Network Management Reference Architecture

Abstract

Information and Communication Technologies (ICT) organizations and the network departments are struggling with the increased complexity of ICT and especially networking technologies. In addition ICT executives and management are challenged by their businesses to show increasing value in their services while decreasing the costs.

This requires ICT organizations to increase innovation and productivity while decreasing operational expenditure and all the time maintaining customer and client satisfaction with service delivery and service levels. This challenge requires a paradigm shift, looking at new ways of finding operational efficiencies and increasing ICT relevance and value to the business.

This paper discusses an architectural approach to network operations, defining a Network Management Reference Architecture (NMRA), which can be used by network executives and managers to ensure that they are addressing how people, processes, and technology are being combined to operate the network effectively, reducing operational expenditure and increasing business value.

An organization's operational posture can be directly related to their operational sophistication. Most companies struggle with taking network operations from a reactive to a proactive paradigm. The level of sophistication can be improved by moving beyond day-to-day reactive needs and looking at network operations holistically.

This means taking a higher-level view of the network lifecycle encompassing preparation, planning, design, implementation, operations, and optimization –ensuring that the entire lifecycle addresses people, processes, and technology and how they are combined to deliver agile network services. The goal is to increase the network's responsiveness to business needs and maximize the business investment in the network infrastructure and resources, while ensuring that the network scales and that services are provided accurately and reliably.

Process and technology are important but equally important are functional capabilities. It is the capabilities that make it possible for people and processes to operate efficiently. This white paper includes a self-assessment at the end to help organizations identify the level of their functional capabilities, any weaknesses, and consequently where they should focus efforts for improvement. The questions represent the requirements of the functional capabilities.

Contents

Introduction

Cisco® developed the Network Management Reference Architecture (NMRA) by consolidating existing industry frameworks and standards into an architectural resource to assist customers in understanding and addressing their operational needs.

Operational Posture

The operational posture of an organization can be determined by evaluating how operations are currently performed and comparing them to the leading practices as defined by various industry frameworks and standards, such as Information Technology Infrastructure Library (ITIL) [1], Control Objectives for Information and related Technology (COBIT) [2], and the Enhanced Telecom Operations Map (eTOM) [3]. These will assist in determining where your organization is today.

Typically, operations are reactively effective in reactive situations: when a business-impacting incident is identified it is resolved quickly and this provides a false sense of maturity. This shows that people are efficient in reacting to incidents, but may not be effective in avoiding incidents.

When adopting a proactive posture the number of incidents should decrease and those incidents that do occur are managed more consistently via well-defined processes and methodologies. The most effective form of proactive management is well-implemented change and configuration management given that a large percentage of incidents arise from poorly implemented changes and lack of change and configuration visibility.

Ultimately the goal of a proactive posture is to reduce or even avoid business impact altogether by reducing the number of incidents and the time to restore services to meet or exceed service level agreements.

Operational Sophistication

While the reactive needs of the organization's business are important and must be met, development of proactive operational capabilities is arguably more important. This requires developing experience and maturity in the operational systems and this sophistication can be achieved through an architectural approach.

The NMRA has been developed by Cisco to assist customers in addressing operational needs. The NMRA identifies the following three operational components:

- People
- Process
- Technology

The outcome of the NMRA is a holistic look at these operational components and how they interact and interrelate.

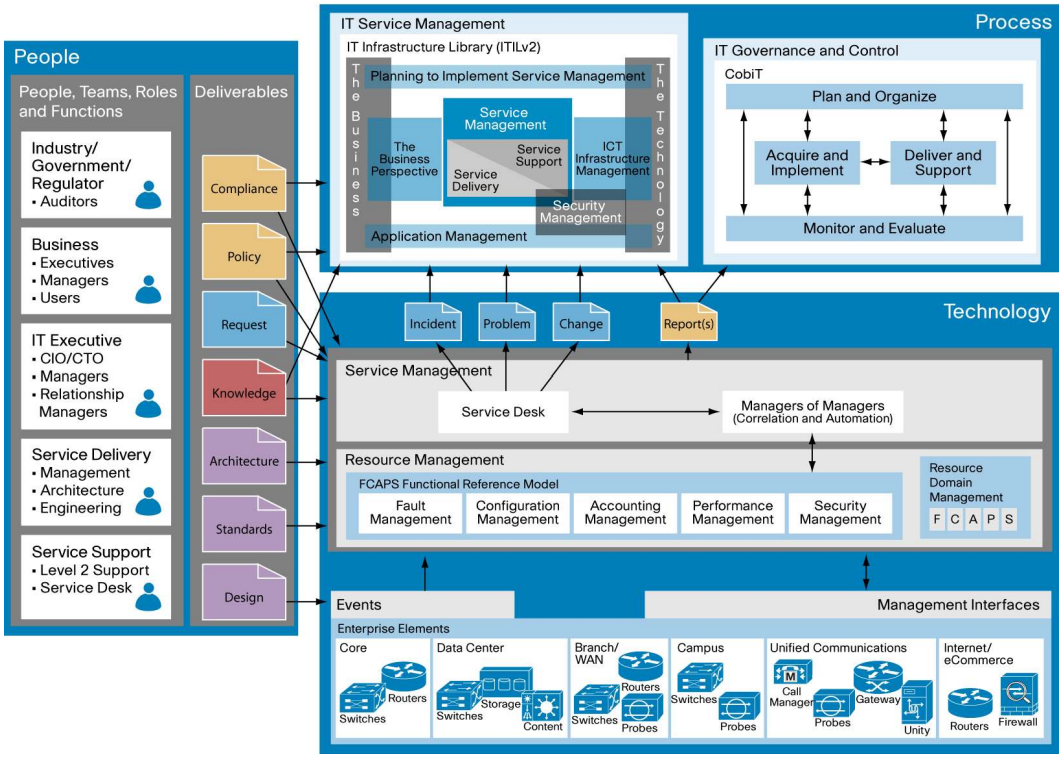
Trying to deploy systems that only address one of the operational components is not going to achieve the anticipated results or return on investment. Many companies have repeatedly tried to deploy operational technologies in the form of tools, and while there may be some initial benefit, a long-term return is not realized.

