The Six Key Decisions For Effective Network Management

By Rich Schiesser in conjunction with Harris Kern's Enterprise Computing Institute

This article will present six key decisions that an infrastructure organization must make for managing IT networks, a nontrivial challenge in light of the diversity of current IT environments. Today's networks come in a variety of sizes, scopes and architectures, from a simple dual-node local network in your house to a sophisticated, encrypted network connecting tens of thousands of nodes world-wide.

As most are probably aware, when Bob Metcalfe, inventor of Ethernet, spoke the above quotation he was referring to the CEOs of Intel and Microsoft. At the time, Intel was producing powerful computer chips that provided almost unlimited processing and transmission capability for servers and networks, while Microsoft was producing software that all but consume all available processing power. Maintaining this balance between hardware capability and software consumption is a key element of sound network management.

There obviously is no single, detailed network management process that applies to all of these various environments. But there are common elements of the process that apply to almost all network scenarios, and the decisions that shape this process is what we will concentrate on in this article. We begin with a definition of network management followed by the prioritized traits of the process owner. We next discuss six key decisions that must be made in order to manage a robust network environment. These decisions apply to all network environments, regardless of platforms, protocols or peripherals, and lay the foundation for a robust network management process. We conclude with the standard assessment sheets customized for the network management process.

The Definition of Network Management

The formal definition of network management is as follows.

DEFINITION:

***Network Management* -** A process to maximize the reliability and utilization of network components in order to optimize network availability and responsiveness.

We see that our definition includes elements of two other processes: availability, and performance and tuning. Maximizing reliability is another of emphasizing high availability by ensuring network lines and the various components such as routers, switches and hubs maintain high levels of uptime.

Maximizing utilization implies: While these two are the primaries, there are actually six other systems management processes with which network management interacts, making network management one of the most inter-related disciplines.

Key Decisions About Network Management

Before an effective, high-level network management process can be designed, much less implemented, six key decisions need to be made that influence the strategy, direction and cost of the process. Figure 1-1 describes the questions that these decisions answer. Once answered, these decisions will define the scope of responsibilities and, more importantly, the functional areas that will be charged with employing the process on a daily basis.

1. What will be managed by this process?
2. Who will manage it?
3. How much authority will be given?
4. What types of tools and support will be provided?
5. To what extent will other processes be integrated with this process?
6. What levels of service and quality will be expected?

Figure 1-1 Key Decisions About Network Management

1. What will be managed by this process? – This may seem like an obvious question with an obvious answer: we will manage the network. But what exactly does this mean? One of the problems infrastructures experience in this regard is being too vague as to who is responsible for which aspects of the network. This is especially true in large, complex environments where world-wide networks may vary in terms of topology, platform, protocols, security and suppliers.

   For example, some infrastructures may be responsible for both classified and unclassified networks with widely varying security requirements, supplier involvements and government regulations. This was the case when I managed the network department at a nation-wide defense contractor. We decided early on exactly which elements of network management would be managed by our department and which ones would be managed by others. For instance, we all mutually decided that government agencies would manage encryption, the in-house security department would manage network security and computer operations with their help desk would administer network passwords.

Was this the only arrangement we could have decided on? Obviously it was not. Is it the best solution for anyone in a similar situation? That would depend, since each environment will vary as to priorities, directions, costs and schedule. It was the best solution for our environment at the time. Did we ever need to modify it? Certainly we did. Major defense programs hardly ever remain static as to importance, popularity and funding. As external forces exerted their influence on the program, we made appropriate changes to what would be included in our network management process. The key point here is to reach consensus as early as possible, and to communicate to all appropriate parties, as to what will be managed by this process.

2. <u>Who will manage it?</u> – Once we decide on "what" we will manage, we need to decide on "who" will manage it. Initially, this decision should determine which department within the infrastructure will be assigned the responsibility for heading up the design, implementation and ongoing management of this process. Within that department will be assigned the person who will have overall responsibility for the network management process. In essence, this decision deals with determining who the process owner will be.

