

Five Tips For Getting the Most Out of Your Network Management System

Monitoring and managing network devices can be challenging, but it shouldn't require a computer science degree or weeks of training to use a network management system (NMS). In order to get the most from yours (whatever NMS you use) just be prepared to put a little thought into tuning your system using these tips to improve the quality of your monitoring efforts and reduce licensing costs.

Tip 1: Only monitor devices you really care about.

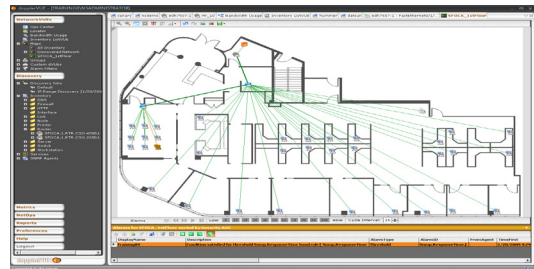
Be sure to review the inventory list discovered by your NMS. Remove from the list any devices that your team does not manage or that you probably would not respond to if a failure occurred. You may be tempted to keep these "just in case," but they can clog your database, slow your system and make it harder to see more important issues. This can even save you money, since most vendors charge by the number of devices your monitor.

Tip 2: Reduce the number of SNMP community strings.

Networks that have a large number of SNMP community strings will take more time in discovery, often much more time since discovery systems must test each community string and timeout before moving on. It's a common problem since strings frequently get added whenever a new Network Engineer joins the team. A better option is to create a uniform policy with no more than one SNMP community string for each type of device. For example, you could create a unique community string for Routers & Switches, Security Appliances and Servers. If you need additional security, consider SNMP v3 or use the SNMP security feature on most devices to block SNMP requests from unknown destinations.

Tip 3: Use visual aids.

When appropriate, use a floor plan or geographical background image as part of your network map. Network layouts become more tangible and you'll recognize devices and where problems or bottlenecks are occurring more quickly.



Tip 4: Implement a standard naming convention for your network.

Use a naming convention that is readable and that can grow with your network. It may seem hard to go back and change all devices now, but recognizing those elements will become much easier in the future. Try something like this:

```
<Citystate>.<location#>.<devicetype>.<vendor>.<model>.<#> SFOCA.1.RTR.CSO.4500.1
```

Which, in friendly terms, means: the San Francisco California, Site 1, router, cisco4500 #1. Now you'll know right away where the problem is and on what device. In addition to being clearer, these types of conventions are scalable. Even though you may not support multiple sites or cities today, you'll be ready when your organization grows.

Tip 5: Set rules and alerts.

Red lights and green lights are fine for showing the hard up/down status of devices, but there are many states in between. Take some time to understand normal performance levels in your network, then tailor the rules of your NMS accordingly. It will pay off if you can be alerted when conditions start to deteriorate and may allow you to respond before customers experience a problem. For example, monitor the Interface utilization of end users or the switch ports they are on. If a user switch port is at 70% utilization, you may want to be alerted of the high bandwidth consumption. On the other hand, bursts above 70% may be normal for your users, so that type of rule would cause an excessive amount of false positives. Instead, some systems will let you set alerts only when the Interface utilization stays above 70% for an extended period, say 30 minutes. dopplerVUE users can go even further and set rules to be alerted when the average Interface utilization is above 70% for the last 30 minutes. Using the average provides coverage in case the user has traffic dips that temporarily go below the 70% mark.

About dopplerVUE

dopplerVUE brings powerful network management features once available only in enterprise-grade solutions to networks of almost any size. **For more information about dopplerVUE visit www.dopplerVUE.com or call (888) 388-3669.**