The same can be said of focusing efforts on process development; if processes do not include tooling considerations and address specifically how, who, and when people will use the processes,

the result is often subject to poor adoption or compliance outcomes. Another common result is that staff becomes dissatisfied as they feel disempowered by the process.

The NMRA (Figure 1) can benefit organizations looking for a way to become more operationally sophisticated. It provides a basis for addressing all three of the operational components and combining these components to build cohesive systems that support network operations and the business services that rely on high levels of network performance and availability.

Figure 1. Satellite View Network Management Reference Architecture



Architectural Best Practices for Network Management

The following best practices are important to the successful development and deployment of a network management architecture.

1. Always consider people, processes, and technology before investing in any network management features and capabilities.
2. Deploy new features and capabilities inside the architectural framework; if the architecture constrains requirements, and then revise the architecture.
3. Where possible integrate network management software to share data and prevent information duplication.
4. Implement a Manager of Managers to assist with integration and facilitate business impact management.
5. Research and develop processes and technologies that will extend network management features and capabilities and provide opportunities for increasing business value.
6. Foster a proactive culture to facilitate a responsive organization that can anticipate business needs.

7. Implement network management tools that provide functional capabilities and enhance strategic capabilities.

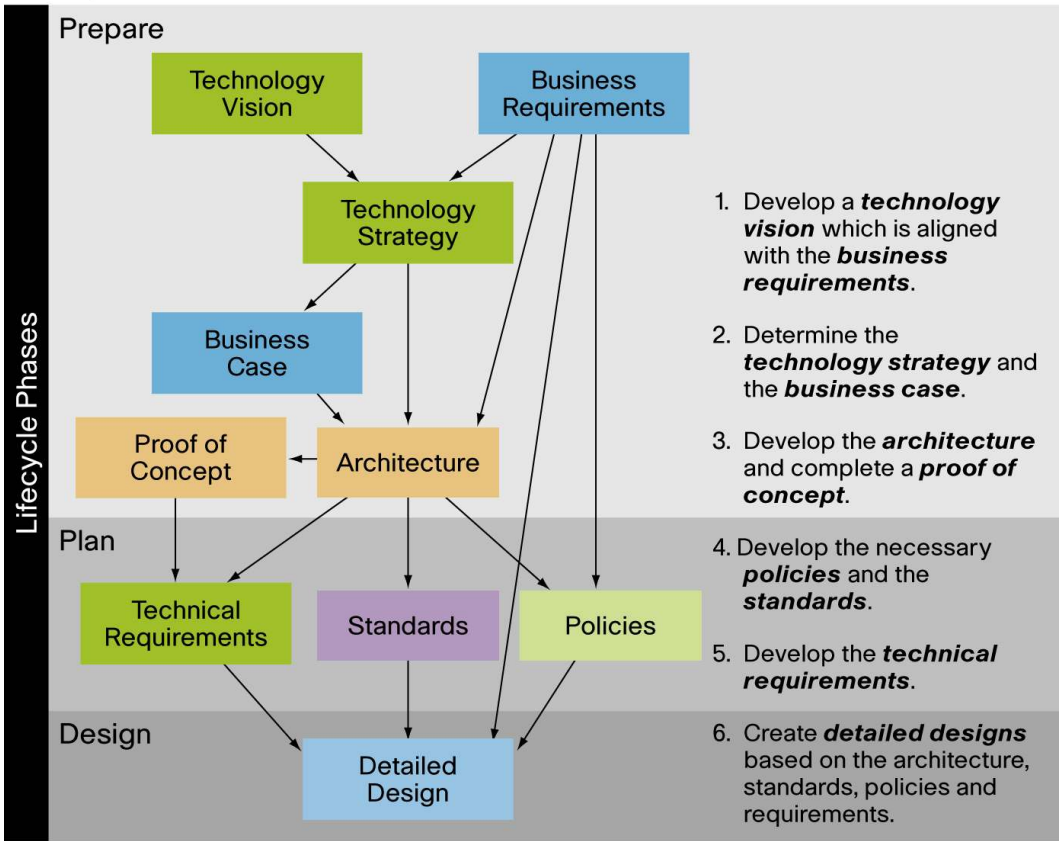
Strategic Architecture Process

While architecture is important, it must be placed into context with the business's needs and must follow a vision and strategy for the overall organization, the ICT division, and the core function of operating and managing the network.

The Strategic Architecture Process helps to differentiate between vision, strategy, and architecture, the confusion between these causes a lot of problems with high-value communications in the hierarchy of the ICT organization.

Figure 2 provides a context for the architecture, and suggests a process for the development of business-aligned strategic management architecture. This is also shown with the Network Lifecycle [6] phases, to provide a mapping to the overall development and lifecycle of the system.

Figure 2. Strategic Architecture Process



It is important to recognize that the strategy is about implementing the vision. A vision that does not address business needs is not viable; there has to be alignment between the vision and the business needs.

Strategic Capability Development

To meet the business expectation of increasing value while maintaining or reducing the cost base, the ICT organization should strategically develop capabilities in the following four areas:

1. Architecture
2. Process
3. Technology
4. Responsiveness

These capabilities underlie all service and network management efforts that an organization should make and are fundamental and foundational to continuous improvement. These capabilities should be developed by the ICT organization by combining people, processes, and technology to meet the business's needs.

Ultimately these capabilities improve the ICT organization's operational efficiencies, providing a direct benefit and increasing the business's satisfaction with services.

Architecture

This is a strategic initiative to improve overall efficiency and effectiveness, overall cohesion in the way the ICT organization operates by showing how people, processes, and technology are integrated into delivering service value.

Process

Process is based on the architecture and improves the consistency and reliability of overall service management.

Technology

It is important to ensure that the necessary operational technologies and tools are in place, and that the right tools are available for the right processes and people.

Responsiveness

Ensure that the ICT organization is able to meet the businesses needs reactively, and provide service management inside an operational framework that ensures that overall both proactive and reactive needs are met. Responsiveness is about communication and meeting or managing customer expectations.

