



# Twin Eagle Network Management:

## *Concepts & Strategies*



*February 19, 2009*



## 1. Introduction

A network exists in order to provide specific services for the business, and effectively managing that network means understanding these services as well as the specific design of the network. There is no “one size fits all” approach to system and network management! *Twin Eagle* designs network management solutions with these realities in mind.

In order to be proactive in managing a complex business-critical network, there are several things that must be clearly defined.

<b>PEOPLE</b>	Are the right people involved in the right things at the right time?
<b>PROCESSES</b>	Are the procedures and workflow clearly understood, and are these processes constructed in the most efficient and effective manner?
<b>TECHNOLOGY</b>	Are the right combinations of computer hardware & software in place to automate and monitor the activities that are critical for the business?

It is only through the coordination of these three types of resources that a company can hope to achieve efficiency in network management and alignment with the needs of the business. So often the network management tools (**TECHNOLOGY**) are viewed as the “silver bullet” that will solve all of the problems, but in reality these wonderful tools may become worse than useless if they are not combined with clearly defined business processes and the appropriate efforts of people within the network operations organization.

## 2. Digging Deeper into Business Processes

Many organizations already follow the discipline of basic business process for handling changes to the network and mobilizing technicians to resolve issues. In order to be truly effective in managing business-critical systems and networks, there are several other areas for business process improvement that should be considered. Here are a few key questions that should be on the mind of everyone responsible for a company’s network:

- How do I ensure that changes to the network do not disrupt my services?  
(**CHANGE MANAGEMENT**)
- How do I handle communication with the operational users and stakeholders of my network? (**SERVICE DESK/CALL CENTER**)
- How do I mobilize technicians in the event of a disruptive network event?  
(**INCIDENT & EVENT MANAGEMENT**)



- How do I guarantee that network hardware and software versions are stable and up-to-date? (**RELEASE & PROBLEM MANAGEMENT**)
- How do I ensure that the agreed-upon services are delivered when and where they are required? (**SERVICE LEVEL MANAGEMENT**)

At a minimum, these types of business processes must be clearly defined and implemented in order to efficiently manage any complex business-critical network.

### 3. Understanding the Business Impact of System Disruptions

It is an obvious fact that a disruption in your network operations may lead to poor customer service, delays & lost user productivity, decreased customer satisfaction, higher costs, and less profit. One of the key success factors that will drive effective network management is to understand the business impact of poorly performing systems. Several questions can be asked in order to flesh out the effect of network and process failures:

- What is the worst thing that could happen to this system?
- How would we know if and when this “worst case scenario” occurs?
- What are the three most common incidents that tend to disrupt our operations?
- When these events happen, how long does it take to get the situation resolved?
- During these incidents, are we still able to “sell” our products or services to our customers?
- Is there a measurable financial impact associated to the most common disruptions?
- What are the costs for dispatching technicians to fix these disruptions?
- During these incidents, are there also costs for “lost opportunities” in servicing our customers?
- Which principle do we tend to operate under?  
***If it ain't broke, then don't fix it!*** or ***If it ain't broke, then improve it!***
- When an incident occurs, how many people need to be involved in fixing the issue as well as in notifications of the outage and justifying the resolution?



When considering the use of network management technologies, these are the types of questions that **PEOPLE**, **PROCESSES**, and monitoring **TECHNOLOGY** should help you answer.



## 4. The Case for Proactive Network Management

One of the primary principles of troubleshooting is that “You cannot solve a problem until you know what caused the problem!” When dealing with complex technology systems, it is often difficult to discover the root cause of a network performance issue. That is why it is essential to have monitoring tools in place which assist in diagnosing the root cause of the incidents that occur within your system. What is needed are monitoring tools that discover issues and show unhealthy trends well in advance of actual system failures.

The goal for having proactive monitoring tools is to minimize downtime and *Mean Time to Repair* (MTTR). It is also important for system operators to discover and accurately diagnose problems in real time, and to quickly collect the data they need for efficient resolution of incidents. Ultimately, it is best to detect, report, and correct problems *before* they result in service interruptions for the business.