   The ideal candidate to serve as owner of the network management process will have strong people skills, knowledge of network resources and a sense of urgency. Table 1-1 offers a more comprehensive list, in priority order, of the traits desired in such an individual. The people skills involve working with developers about application profiles, transaction mix and arrival patterns, and planned increases in workloads, and working effectively with users about desktop requirements, connectivity and security.

   A network management process owner should be knowledgeable about network operating systems, utility programs, support software and key hardware components such as routers switchers, hubs and repeaters. One of the most valuable traits for the owner of this process is a sense of urgency in tactically responding to, and resolving, a variety of network problems. Other desirable traits include knowledge of infrastructure software and hardware, and the ability to analyze metrics.

Table 1-1 Prioritized Characteristics of a Network Management Process Owner

	Characteristic	Priority
1.	Ability to work with IT developers	High
2.	Ability to work effectively with users	High
3.	Knowledge of network software and components	High
4.	Ability to think and act tactically	High
5.	Knowledge of systems software and components	Medium
6.	Knowledge of software configurations	Medium
7.	Knowledge of hardware configurations	Medium
8.	Knowledge of desktop hardware and software	Medium
10.	Ability to analyze metrics	Medium
11.	Ability to evaluate documentation	Medium
12.	Knowledge of applications	Low
13.	Knowledge of company's business model	Low
14.	Ability to manage diversity	Low
15.	Knowledge of backup systems	Low
16.	Ability to think and plan strategically	Low

3. How much authority will this person be given? – This is probably the most significant question of all because without adequate authority, the necessary enforcement and resulting effectiveness of the process rapidly diminishes. Few practices accelerate failure more quickly than giving an individual responsibility for an activity without the appropriate authority. Executive support plays a key role here from several perspectives. First, managers must be willing to surrender some of their authority over the network to the individual now responsible for overseeing its management. Second, managers must be willing to support their person in situations of conflict that will surely arise. Conflicts involving network management can originate from several sources.

   One source of conflict can come from enforcing network security policies such as if, when and how data over the network will be encrypted, or under what instances a single sign-on scheme will be employed for network and application logons. Another common source of network conflict involves user expectations about the infrastructure backing up desktop data instead of the more practical method of saving it to the server. The degree of authority a network management process owner has over network suppliers can also instigate conflict, particularly if managers have not communicated clearly to supplier management about the delegation that is in effect.

   Enforcing network connectivity standards is one of the greatest sources of conflict for network administrators. This is because most users feel they have adequate justification to warrant an exception, and very few administrators effectively convey the legitimate business reasons for having such a standard. More than once I have heard IT users in highly creative industries such as motion picture and television production companies present their arguments. Their claim is usually that their specialized artistic requirements should allow them to connect suspect devices with unproven interfaces to the network, even though alternate devices with standard interfaces could be used.

Table 1-2 Reasons For Network Connectivity Standards

Category	Explanation
1. Availability	Non-standard devices can lock up networks causing online system outages.
2. Performance	Non-standard hardware can cause non-stop transmissions, so-called network storms, which can significantly slow down online transactions.
3. Deployment	The deployment of a new application often requires installing additional desktop computers. Adhering to standard configurations simplifies the staging and deploying of large numbers of desktop computers.
4. Capacity	Some devices that deviate from standards are improperly configured for the network on which they are connected. This can cause countless re-transmissions, unanticipated network traffic, and problems for capacity planners.
5. Security	Most users want to feel assured that their data and applications are secured from external hackers and internal saboteurs. Standard interfaces help to ensure this.
6. Maintenance	Network connectivity standards simplify maintenance time and material costs by reducing training needs, spare parts inventory and supplier management.
7. Trouble-shooting	The smaller the variety of devices on the network, the smaller the need for specialized skills and diagnostic equipment to trouble-shoot problems.

On the other hand, when it comes to network administrators and process owners who either help or hurt their cause of enforcing network connectivity standards, I have had opportunities to work with both such groups. The group that undermined their own efforts at enforcement failed for two reasons. One was that they failed to offer compelling arguments to users as to why it was in their own best interest to comply with connectivity standards. The second was that the network group did not have adequate tools in place to enforce compliance with the standards.

