Ultimate Guide to Network Management in The Enterprise
In this e-guide:

- Ultimate guide to network management in the enterprise  p. 2
- Why is network management important?  p. 2
- Network management functions  p. 5
- Best practices for managing networks  p. 6
- Network management challenges  p. 8
- Network management tools  p. 10
- Next-generation network monitoring techniques  p. 14
- Further reading  p. 17

This network management guide explains the challenges of enterprise oversight, best practices for automating tasks, and the next-gen with AI and machine learning.
In this e-guide

- Ultimate guide to network management in the enterprise  p. 2
- Why is network management important?  p. 2
- Network management functions  p. 5
- Best practices for managing networks  p. 6
- Network management challenges  p. 8
- Network management tools  p. 10
- Next-generation network monitoring techniques  p. 14
- Further reading  p. 17

Ultimate guide to network management in the enterprise

Sandra Gittlen, Editor at Large, SearchNetworking

Network management is a cornerstone of IT that helps ensure that enterprises run efficiently and effectively end to end. In recent years, network administration and management, which includes provisioning, security and optimization, have become greatly automated and have started to incorporate advanced technologies. Artificial intelligence (AI) and machine learning expand visibility into and control of the network and its devices without increasing the burden on IT teams.

In this network management guide, we dig deep into functions, techniques, best practices, next-generation technology and more. The links embedded throughout the article lead to even more information and provide a better understanding of the important role network management plays in every enterprise.

Why is network management important?

To best illustrate the business need for a well-considered network management strategy, IT should calculate the cost of network downtime. Network downtime affects
revenue, employee productivity, reputation damage, monetary damage and general Opex costs.

The monetary damage from network brownouts, which are unanticipated and unplanned drops in network quality, averages about $600,000 per organization, according to a survey from network monitoring software provider Netrounds. Whether expected or unexpected, downtime incurs costs that organizations can avoid or at least reduce with the help of network management.

In the past, companies might have justified taking a lighter approach to network management because achieving comprehensive visibility and monitoring required a large amount of skilled staff. Network automation has eased that burden by eliminating common labor-intensive manual network tasks, such as provisioning, scripting, implementing change requests and identifying causes of slowdowns and outages.

Automation also has brought about the following benefits:

- reductions in human errors;
- rapid provisioning of new services;
- the ability to locate and identify the root cause of network security issues; and
- reduced security risks because fewer manual processes mean fewer configuration or policy errors that can create vulnerabilities.

Network automation is just one of many concepts and terms that are important to know as you deepen your understanding of network management.
In this e-guide

- Ultimate guide to network management in the enterprise  p. 2
- Why is network management important?  p. 2
- Network management functions  p. 5
- Best practices for managing networks  p. 6
- Network management challenges  p. 8
- Network management tools  p. 10
- Next-generation network monitoring techniques  p. 14
- Further reading  p. 17

10 essential network management tasks

These 10 network management tasks are crucial to building and maintaining a resilient network that can meet current and future demands.

1. Network configuration
2. Network monitoring and alerting
3. Troubleshooting and root cause analysis
4. Change control management
5. Firmware bug and vulnerability patching
6. Configuration backup and secure storage
7. Policy and compliance validation
8. Network diagrams
9. Network resiliency
10. Short- and long-term roadmapping

Next section
Network management functions

Network management comprises five major elements: fault management, configuration management, account management, performance management and security management (also known as FCAPS). Network management expert Amy Larsen DeCarlo detailed each of these elements, explaining their importance in administering and managing enterprise operations.

To account for the efficacy of these elements, network professionals use monitoring tools that watch the network end to end. These tools provide visibility into performance, traffic, usage, faults and availability. As expert Ed Tittel and IT writer Kim Landros explained, "... careful network monitoring can facilitate proactive strategies, such as justifying the cost of hardware or infrastructure upgrades required to eliminate chronic network bottlenecks."

Network monitoring -- while available as network device logs, open source tools or proprietary monitoring features built into network products -- often performs better as a fully dedicated platform with a rich feature set and vendor support.

Along with network monitoring, organizations should carefully consider implementing a network analytics tool to compile the data gathered through monitoring and generate insightful and actionable reports. Network analytics and network monitoring tools should be able to span on-premises, cloud or hybrid environments as well as uniformly deal with wired and wireless infrastructure.
In this e-guide

- Ultimate guide to network management in the enterprise p. 2
- Why is network management important? p. 2
- Network management functions p. 5
- Best practices for managing networks p. 6
- Network management challenges p. 8
- Network management tools p. 10
- Next-generation network monitoring techniques p. 14
- Further reading p. 17

Conducting a network assessment that accounts for the various network components that can gather and analyze telemetry data will be essential to pick the tools most appropriate for your corporate enterprise. For instance, some platforms focus heavily on monitoring and reporting with a few out-of-the-box analytics features while others focus on deep root cause analysis and AI customization. Make sure to include IoT environments, if you have them, in your assessment.