Increasing Network Services Business Value

There are two distinct tracks to business value in relation to developing an architecture that encompasses service management and operations: first, a value case for the strategic capabilities that benefit the business and second, a business case for how the architecture will benefit the ICT organization and ultimately the company's profit line.

To support these tracks, several service management capabilities have been identified which will benefit the business, and also a brief business case has been identified for the ICT organization to invest in an operational architecture. The architecture will become the platform to improve service management value to the business.

Measuring Value

The ultimate value from effective network service management will be received by the business. The business will perceive value from a service they are satisfied with. Satisfaction requires consistency in service management and awareness of the business needs and the potential impact the operations have on the business.

Value in service management can be defined by four attributes:

1. Capable
2. Reliable
3. Accurate
4. Responsive

These attributes create consistency in service management and provide the business with determinism in how they can use the services being provided and managed. The value that this creates with the business is very high and is perceived through customer satisfaction and can be measured by monitoring and soliciting customer satisfaction feedback.

However, failure to deliver services with all of these attributes will create a feeling of disappointment with the customer which will ultimately reduce customer satisfaction.

Capable

The services being offered must have the features that people need, and must measure up to similar services. The service-delivery resources need to be people who have the necessary skills to deliver and support the services.

Reliable

The service needs to be reliable, being available when required and within the agreed service levels.

Accurate

The service needs to be accurate, so that the service can be trusted by its customers. Accuracy in this context could also be termed quality. The service needs to be of a quality that reflects the agreed service levels and the expectation of the customer, and this should be managed through the service level and customer relationship management.

Responsive

The service management needs to be responsive to customer requests and needs, within the agreed service levels. It is important that the service also be proactive, anticipating the customer's needs; simply reacting to customer needs will meet expectations but not exceed them. Being proactive by anticipating needs creates satisfaction.

Value Proposition

While the ICT organization will receive direct business benefit from development and implementation of an operational architecture, the internal capabilities will enhance the service management considerably and will benefit the overall business. The capabilities discussed previously are believed to benefit the business directly through:

- Improved business agility, increasing the business's competitive advantage and ability to respond to business-impacting issues.
- Increased operational efficiencies, reducing time to resolve and improving customer perceptions.
- Improved risk management, ensuring that operational risks are managed according to their likely impact and potential cost.
- Improved relationship and trust between the business and the ICT organization.

In simple terms, most of the business case for the ICT organization focuses on improved productivity and for the business it is about improving business agility – getting better service levels for the same or a reduced cost.

Improve Business Agility

Improving business agility will help the business to accommodate rapid growth, whether through mergers and acquisitions, or in response to unplanned business opportunities.

The business will derive a more direct benefit from service management capabilities, as these will provide increased visibility and awareness of the network and its impact on the business, and assist with improved business continuity.

For the ICT organization, service management provides an improved understanding of impact on the business and the ability to better prioritize resource and effort. Through improved technology management, the ICT organization will be able to improve the speed by which services are added or changed, providing the business direct benefits.

Increase Operational Efficiencies

Operational efficiencies can be broken into implementation (projects) and operations. By increasing efficiency through improved process and automation, a better job can be done with same number of people, or less people.

In the area of operations, for the business this means faster resolution of requests and incidents, ultimately reducing impact of the business. For the ICT organization this means an improved time to resolve, and improved ability to meet service levels.

In implementation, this means improved delivery of projects and this translates to faster business response for new business ventures, assisting with business agility.

Improve Risk Management

Businesses operate by understanding the key factors that can impact the profit line, and this includes risks. ICT organizations assist the business through understanding the risks that can impact the infrastructure and systems and ultimately the business and ensuring that they are mitigated where appropriate.

Effective risk management helps ensure business continuity and enables ICT organizations to establish important trust and credibility with the business.

Improve Relationship with Business

Business relationships are built on trust, communication, and consistency. In many companies today, ICT organizations face obstacles in building trust with the business groups, primarily due to increased complexity in the ICT infrastructure and unplanned outages that impact the business.

It is vital that business relationships are managed through consistent communication. This communication needs to be timely and accurate. Over time this type of open communication builds trust and results in improved relationships all around.

Operational Components

People

When the Network Management Reference Architecture was developed, the first consideration was to determine who the stakeholders are in an organization. These are the functional roles with an interest in how the network is performing as a business support system.

The high-level architecture identifies the stakeholders and addresses how these functional roles interact with the people, processes, and technology that comprise the operational system. Ultimately it is the stakeholders and users of the network, not the network team, who determine if the network performance and availability are suitable to support the business.

In many organizations there are five main groups of stakeholders in the network; these are:

1. Industry/government/regulator
2. Business leadership/end user
3. IT executive
4. Service delivery
5. Service support

The first three groups are concerned with the definition of requirements and policies to support business objectives while the latter two groups are focused on the instantiation of those requirements and policies as network and operational systems.

Stakeholder Requirements

Table 1. Stakeholder Requirements

Stakeholder Group	Requirements
Industry/government/ regulator	• Ability to audit compliance to relevant regulations that are generally targeted at consumer protection, national security, or fiscal stability. For example, in the U.S., Sarbanes-Oxley (SOX) [7] and Health Insurance Portability and Accountability Act (HIPAA) [8] are applicable.
Business	• Risk-management data • Visibility into network operations activities that could impact business operations • Reporting on delivery of network service components and availability to ensure network clients have timely access to appropriate business intelligence or services • Capacity reporting for network service components impacting business operations
IT executive	• Reporting on operational state of network infrastructure • Summary reporting for various aspects of network service delivery • Status reporting on network for business locations • Network capacity summaries
Service delivery	• Visibility into device, network, and service operation and performance • Tools for analyzing network usage and determination of future impact of business growth • Reporting on proactive issues that may impact network in the future • Tools for reporting on compliance to relevant regulations
Service support	• Incidents for problems impacting service delivery • Views of network status • Tools for incident and problem determination • Proactive reporting on issues that may impact network and services in the future

Stakeholder Responsibilities

In addition to their requirements, each of the stakeholder groups has responsibilities in the operation of the network.

