured to log any failed attempts.

**SNMP Polling Standards**

A set of polling standards needs to be created for fault management and performance management that define how network devices are polled, by which applications, and at what intervals. This will eliminate unnecessary traffic on the network and conserve device resources. Adherence to polling standards should be part of any periodic audit process. ACLs can be used to limit polling access only to authorized applications and networks.

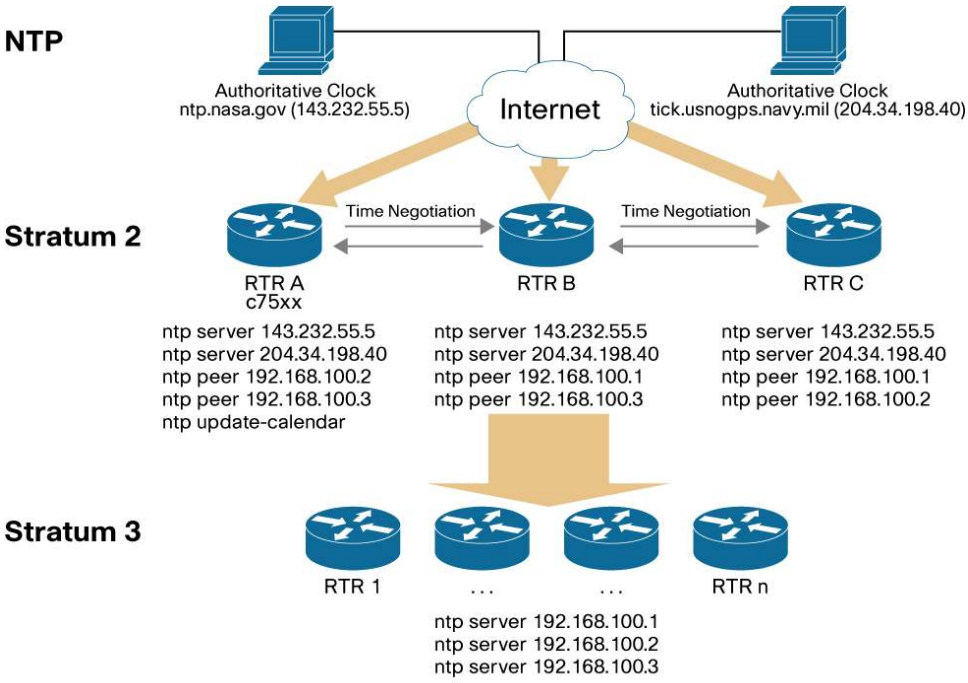
**NTP**

All systems will also need to process the messages from elements that are multihomed and determine which interfaces (and subnets) are causing the error messages and their effect on the whole network. One issue that the management platform must address is the differences in the manner in which timestamps are attached to messages by different network elements. The management system will need to recognize which method the elements are using and adjust appropriately. To alleviate some of the timing issues, the Network Time Protocol (NTP, RFC 1305) should be used in the network. Any tools that are considered should be interoperable with the NTP standard (Figure 3).

Recommendations:

- Use a minimum of two reference clocks (GPS and Internet derived are popular) - three are recommended.
- Set up “peer” time between the reference clocks.
- Subnets of multiple NMSs or routers and switches may consider using NTP in multicast mode.

**Figure 3.** NTP Hierarchical Model




### DNS

Network devices should, at a minimum, put loopback addresses, switch sc0 interface or alternate management interface address in the Domain Name System (DNS) servers. It is also recommended to set the local device hostname to match DNS node names.

### Telnet/SSH

Wherever possible, all devices should be configured to utilize Secure Shell (SSH) Protocol as the sole vty access method. A network audit should be conducted periodically to ensure SSH access compliance.

## Glossary of Terms

Table 3 contains a list of terms used throughout this paper.

**Table 3.** Glossary of Terms

| Term | Definition |
|---|---|
| **CERT®** | A registered service mark of Carnegie Mellon University commonly used to refer to the CERT® Coordination Center, a major reporting center for Internet security problems |
| **CORBA** | Common Object Request Broker Architecture |
| **FCAPS** | Fault, configuration, accounting, performance, and security (FCAPS) functions of the Open Systems Interconnection (OSI) management model |
| **ICMP** | Internet Control Message Protocol |
| **ISDN** | Integrated Services Digital Network |
| **ISO** | International Organization for Standardization |
| **ITU** | International Telecommunication Union |
| **LAN** | Local area network |
| **MIB** | Management information base |
| **MTBF** | Mean time between failure |
| **MTTR** | Mean Time to Repair |
| **NOC** | Network operations center |
| **OSI** | Open Systems Interconnection |
| **OSS** | Operational support system |
| **ORA** | Operational readiness assessment |
| **PTN** | Private telecommunication network |
| **SLA** | Service-level agreement |
| **SNMP** | Simple Network Management Protocol |
| **SP-ANS** | (Cisco) Service Provider Advanced Network Services |
| **STP** | Spanning Tree Protocol |
| **TMN** | Telecommunications Management Network |
| **VLAN** | Virtual local area network (LAN) |
| **WAN** | Wide area network |
| **XML** | Extensible Markup Language |
| **vty** | (virtual teletype) A command-line interface (CLI) created in a device for a Telnet/SSH session. The device is able to generate a vty dynamically. |

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA C07-400447-00 09/07