Best practices for managing networks

**Inventory the enterprise.** Take an accurate inventory of all the devices and applications in the network. Use tools that can discover devices automatically to spare IT the difficulty and tediousness of this task.

**Reduce manual management.** Automating network management is considered a best practice but is far too general a notion to implement wholesale. Automation should be kept simple, low risk and quickly implementable to start. For instance, network teams can automate device locators to find out where a device connects to the network, perform application connectivity checks, verify each network infrastructure device is properly connected to its neighbor, and find discrepancies between parts of network configurations and the organization's configuration templates. As teams achieve success with this low-hanging fruit, they can move up to automating intermediate and advanced tasks, which include verifying Border Gateway Protocol connectivity and automating access control list updates.
Evaluate the scope and risk of changes. Even the network change management process is driven by best practices, which reduce the risk of a failed change. Applying some basic operating principles, such as evaluating the scope of a proposed change, will prevent possible missteps down the road.
Some questions to include the following:

- What are the number of endpoints affected by the change?
- What is the importance of the services a change might affect?

Evaluation of the scope should be accompanied by a risk analysis. After that, network teams should put the change through a peer review, pre-deployment testing and validation, implementation and testing, and documentation and network management updates.

**Make processes, including troubleshooting, repeatable through documentation.** Documentation is useful in most areas of network management, especially when trying to troubleshoot issues with wired and wireless connectivity. For instance, how IT approaches identifying and resolving wireless network connectivity problems should be documented and repeatable to save time and avoid misconfigurations.

TechTarget contributor Lisa Phifer offered 10 steps to troubleshooting wireless network connection problems that take readers from basic problems, such as making sure the correct Wi-Fi access point is selected, to more advanced client issues.

**Network management challenges**

Even with best practices in place, network management can pose challenges for enterprises.
In this e-guide

- Ultimate guide to network management in the enterprise  p. 2
- Why is network management important?  p. 2
- Network management functions  p. 5
- Best practices for managing networks  p. 6
- Network management challenges  p. 8
- Network management tools  p. 10
- Next-generation network monitoring techniques  p. 14
- Further reading  p. 17

Monitoring 101 for virtual and automated networks

VIRTUAL NETWORKS
Monitor the performance of virtual machines and the hypervisor platform. Don't forget to track compute, memory and storage resources, as well.

AUTOMATED NETWORKS
Monitor and log all automation processes and changes. This allows network teams to better identify potential issues in network performance.
Legacy networks. If an organization is relying on cumbersome legacy monitoring tools, then managing disparate environments, including virtual and cloud-based networks, could prove difficult. Legacy tools also can impede efforts to gain end-to-end visibility.

Complexity and abstraction. Modern technologies also have their challenges as they add to the complexity of network environments. For instance, in virtualized environments, traditional network monitoring tools are forced to interact with hypervisors. Hypervisors force a split between appliance-based networking components, virtual routers, switches and firewalls and can complicate end-to-end visibility.

Overlay networks are similarly problematic as they can hide underlying hardware and software from monitoring tools.

Interconnectivity. Although multi-cloud environments are gaining interest, the bridges that connect the environments are causing provisioning headaches, performance inconsistencies and security blind spots that network professionals are left to resolve. They make applying sound network management principles a difficult endeavor.

Network management tools

Network management vendors are spending a great deal of time trying to reduce the complexity and increase the interoperability and feature sets of their products. Even so, most companies still use multiple network management tools for various products
and devices, which only adds to the complexity. Below are some examples of progress being made with network management interoperability.

**Integrated network monitoring and security**

Integrating network management and monitoring with security tools to *distill more comprehensive security insights* provides incredible value to businesses. With this capability, network managers can play a larger role in addressing security risks, and they will be able to share important information with security teams.

Integrating network management security can also be beneficial when it comes to the labor-intensive task of running security audits. IT teams can *automatically verify configurations and standards* across devices and relay the results more efficiently.

**As-a-service network monitoring**

Vendors also are concentrating on how to help network teams *monitor cloud environment performance*, especially SaaS, PaaS and IaaS. In terms of SaaS monitoring, network teams must find a tool that lets them monitor the end user's path from the internet service provider to the public cloud to measure service latency, DNS speed and accessibility, and content delivery network responsiveness from an end-user perspective.

Check out how network performance monitoring *tools have evolved* to account for as-a-service environments.
Hybrid cloud monitoring

Cloud providers often help businesses monitor within their own environment only, but a new crop of network monitoring tools is emerging to satisfy the multi-cloud monitoring need. Hybrid cloud monitoring platforms use a passive network appliance to capture traffic data across the entire hybrid cloud environment. Along with analytics capabilities, they can identify a potential break before it causes significant problems.