Table 2. Stakeholder Responsibilities

Stakeholder Group	Requirements
Industry/government	• Define regulatory compliance
Business	• Define service requirements from business • Define policy
IT executive	• Define service requirements from IT • Define policy
Service delivery	• Network architecture • Network standards • Network designs • Meeting business requirements • Technical policy
Service support	• Support policy • Network operations • Network optimization

Process

Process ties together people and technology. Without good process interaction, the technology components are just tools and the ability of the people component of the system to produce deterministic outcomes is undermined.

It is important to acknowledge that network management needs to align with the overall IT organization when it comes to processes. This is especially true if the IT organization has undertaken a service-management approach.

At this level, the architecture defines the key deliverables for which people are responsible. These deliverables are foundational to the operational system defined by the NMRA. They must be addressed and linked into the process and technology components to bring the architecture together.

The deliverables at this level are:

- Compliance
- Policy
- Requirements
- Architecture
- Standards
- Designs
- Knowledge

Later sections of this document will provide more detail around the processes and define the tasks which people are responsible for working on in support of and in addition to these high-level deliverables.

Deliverables are also used as inputs for other teams. For example, several of the stakeholder groups define requirements and policies that are deliverables used as inputs for service delivery, and the architect role generates several deliverables including architecture and standards, which are inputs to designs.

Deliverables-Based Process

Defining deliverables as output from people who are engaged in the delivery of ICT services, creates lines of demarcation as well as measurable, visible milestones for the various phases of the lifecycle and operational activities.

Compliance

Many organizations, in particular those with public responsibilities like financial institutions, healthcare organizations, and publicly listed companies will have requirements from external regulators for compliance. Many organizations are looking at IT Governance as a means to provide the necessary framework for compliance.

Formal compliance will be defined by regulators based on government- or industry-adopted standards. An organization's ability to meet compliance requirements is measured through audits.

Policy

The way to translate many specific business and management requirements is to define policies. All ICT systems should have a set of defining policies which govern how decisions will be made by people, processes, and any involved technology, especially in the case of automated systems.

These policies translate high-level needs into implementation in the systems. Systems built around policies also provide improved flexibility and business agility, being more easily adapted as requirements change over time. Policies provide an alternative to the typical hard coding of decision points on which many systems rely. The network architecture will also define various policies necessary to meet the requirements.

Requirements

Systems need to be built to meet needs of the stakeholders; these needs are expressed through requirements. The primary stakeholders of ICT system are usually the people responsible for the core function of the organization.

These business requirements need to be acknowledged when building the systems; additional requirements may be defined by managers and executives of the ICT systems.

Gathering requirements is important to ICT, and it is frequently challenging to get input from the business. The role of business relationship managers assists in streamlining this part of the process.

Architecture

Cisco defines many reference architectures, and the existing network may already be based on these architectural principles. The network architecture has to be documented, if it hasn't already been. The network architecture should be hierarchical and structured; this creates points where new infrastructure connects, whether it is a new building, floor, or remote office.

Then the network architecture should be communicated with the ICT organization and with business stakeholders. Part of network architecture is about normalizing and generalizing; this creates patterns and building blocks in the network that can be more easily scaled.

The network architecture should define the necessary technical requirements of the system, the standards to be developed and used, and any applicable polices.

Standards and Designs

Many network teams will design every deployment or project; this is an engineering way of approaching things. What is required is a paradigm shift in network engineering to allow the network teams to spend more time on network architecture, standards, and designs.

From the building blocks defined in the network architecture, standards can be developed. These standards include products, configurations, and designs. The standard designs improve the ability to quickly meet business requirements and reduce the total cost of ownership through consistent deployments, in much the same way as desktop teams have an a standard operating environment (SOE).

Standardizing products is part of this, as well as defining a set of network solutions that the network team offers to the business. This could be considered the “Service Catalogue” from ITIL.

Initially, work is required to document and build out the network architecture and these standards. In time, this reduces the load on network resources by providing pre-built “wheels” that can be used.

Knowledge

The capture and reuse of knowledge is key to scalability and productivity in network design, operations, and management. Without effective capture and reuse of knowledge, leverage is not possible by the different parties involved in requirement gathering, architecture development, and network design and implementation.

This creates the void of information currently experienced by operations groups today. Knowledge may be in the form of documents, diagrams, requirements, test results; it may also be small fragments of “informal” information, as captured in blogs and wikis on the Internet.

A knowledge management system should provide a way to capture and consolidate all this information and make it available for all parties involved in the network.

Service Management

IT service management is currently a focus for many ICT organizations. Frameworks such as ITIL and COBIT can help an organization to develop the necessary processes for operations.

As shown in the high-level architecture, ITIL is made up of two main functions and each function has five processes. These functions are linked together through the service desk application.

COBIT defines four domains for the best practices for IT management. These domains address all aspects of IT management for the network through its lifecycle. COBIT provides a set of metrics and best practices to assist in maximizing return on investment from IT as well as providing governance and control.

The four domains in COBIT are:

1. Plan and organize
2. Acquire and implement
3. Deliver and support
4. Monitor and evaluate

These domains also encompass a lifecycle for services, and the networks on which the services are based.

IT Governance and Control

More specific to the wider IT organization, it is beneficial to consider some of these concepts as they relate to network management. The IT Service Capability Maturity Model (IT Service CMM) [9] defines five levels that encompass an organization's processes:

1. Level 1: Initial
2. Level 2: Repeatable
3. Level 3: Defined
4. Level 4: Managed
5. Level 5: Optimizing

These levels show how processes evolve from reactive to proactive. The first step toward improving operational posture is becoming more sophisticated with how operations are performed, which means making process-driven operations.

Technology

An ICT infrastructure can be defined as a set of logical and physical components that interoperate to provide a set of functions that are consumed by the business they support.

This view of the ICT infrastructure underpins the decision within the NMRA to adopt the TM Forum concepts of service and resource management and blend them with the ISO systems management functional areas as the means of visualizing how the different management activities required to support the business effectively should be organized.

In the NMRA, the functions delivered by the ICT infrastructure are referred to as services, while the logical and physical components required to support these functions are referred to as resources. For example network elements, software, and IT systems would all be considered resources. As resources perform different functions they themselves are further classified as belonging to specific technology domains such as application, computing, and networking resources.

Services management within the NMRA encompasses all the activities required to define and operate the instances of services consumed by the business.