### Designing an effective Network Operations Center leads to:

- Significant reductions in downtime
- Immediate management of incidents whenever they occur
- Increased productivity and job satisfaction for network and support staff
- Increased customer satisfaction for users of the system

The more business-critical your system is, then the stronger is the case for adopting proactive network monitoring methods. Management requires tools which provide an understanding of how system issues are affecting the users and the business as a whole, and most business-critical systems have a *direct* impact on the financial bottom line of the company.

The most effective organizations are those that leverage monitoring tools combined with “bullet proof” operational processes and well-trained staff. This moves the organization in the direction of becoming more and more proactive in the support of the services they deliver. Once these **PEOPLE**, **PROCESSES**, and **TECHNOLOGIES** are in place, then the organization becomes an efficient link in the chain supporting the entire business.

## 5. The Effectiveness of “Management by Exception”

Network management tools are capable of generating a large amount of information about the behavior of the system. However, it is not practical or even possible for a network technician to look at and evaluate every single data point. In order to make the best use of network monitoring tools, an organization needs to adopt a policy of “**Management by Exception.**” Implementing this policy involves determining the baseline for acceptable performance of the



network or system, and then deciding what actions to take when an event is detected that is outside of this acceptable range of behavior.

Thresholds must be established for the key metrics that show acceptable performance, and actions should be defined for cases when those thresholds are crossed. Often a team of key users, operators, technicians, and engineers work together to determine the important metrics and threshold values, as well as the actions that must be triggered for exceptions.

If this exercise is not accomplished, then the typical result is network management tools which are ignored because they produce too many alerts or because the defined actions are not meaningful. The death knell for network monitoring tools is having the **exceptions** become the **rule**. When threshold violations are not meaningful or when appropriate actions are not associated with these exception events, then network monitoring tools become useless “shelf-ware” and a wasted expense.

To simplify the exercise of establishing performance thresholds and defining appropriate actions for each exception, several key questions need to be asked:

- What are the essential metrics that indicate acceptable system performance?
- What is the specific range of acceptable values for each of these metrics?
- What is the definite time period when each system component must meet its thresholds?
- If an exception is generated when a threshold is crossed, what are the acceptable limits associated with values that are out of range? For example:
  - Can a particular threshold be crossed a certain number of times before an exception is generated?
  - If an exception occurs, but the value returns to the normal range within a certain period of time, should an exception event be generated?
  - If a “bouncing” exception occurs (“flapping” between normal and abnormal), how many bounces should be allowed within a certain period of time?
- If a system component breaches its appropriate level of performance, what specific action should be taken?
- Who will be the responsible party for taking the initial action, and what is the escalation path if the incident cannot be resolved by the original responder within a certain period of time?
- How will the business costs be defined and tracked for each threshold exception?





- How will exception events and their impacts be reported to the business stakeholders of this network or system?

## **6. Designing Network Management for Unique Business Needs**

Since there is no “one size fits all” approach to system and network management, *Twin Eagle* designs network management solutions to meet the unique business needs of your organization. The systems and networks in the typical environment form a complex and interdependent set of working components – with hardware, software, wires, and radio waves being used in various combinations to form the “nervous system” for your company’s business activities.

A *Network Operations Center (NOC)* should be designed to serve the specific needs of your organization, and this can include any or all of the following:

- Monitoring the computer systems and core applications that provide essential services to the business (hardware, software, databases, web services, etc)
- Monitoring the network backbone, including the microwave backhaul infrastructure
- Monitoring the end-point devices in your network, whether serial or IP-based
- Monitoring the Access Point or Master Radio devices in your wireless network
- Regular reporting on system & network performance and issue resolution
- Providing backup & restoration of critical equipment configurations
- Remotely aiding technical staff members with troubleshooting and training

These and many other services are available through the experienced team at Twin Eagle Consulting. Please contact us at the following address to discuss your unique needs for the efficient operation of your business.

**Twin Eagle Consulting, LLC**  
**7330 South Alton Court**  
**Centennial, Colorado 80112**  
**Office: 303-531-4598**  
**FAX: 303-482-1423**

[info@twineagleconsulting.com](mailto:info@twineagleconsulting.com)  
<http://www.twineagleconsulting.com>