The group who helped their cause of enforcing network connectivity standards did so by presenting several persuasive reasons why adhering to these standards would benefit users and suppliers alike. Table 1-2 lists the seven categories, with explanations, into which these reasons fall.

There is a third perspective concerning an executive who delegates security enforcement authority to a network administrator. This involves the executive's reaction to mistake's the administrator may make. Factors such as experience, training, fatigue, judgment, negligence, oversight, attitude and abuse should all be considered in determining the appropriate response to a potential mis-use of authority.

4. What types of tools and support will be provided? – Decisions about the type of tools and the amount of vendor support that will be provided directly influence the costs of managing networks. In general, the costs of these two entities are inversely proportional. As more cost is spent on vendor support, the need for expensive, sophisticated diagnostic tools should lesson. As more advanced tools are acquired and effectively used by in-house personnel, the need for costly, premium vendor support should correspondingly go down. One exception is classified networks where the granting of security clearances may reduce the number of vendor personnel cleared to a program. In this instance, the costs of vendor overtime and the expenses for sophisticated tools to trouble-shoot encrypted lines could both increase.

   A variety of network tools are available to monitor and manage a network. Some are incorporated in hardware components while most are software-based. Costs can range from just a few thousand dollars to literally millions of dollars for multi-year contracts with full onsite maintenance. Leveraging what other sites may be using, by negotiating aggressive terms with reluctant suppliers, and by inventorying your in-house tools can sometimes mitigate the expense for tools. More than one of my clients have discovered they were paying software licenses for products the client was unaware they owned.

   One tool often overlooked for network management is one that will facilitate network documentation. The criticality and complexity of today's networks require clear, concise and accurate documentation for support, repair and maintenance. Lack of emphasis on this important aspect or network management often results few pieces of network documentation that are both simple to understand yet thorough enough to be meaningful. Couple this with senior network designers' general reluctance to document their diagrams in a manner meaningful to less experienced designers, and the challenge of providing this information becomes clear.

There are a number of standard network diagramming tools available to assist in generating this documentation. The major obstacle is more often the lack of accountability than the lack of tools. The executive sponsor and the process both need to enforce documentation policy as it pertains to network management. One of the best tools I have seen offered to network designers is the use of a skilled technical writer who can assist designers over the hurdles of network documentation.

5. To what extent will other processes be integrated with this process? – A well-designed network management process will have strong relationships to six other systems management processes. These processes are availability, performance and tuning, change management, problem management, capacity planning and security. The extent to which network management integrates with these other processes by sharing tools, databases, procedures or cross-trained personnel is a decision that will influence the effectiveness of the process.

   For example, capacity planning and network management could both share a tool that simulates network workloads to make resource forecasts more accurate. Similarly, a tool that controls network access may have database access controls, which the security process could use.

6. What levels of service and quality will be expected? – The levels of service and quality that network groups negotiate with their customers directly affect the cost of hardware, software, training and support. This is a key decision that should be thoroughly understood and committed to by the groups responsible for budgeting its costs, and delivering on its agreements.

   Suppliers of network components, such as routers, switches, hubs and repeaters should also be part of these negotiations since their equipment has a direct impact on availability and performance. Long distance carriers are another group to include in the development of service level agreements. Many carriers will not stipulate a guaranteed percentage of uptime in their service contracts because of situations beyond their control such as natural disasters or man-made accidents such as construction mishaps. In these instances, one can specify conditions in the service contract for which carriers will assume responsibility such as spare parts, time to repair and on call response times.

   Service level agreements for the network should be re-visited whenever major upgrades to hardware or bandwidth are put in place. The SLAs should also be adjusted whenever significant workloads are added to the network to account for increases line traffic, contention on resources or extended hours of service.