These activities include:

- Initial definition and cataloging of services
- Managing of business user requests for services
- Mapping of service requests to the resources required to fulfill the request
- Maintaining an inventory of deployed services
- Monitoring impact of resource behavior on the availability and quality of the services being delivered
- Managing and reporting on the quality of services being delivered
- Monitoring of compliance to corporate security standards and reaction to security threats
- Billing and financial management of services support

Planning to ensure that the set of services being delivered to evolve to meet changing business needs

Domain resource management within the NMRA encompasses all the activities which focus on the direct management of resources related to a particular technology domain.

These activities include:

- Planning and implementation of new resource capability within the domain
- Maintaining an inventory of the resources currently deployed in the domain
- Obtaining, allocating, and configuring resources to support fulfillment of requests for services
- Proactive and reactive monitoring of resource failures to determine root cause and initiate repairs
- Analysis, control, and reporting of the performance of individual resources to ensure that they have sufficient capacity to support the services they deliver
- Sharing of management data with other areas such as service management and resource management
- Monitoring of compliance to corporate security standards and reaction to security threats

The main goal of domain resource management is to hide the complexities of managing a particular technology from the rest of the management architecture in much the same way that a device driver hides hardware complexity from an operating system.

By contrast resource management consolidates information from different resource management domains to provide an end-to-end view of the IT infrastructure. At this level management activities are largely focused on:

- Orchestrating the fulfillment of requests for services that span multiple resource-management domains
- Performing cross-domain root cause analysis on faults from multiple resource-management domains
- Consolidating domain-specific inventory to provide an end-to-end view of the IT infrastructure and a mapping of service instances to supporting resources
- Analyzing and managing performance issues that span multiple resource-management domains
- Monitoring compliance to corporate security standards and reaction to security threats
- Sharing management data with other areas such as Service Management

Functional Management

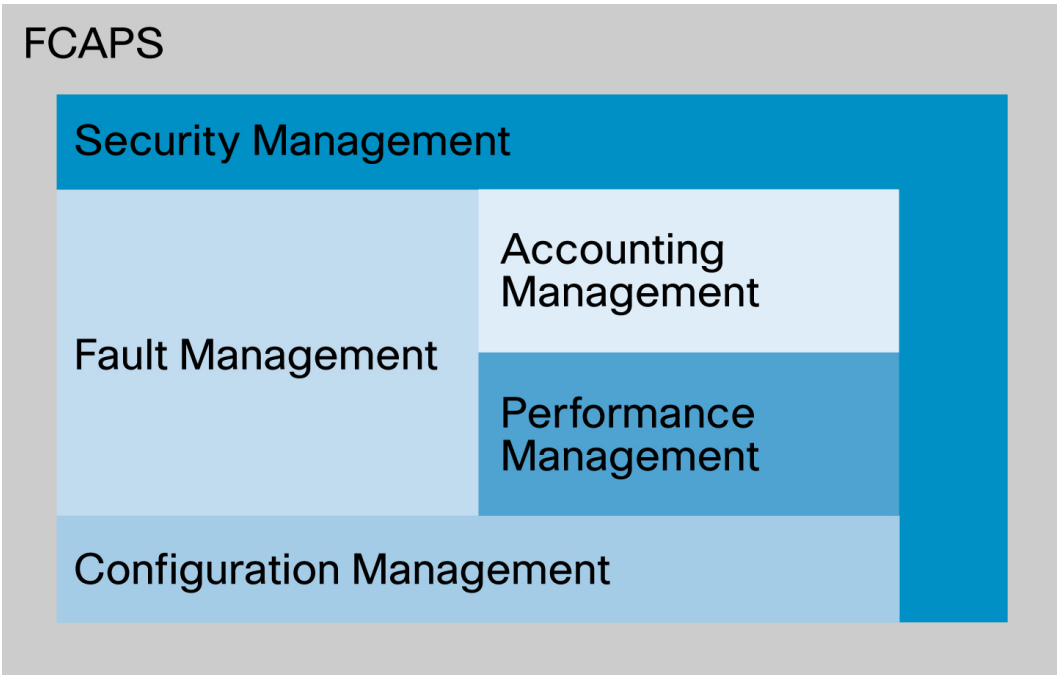
The network management reference architecture uses the functional management model consisting of five functional areas made up of:

- Fault
- Configuration
- Accounting
- Performance
- Security

The NMRA uses this model to provide more functional granularity to the architecture.

This model is often referred to as the FCAPS [5] model and while many people think of each function of FCAPS as being equal, in reality they create a set of foundations and overlays as shown in Figure 3: Interactions of the FCAPS Functions.