Pros and cons of open source network monitoring tools

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low cost, usually free</td>
<td>Historically difficult to install and not user-friendly</td>
</tr>
<tr>
<td>Customization capabilities tailored to specific environments</td>
<td>Lack solid customer support teams</td>
</tr>
<tr>
<td>Improved quality and reliability compared to previous open source software</td>
<td>Despite advances, many tools still unwieldy and time-consuming to implement</td>
</tr>
<tr>
<td>Created and fully researched by skilled developers</td>
<td>Command-line interfaces require extensive input of commands</td>
</tr>
<tr>
<td>Easier to implement and use compared to earlier open source tools</td>
<td>Many user interfaces not easy to navigate</td>
</tr>
<tr>
<td>Many tools work across different platforms</td>
<td>Some tools lack customization and report generation</td>
</tr>
</tbody>
</table>
Open source network monitoring

For companies on tighter budgets but still under pressure to meet service-level agreement demands, open source network monitoring is an attractive and cost-effective choice. The industry’s most skilled developers have collaborated on these offerings, which have undergone rigorous peer and user review.

Open source tools also can help organizations avoid the increasing licensing costs that arise from adding more components that need monitoring. With open source, enterprises can expand the environment they need to manage, including servers and switches, without breaking the budget on licensing and support contracts.

Configuration management

Configuration management improves network maintenance and helps keep track of connected devices, device configurations and device connections. With configuration management, network teams can achieve three goals: maintain accurate configuration records, enable efficient network scans and enable network automation capabilities.

Automated network testing

Automated network testing can supplement network management tools, verifying physical connectivity, routing protocol functionality, path performance and more. However, the same problems that can plague network management around abstraction, virtualization and overlays apply to automated network testing.
Network automation tools come in three varieties:

- tools that were primarily built for server and application automation but have expanded to include the network;
- tools that are purpose-built for the network; and
- software-defined platforms that create a software overlay across LAN hardware.

All of these bring features and capabilities to the table that eliminate manual, error-prone tasks such as configuration backups, tool access control, compliance monitoring and verification, vulnerability assessments and network orchestration. Read more from Andrew Froehlich to explore the leading network automation tools. Soon, network professionals will be looking to combine network automation tools to create an end-to-end service to aid in design, implementation and testing.

Next-generation network monitoring techniques

One of the most promising technologies for network management is intent-based networking. Intent-based networks use automation and orchestration to change how network configurations are deployed. The goal is to have self-managing, self-healing networks that draw on AI and machine learning to carry out network tasks.
Intent-based networking: What happens behind the scenes?

**Intent**
A user inputs a business request into the IBN system using a GUI or conversational UI.

**Validation**
The IBN system validates the request to make sure it's feasible. The system then sends potential configurations to the network engineer for approval, without applying them.

**Approve/deploy**
The network engineer approves the configurations and the IBN system uses automation to deploy them.

**Behind the scenes**

**Abstraction**
The IBN system builds a working model of the network—using advanced analytics—that is aware of network behavior. It uses this model to gauge how configurations will affect the network.

**Network orchestration**
Automation and orchestration have central roles in validating intent, generating and deploying configurations, and monitoring the network.

**Outcome**
After initial provisioning, the IBN system continues to glean network data and apply it to the working network model. This process allows the system to monitor the network, make adjustments and ensure everything aligns with the original intent.
Admittedly, IT teams are wary of this level of automation, fearing it will make them far too removed from day-to-day operations. As organizations hire network professionals, they should ensure candidates are comfortable ceding some control to emerging automation and intelligence tools to better implement automation adoption in the enterprise.

On the security front, AI and machine learning will help network teams discern dangerous activity from harmless anomalies by recognizing disruptive traffic patterns that diverge from normal activity. This becomes especially important in IoT environments.

AI and machine learning also will improve network operations, enabling analytics applications to discover the root cause of an issue and automatically implement the correct fix.

One of the biggest wins to come from AI and machine learning is a significant drop in the volume of events IT staff members must handle each day, potentially decreasing from millions and thousands to just a few critical ones.

Network management is evolving quickly as advanced technologies are built into them, leaving IT to become more strategic in how they administer and manage their next-generation networks.
In this e-guide

- Ultimate guide to network management in the enterprise p. 2
- Why is network management important? p. 2
- Network management functions p. 5
- Best practices for managing networks p. 6
- Network management challenges p. 8
- Network management tools p. 10
- Next-generation network monitoring techniques p. 14
- Further reading p. 17

About SearchNetworking

Network managers and other IT professionals in a variety of industries rely on us for up-to-date industry news, must-have technical tips, and valuable best practices on top networking trends like wireless LANs, IP addressing and subnetting, network security and firewalls, Ethernet, virtualization, and network and systems management and monitoring. Plus, we cover the latest on career-boosting network certifications, such as the popular CCNA and CCNP.

So, whether you are looking for advice on micro-segmentation, upgrading legacy network infrastructure, or seeking new management strategies to improve the performance of your network and save money, our accomplished editorial team and contributors have you covered.

For further reading, visit us at http://SearchNetworking.com/

©2020 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.