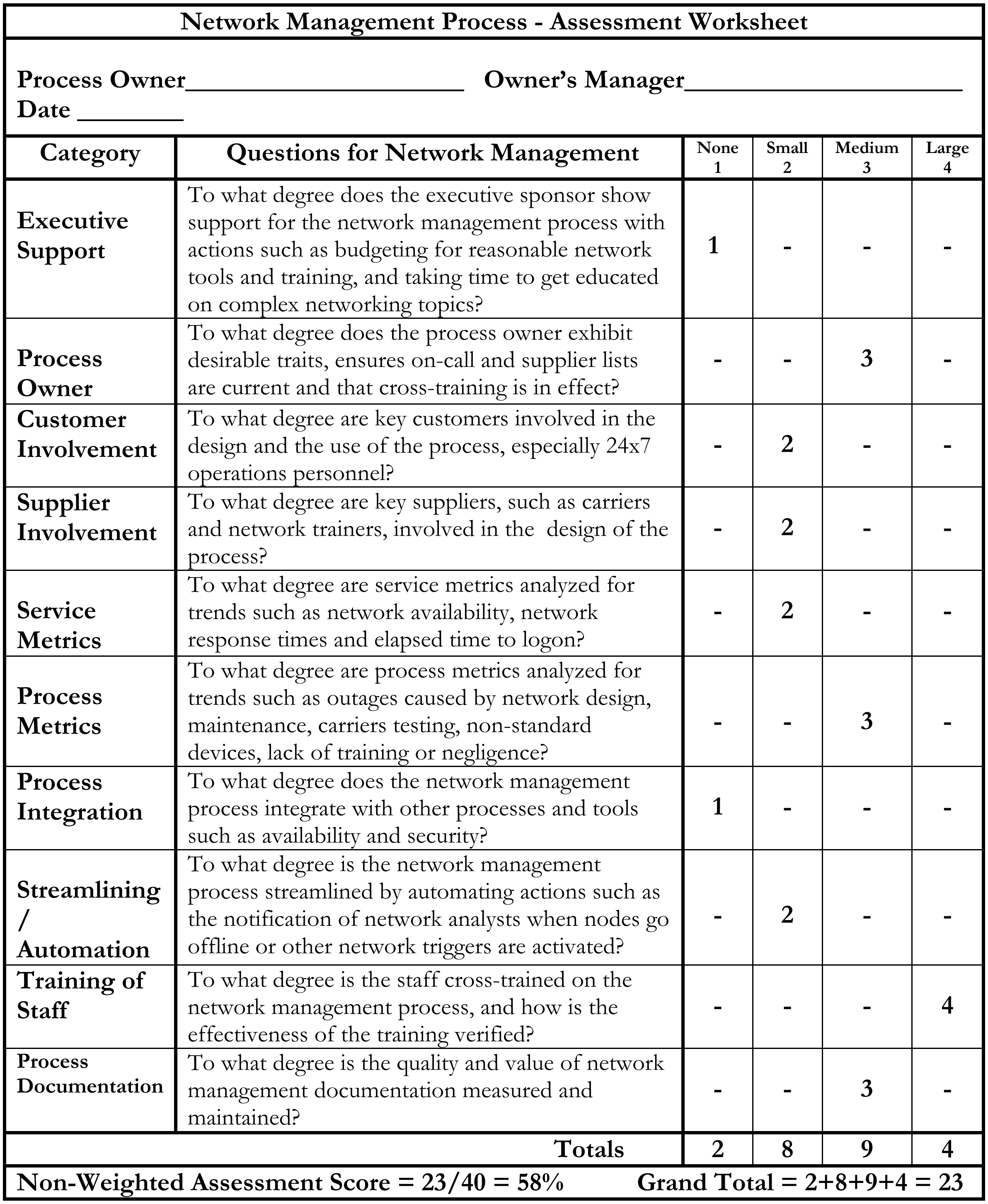
Assessing an Infrastructure's Network Management Process

The worksheets shown in Figures 1-2 and 1-3 present a quick and simple method for assessing the overall quality, efficiency and effectiveness of a network management process. The first worksheet is used without weighting factors, meaning that all ten categories are weighted evenly for the assessment of a network management process. Sample ratings are inserted to illustrate the use of the worksheet. In this case, the network management process scored a total of 23 points for an overall non-weighted assessment score of 58%, as compared to the second sample worksheet, which compiled a weighted assessment score of 61%.

The above referenced worksheets apply only to the network management process. However, the fundamental concepts on the use of these evaluation worksheets are the same for all disciplines.