Figure 3. Interactions of the FCAPS Functions



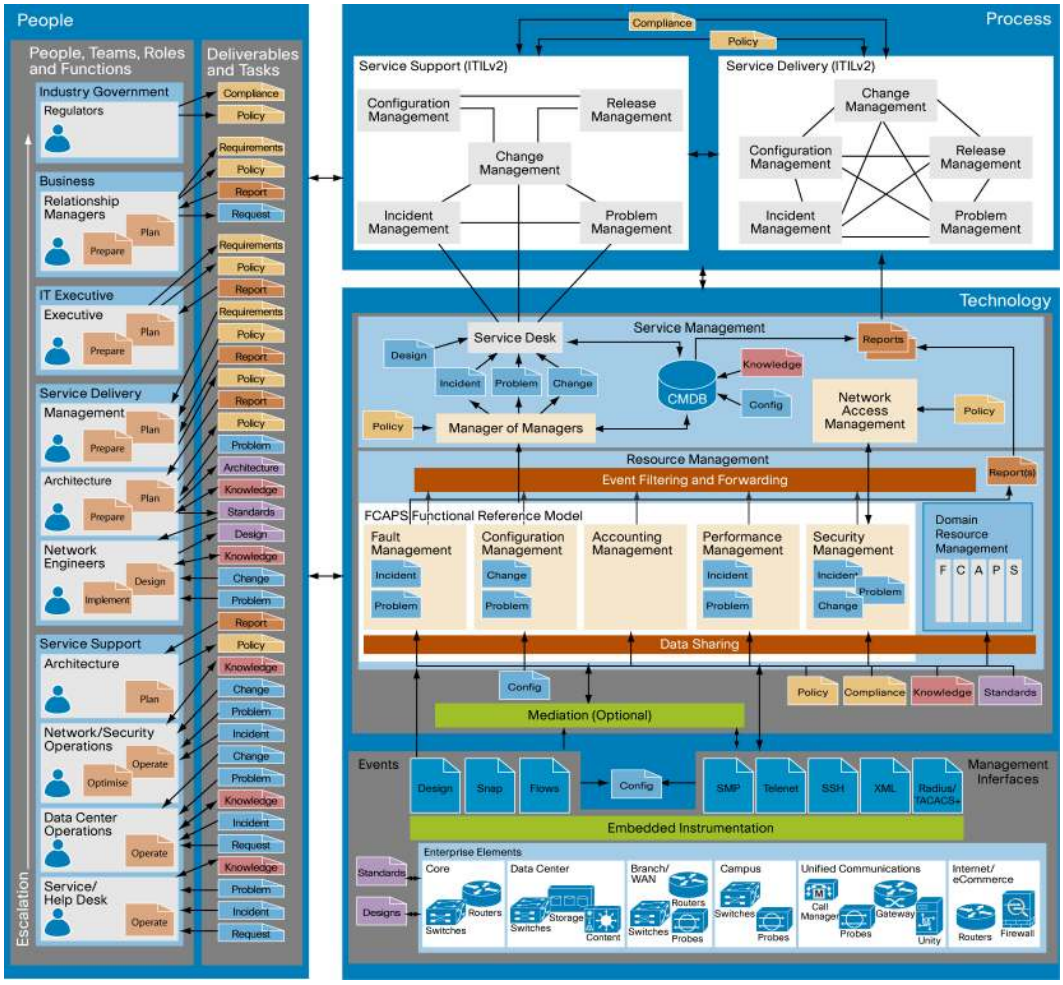
Each of the functions interacts with each of the others. Security has to touch all the functions to be effective, while configuration management provides the essential data that underpins the other functions.

Reference Architecture

The operational components section introduced the high-level aspects of the network management reference architecture; this section will drill into the next level of detail. The NMRA diagram provides additional information that includes the tasks, being the units of work that people carry out on a day-to-day basis.

The reference architecture shows how people, processes, and technology can be combined to build cohesive network operations function. Productivity benefits from automation. Automation comes from implementing a process then applying technology to the process, selecting which steps can be automated.

Figure 4. Network Management Reference Architecture



People

Figure 4 identifies the specific roles within the stakeholder groups and, in addition to the deliverables already defined, the day-to-day tasks that people work on are now defined. The tasks are:

- Request
- Incident
- Problem

- Change

In addition to these tasks, reports are also generated by the systems. These reports are the primary results of collecting and analyzing data and are important inputs for people and processes.

A defined escalation process is vital to ensuring that issues are dealt with appropriately. When necessary, issues are escalated through the organization over time. Communication is key and it is important that escalations happen in conjunction with early notifications to avoid surprises during critical situations.

Ultimately people are responsible for capturing the knowledge relevant to their role. This knowledge is fed into the technology and process components, and is available for other people. Knowledge capture and reuse is a key indicator of operational maturity.

Organizations are feeling the pain of the skills shortage, in particular when key staff leaves, making knowledge capture even more critical. It is also important to ensure that all staff has suitable training, the team structure is working, and that the staffing levels are sufficient to support proactive as well as reactive activities. This can help prevent dependencies on particular people.

Request

A request or service request is a general description of any request made by a user for services; this includes requests for information or advice, a standard change, or access to a service.

Incident

An incident is an unplanned interruption to an IT service or the reduction in the quality of an IT service. It can also be the failure or degradation of an element of the infrastructure, in the case of the network a switch or router, which has not yet affected the service. For example, when a router or switch that is part of a redundant system fails, but the network is still up, this is considered an incident.

Problem

A problem is the unknown root cause of one or more incidents as defined in ITIL. A problem is created when a deeper unknown cause is suspected and requires investigation. Problem management is often referred to as proactive management.

Change

A change or change request is the mechanism used to make changes to the production network. A change is part of change management as defined in ITIL, and the primary purpose of change management is to enable beneficial changes to be made in a controlled way with minimum disruption to services, while ensuring that the changes have been evaluated, prioritized, planned, tested, implemented, and documented.

Network Lifecycle

Because a network is always evolving, in any process it is important to address the cycle of continuous improvement. The NMRA maps the network lifecycle [6] phases to the people, showing which people are responsible for which parts of the lifecycle. Phases in the network lifecycle are:

- Prepare
- Plan
- Design
- Implement
- Operate

- Optimize

The network lifecycle applies to the entire life of the network as well as any smaller projects that extend the network over time. A general definition for a project is anything that requires design. All designs should fit into the overall network architecture or the architecture should be updated as new requirements are identified. Any change to the network not requiring design, including optimization to the production environment, should be considered operational and handled through change management processes.

Process

Process plays a crucial role in the architecture, tying people and technology together and ensuring consistent delivery of network services through service management. The service management framework being used will define the leading practice processes to support the defined tasks.

Currently the NMRA is based on the popular ITIL V2 framework, which works well for Information Technology Service Management (ITSM) and is widely implemented in many organizations worldwide. ITIL V3 was released in June 2007 and builds on ITIL V2; future versions of the NMRA will be based on ITIL V3.

It is important to determine which processes from the framework are relevant to the organization and to focus efforts on those.

Technology

Cisco has done a lot of work on the technology aspects of network management systems, and recently published a white paper that complements this paper, “Network Management Systems Architectural Leading Practice” [4]. Overall the technology component:

- Provides capabilities and functionality to assist in performing tasks
- Shows how the tasks are handled functionally
- Element management handles devices and technology management, specific features needed for different technologies
- Element managers take raw events and network data, and consolidate and correlate and then send these to the Manager of Managers (MoM)

Mediation

An optional mediation layer provides consistent device interfaces for element management. The mediation layer assists in scaling device access.

