



10 Steps to Streamline the Deployment of Network Monitoring Software for SMBs

WHITE PAPER

EXECUTIVE SUMMARY

You have decided that you want to install network monitoring software at your small-to-medium size business (SMB). A little preparation before the installation and configuration will save a lot of time. If you have some basic information at your fingertips on how you will be using your new network monitoring solution, the deployment process will not be sidetracked as you try to find information or make decisions that could have been made in advance. These best practices will insure that the process goes as smoothly as possible.

HOW CAN YOU STREAMLINE YOUR NETWORK MONITORING DEPLOYMENT?

- Review your goals for deploying a network monitoring solution
- Select the machines that will run the network monitoring software
- Create a list of the IP addresses for devices that you want to monitor
- Decide how you are going to structure your network maps
- Configure firewalls for access
- Determine the SNMP community strings you'll need
- Know what information you require from each device
- Identify who will receive alerts
- If you are monitoring NetFlow information, identify the routers and switches that should be exporting data
- Specify what data is going to be charted and what reports you need



You can streamline the initial deployment of network monitoring software by spending time to gather information and make decisions that will be necessary during the installation and configuration process before you commence. It can be quite frustrating if you have to interrupt the install to decide between different preference options or to collect the necessary data to complete the configuration. By following the recommendations below your implementation will be more efficient.

Review Goals

During the early stages of defining the need and determining which features are required, you most likely documented the goals for deploying a network monitoring solution. Now is a good time to review those goals so that when you “go live” you have set –up the software and administrative processes to achieve these goals.

Select Machine for Install

A small to medium size network usually only needs a single network monitoring system in a central location. However, it may make sense to install your network monitoring solution on more than one server, especially if you have a network distributed across multiple sites. For remote use of the monitoring software, there is generally a web or client-based access tool. Decide who has access to each part of the network and determine their appropriate access permissions.

Create IP Address List

A robust auto-discovery function should be able to map out most of the devices on your network, but if you do not want to monitor every node on your network you can also import, or enter lists of IP addresses manually.

Decide Map Structure

Many network monitoring systems offer tools for displaying the network topology by geography, hierarchy, physical connections or function. Depending on how you divide responsibility for monitoring, one of these may be more appropriate. For instance, if you need to monitor a remote site you might want to put all devices at each location together. Alternatively, if one technician is responsible for servers and another for routers, grouping similar devices together in a map may be more useful.

Configure Firewalls

You’ll want to configure any firewalls to allow remote access to the monitoring server, as well as to allow the central monitoring server to reach certain devices.



Collect Security Codes

You've set-up security to protect the important parts of your network. Make sure to have all the necessary security codes available. The simple network management protocol (SNMP) community strings are like passwords to enable monitoring of all parts of your network. In addition, on some devices you will need to add the monitoring station to a list of allowed SNMP managers (access control list).

Gather Device Information

Pings can return basic information, such as availability or packet loss for any device. SNMP can provide much more information, such as traffic, packet errors and discards, as well as a wealth of operational data. Collecting more customized information may require special probes, plug-ins or queries – which are designed to collect unique pieces of data from specific devices.

Identify Who to Alert

Once you begin gathering statistics from your equipment a thoughtful procedure for sending and responding to alerts becomes a critical part of the success of your monitoring program. You'll want to set-up the threshold, schedule and mechanisms for alerting within the network monitoring software, as well as training personnel on how to respond.

Identify Flow Exporters

NetFlow exporters are like traffic counters on a highway. They report on the traffic flowing through them. Consequently, you should configure your routers and switches to export flow records at the major points in your network; your external network connection, backbone switch, etc.

Enable Data Analysis

Be sure to activate charts or create reports for data on which you want to analyze historical trends, or real time network activity. Keep in mind, some monitoring solutions require the administrator to separately install or turn on a database to capture this information.

Conclusion

Having the above information at your fingertips will streamline the deployment process of your network monitoring system. Don't worry if every piece of information is not available for the initial software set-up. Do what you can to get network monitoring, mapping and alerting up and running. A good system will allow you to refine your decisions later, as you learn more about your network and how it is best monitored.



66 Benning Street, Suite 7
West Lebanon, NH 03784 USA
877.276.6903
info@intermapper.com

www.intermapper.com

ABOUT DARTWARE

Dartware is a leading developer of network monitoring, mapping and alerting software. Our flagship product, InterMapper® is an easy to configure and fully featured management tool. It is integrated with a reporting package, a Layer 2 discovery module and a robust NetFlow analyzer. Available for major operating systems, these innovative tools earn quick return-on-investment by proactively notifying administrators to potential hardware, software and bandwidth issues that could cause business interruptions. Powered by an extensive library of probes, its color-coded maps and graphical reports provide a real-time view of any device on the network. More than 25,000 IT professionals worldwide use InterMapper as a cost-effective way to maximize network uptime.