Measuring and Streamlining the Network Management Process

A network management process can be measured and streamlined with the help of the assessment worksheet showed in Figure 1-2. The effectiveness of a network management process can be measured with service metrics such as network availability, network response times and elapsed time to logon. The efficiency of this process can be measured with process metrics such as outages caused by network design, maintenance, carriers testing, non-standard devices, lack of training or negligence. A network management process can be streamlined by automating actions such as the notification of network analysts when nodes go offline or other network triggers are activated.



Network Management Process - Assessment Worksheet

Process Owner_____________________ Owner's Manager_____________________
Date ________

Category	Questions for Network Management	None 1	Small 2	Medium 3	Large 4
Executive Support	To what degree does the executive sponsor show support for the network management process with actions such as budgeting for reasonable network tools and training, and taking time to get educated on complex networking topics?	1	-	-	-
Process Owner	To what degree does the process owner exhibit desirable traits, ensures on-call and supplier lists are current and that cross-training is in effect?	-	-	3	-
Customer Involvement	To what degree are key customers involved in the design and the use of the process, especially 24x7 operations personnel?	-	2	-	-
Supplier Involvement	To what degree are key suppliers, such as carriers and network trainers, involved in the design of the process?	-	2	-	-
Service Metrics	To what degree are service metrics analyzed for trends such as network availability, network response times and elapsed time to logon?	-	2	-	-
Process Metrics	To what degree are process metrics analyzed for trends such as outages caused by network design, maintenance, carriers testing, non-standard devices, lack of training or negligence?	-	-	3	-
Process Integration	To what degree does the network management process integrate with other processes and tools such as availability and security?	1	-	-	-
Streamlining / Automation	To what degree is the network management process streamlined by automating actions such as the notification of network analysts when nodes go offline or other network triggers are activated?	-	2	-	-
Training of Staff	To what degree is the staff cross-trained on the network management process, and how is the effectiveness of the training verified?	-	-	-	4
Process Documentation	To what degree is the quality and value of network management documentation measured and maintained?	-	-	3	-
	Totals	2	8	9	4

Non-Weighted Assessment Score = 23/40 = 58% Grand Total = 2+8+9+4 = 23

Figure 1-2 Sample Assessment Worksheet for Network Management Process

Network Management Process - Assessment Worksheet

Process Owner______________________ Owner's Manager______________________
Date ________

Category	Questions for Network Management	Weight	Rating	Score
Executive Support	To what degree does the executive sponsor show support for the network management process with actions such as budgeting for reasonable network tools and training, and taking time to get educated on complex networking topics?	**3**	**1**	**3**
Process Owner	To what degree does the process owner exhibit desirable traits, ensures on-call and supplier lists are current and that cross-training is in effect?	**3**	**3**	**9**
Customer Involvement	To what degree are key customers involved in the design and the use of the process, especially 24x7 operations personnel?	**1**	**2**	**2**
Supplier Involvement	To what degree are key suppliers, such as carriers and network trainers, involved in the design of the process?	**5**	**2**	**10**
Service Metrics	To what degree are service metrics analyzed for trends such as network availability, network response times and elapsed time to logon?	**3**	**2**	**6**
Process Metrics	To what degree are process metrics analyzed for trends such as outages caused by network design, maintenance, carriers testing, non-standard devices, lack of training or negligence?	**5**	**3**	**15**
Process Integration	To what degree does the network management process integrate with other processes and tools such as availability and security?	**1**	**1**	**1**
Streamlining / Automation	To what degree is the network management process streamlined by automating actions such as the notification of network analysts when nodes go offline or other network triggers are activated?	**3**	**2**	**6**
Training of Staff	To what degree is the staff cross-trained on the network management process, and how is the effectiveness of the training verified?	**3**	**4**	**12**
Process Documentation	To what degree is the quality and value of network management documentation measured and maintained?	**3**	**3**	**9**
Weighted Assessment Score = 73/(30*4) = 61%	**Totals**	**30**	**23**	**73**

Figure 1-3 Sample Assessment Worksheet for Network Management Process With Weighting Factors