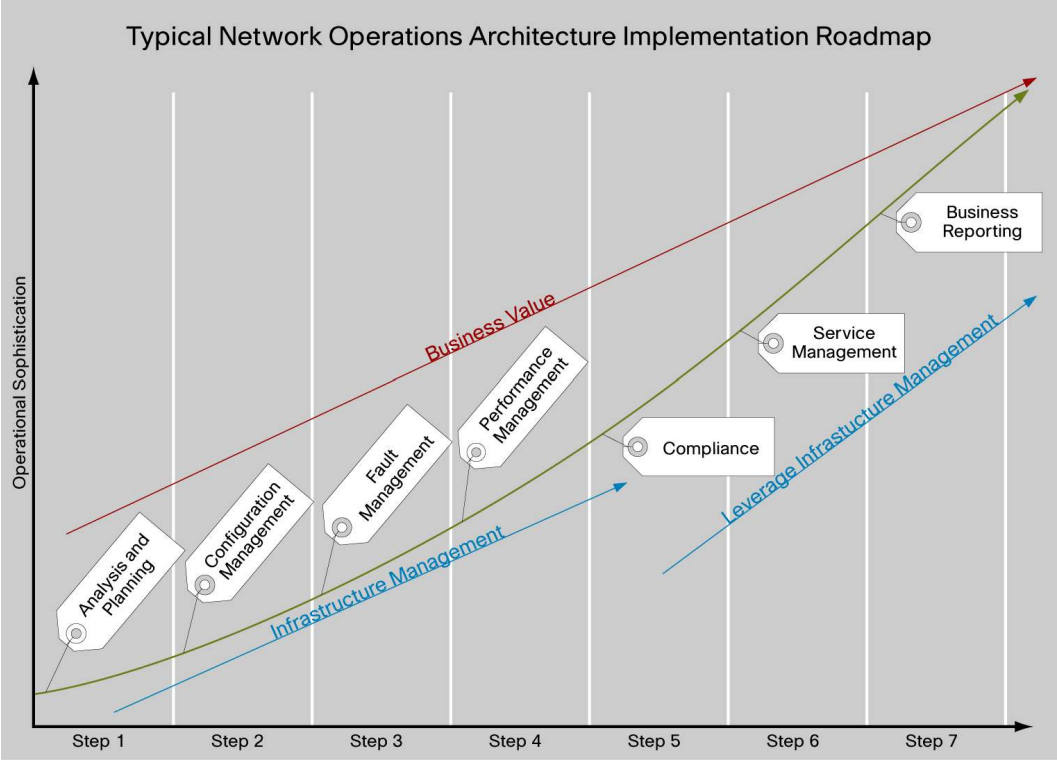
Architecture Implementation Roadmap

The key to implementing the NMRA is to understand your current position and determine what the desired state is. The following roadmap outlines a simple seven-step plan:

1. Analysis and planning
2. Configuration management
3. Fault management
4. Performance management
5. Compliance
6. Service management
7. Business reporting

The goal is to manage the infrastructure first, then to leverage this foundation and add more advanced capabilities, which are needed by the business. Figure 5 illustrates this concept.

Figure 5. Typical Network Operations Architecture Implementation Roadmap



Many organizations try to build an operational system that deploys all these capabilities at one time, but this requires a considerable resource investment, and frequently it is a challenge to remain relevant to the original requirements by the time the system is completed.

It is recommended to build the system one capability at a time. By delivering progressive capabilities, value is realized progressively as is the return on investment.

The exact order of these seven steps will vary, and there may be additional steps required, such as security management and accounting management. That is why the first step is an analysis and planning phase.

The following section includes a self-assessment that will assist in determining which functional capability is the most sophisticated, and the functional capability that requires development.

Configuration management is the foundation of the architecture; it provides the necessary information to other functional areas and through integration provides the key data to other systems.

Self-Assessment

The first step in bringing about change is to determine the desired state; the NMRA represents a desired state for a company's operations and network management. The second step is to determine the current state, which is to understand your current operational posture. The third step is to accept the position you are in and determine that change is needed. The fourth step is to decide that you want to change and execute.

The focus of this assessment is on the technology component of the NMRA, this will help identify which functional areas are lacking, and provide a focus for immediate remediation. From this technology assessment, the next step is to assess how effectively the technology combines with people and processes and to drill into more detail on the technology component.

The self-assessment will help you to determine a baseline for your current operational posture. It focuses primarily on functional management capabilities and asks questions about functional management capabilities, and these questions reflect the key functional requirements and the considered leading practices in each of these functional areas.

Honesty with these assessments is the best way to understand your position. A good way to derive some honesty is to have several people from your team complete them independently and average the scores.

Once the scores have been determined, plot them on the provided chart. This chart shows scores 1 to 5 for each of the functional areas and highlights the gaps that exist in your functional capabilities. The lowest scores should be addressed first.

This assessment does not determine how well these capabilities are performed but that the capability exists and that it is being performed.

Answer each question honestly, and for each “Yes”, a score of 1 is the result.

Fault Management Self-Assessment

Table 3. Fault Management Self-Assessment

Question	Yes/No	Score
Does the organization have a ping poller which results in a fault being raised when a device fails to respond to a ping?		
Are SNMP traps monitored, and specific traps result in a fault being raised?		
Are syslog events monitored, and specific syslogs result in a fault being raised?		
Is device hardware status monitored and faults raised for environmental exceptions, including power supply failure, redundant system failover, device temperatures, etc?		
Are faults sent to the service desk and managed using an incident management process?		
Total		

Configuration Management Self-Assessment

Table 4. Configuration Management Self-Assessment

Question	Yes/No	Score
Is inventory information collected from the network including all chassis, modules, and their serial numbers?		
Are device configurations collected on a regular basis?		
Are changes in device configuration detected, reported, and investigated?		
Is there a well documented base configuration template?		
Can running configurations be audited against config templates?		
Total		

Accounting Management Self-Assessment

Table 5. Accounting Management Self-Assessment

Note: If usage-based billing is not required within your organization, mark a total score of 5 and go to the next section.

Question	Yes/No	Score
Is NetFlow export or equivalent enabled on any devices?		
Is NetFlow or equivalent data being collected and stored?		
Is the collected data rated according to service type or application?		
Can the collected data be attributed to specific users or user groups?		
Are accounting adjustments made for SLA violations?		
Total		

Performance Management Self-Assessment

Table 6. Performance Management Self-Assessment

Question	Yes/No	Score
Are devices polled for interface statistics, and the results stored for historical analysis?		
Are devices polled for CPU and memory statistics, and the results stored for historical analysis?		
Can a report of the 10 most loaded WAN links be produced?		
Does the collected performance data have thresholds checked and raise a fault when the threshold is exceeded?		
Is business reporting in support of capacity planning including analysis of WAN links and device performance metrics?		
Total		

Security Management Self-Assessment

Table 7. Security Management Self-Assessment

Question	Yes/No	Score
Is TACACS or RADIUS used for device administration, authorization, access, accounting?		
Are there different access and authorization levels for service desk, operations, and level 3 support?		
Are device syslogs fed into a common syslog server?		
Are server, router, switch, firewall, and application logs monitored and/or reviewed and analyzed manually or by software?		
Can a global configuration change be implemented on all devices in less than 24 hours? (such as CERT or PSIRT configuration workaround)		
Total		

Self-Assessment Score

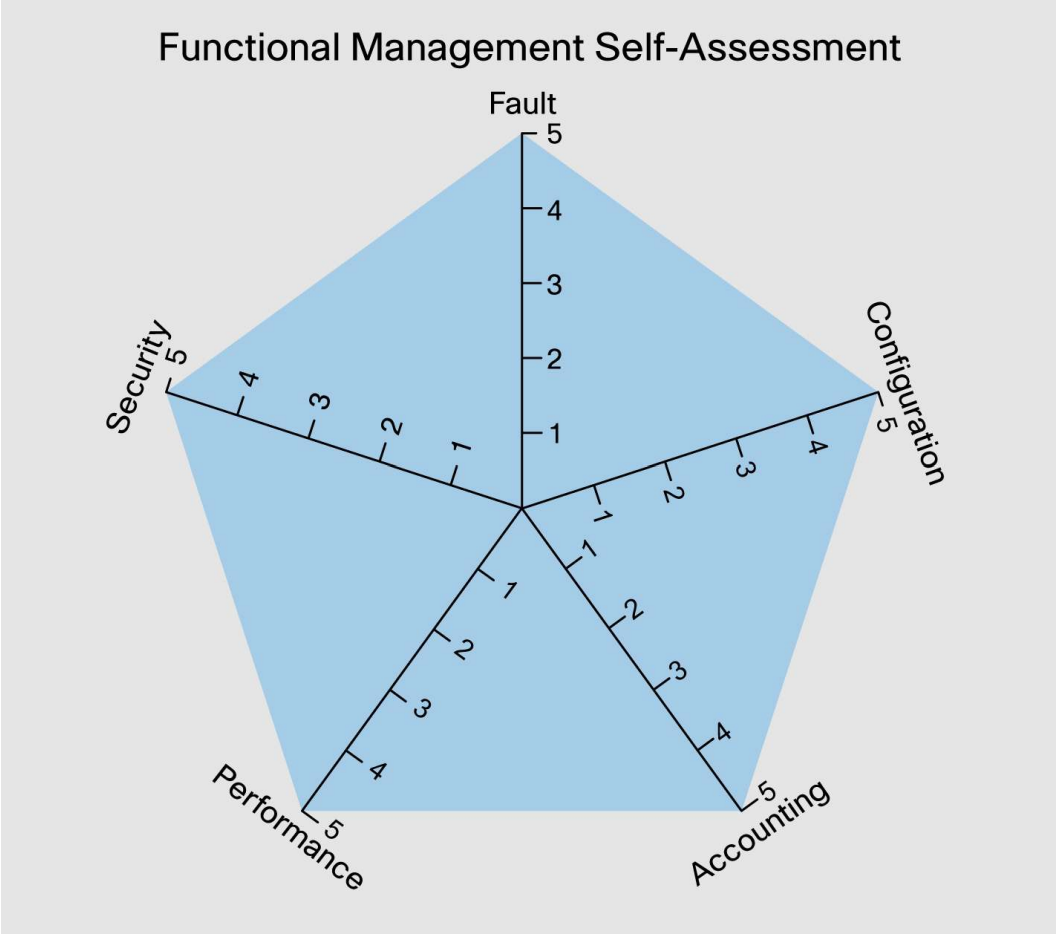
Table 8. Score Summary

Circle the score from the assessment questions.

Functional Area	Score
Fault	1 2 3 4 5
Configuration	1 2 3 4 5
Accounting	1 2 3 4 5
Performance	1 2 3 4 5
Security	1 2 3 4 5

Figure 6. Functional Management Self-Assessment Results

Mark the score on the chart below and connect the scores. This shows the gap from best practices to the current state.



References

1. http://www.itlibrary.org/
2. http://www.isaca.org/cobit.htm
3. http://www.tmforum.org/browse.aspx?catID=1647
4. http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper0900aecd806bfb4c.shtml
5. http://www.tech-faq.com/fcaps.shtml
6. http://www.cisco.com/warp/public/437/services/lifecycle/LifecycleServicesWhitePaper.pdf
7. http://www.sarbanes-oxley.com/index.php
8. http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
9. http://www.itservicecmm.org/

Recommended Reading

Network Management Fundamentals, Alexander Clemm, Ph.D., Cisco Press, ISBN 1-58720-137-2

Frameworks for IT Management, Jan van Bon et al, itSMF, Van Haren, ISBN 90 77212 90 6

IT Service Management, Ivor Macfarlane and Colin Rudd, itSMF, ISBN 0-9524706-1-6

IT Service Management Based on ITILv3, Jan van Bon et al, itSMF, Van Haren, ISBN 978-90-8753-102-7

Network Management Systems Architectural Leading Practice
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper0900aecd806bfb4c.shtml

Network Configuration Management
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper0900aecd806c0d88.shtml

Change Management: Best Practices
http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.html

Problem Management in the Networking Environment
http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c3eee.html

IP Service Level Agreement
http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb52.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

C11-453503-00 05/08