SPONSORED BY

InterMapper

GEEK GUIDE

Finding Your Way

Mapping Your Network to Improve Manageability

LINUX™ JOURNAL

Table of Contents

BILL CHILDERS is the Senior Development Operations Manager for a mobile device management company. Bill has worked in IT and DevOps since before the DevOps term was coined, and he has performed a variety of roles in software organizations: systems administrator, technical support engineer, lab manager, IT Manager and Director of Operations. He co-authored *Ubuntu Hacks* (O'Reilly and Associates, 2006), and has been a Virtual Editor of *Linux Journal* since 2009. He's spoken at conferences, such as Penguicon and LinuxWorld, and is enthusiastic about DevOps, IT and open source. He blogs at http://wildbill.nulldevice.net and can be found on Twitter at @wildbill.

GEEK GUIDES:

Mission-critical information for the most technical people on the planet.

About the Sponsor

The HelpSystems Solution for Network Monitoring

InterMapper: Comprehensive Network Monitoring, Mapping, and Alerting Software

HelpSystems has more than 30 years of experience creating IT management software that expertly solves business problems with elegant solutions. Part of the HelpSystems family of brands, InterMapper is an easy-to-use network monitoring, mapping, and alerting software that's powerful enough for the enterprise but affordable enough for small-to-medium-sized businesses. InterMapper starts by auto-discovering every IP-enabled device in your network and helps you create maps that display real-time statistics on each one. InterMapper can monitor your devices for everything from response time and bandwidth utilization to temperature and packet loss. If a threshold appears to be exceeded, InterMapper can alert you to this possibility before it may cause larger problems. With InterMapper, you have real-time, in-depth knowledge into the health of your network, and the peace of mind that you'll always be one step ahead of costly network outages or slowdowns.

Finding Your Way

Mapping Your Network to Improve Manageability

BILL CHILDERS

Introduction

Networking has come a long way since its beginnings. In the early days of computer networks, an average business' deployment may have had a couple hubs and maybe a router if it connected to a wide area network or the Internet. Today, however, the complexity of the

typical business network has increased many times, in no small part due to the price of computer equipment dropping and the proliferation of smartphones and tablets into the enterprise. As a result, having a solid idea of what's running on your network at any given time has become a top priority for network engineers and IT staff, and having an accurate, up-to-date network map is a huge part of that.

A topographical map of your networking environment is critical to staying on top of your overall network and system health. In the same way that a road map can help you find your way as you drive a car, a network map will help you and your team plot your way around design issues. A good map will help you spot early signs of trouble before they become problems, and it will act as a great reference document for your staff—both old hands and newcomers to your team.

What Is a Network Map?

A network map, in its simplest form, is a diagram of your network and each device attached to it. It should include not only switches, routers, firewalls, VLANs and access points, but also hosts on the network. Traditionally, these network maps were made by network and systems administrators using tools like Visio. The issue with making maps like this is that manually generated maps quickly fall out of date and generally don't include clients on the network, due to the dynamic nature of client systems (laptops, phones and tablets) constantly joining and leaving the network.

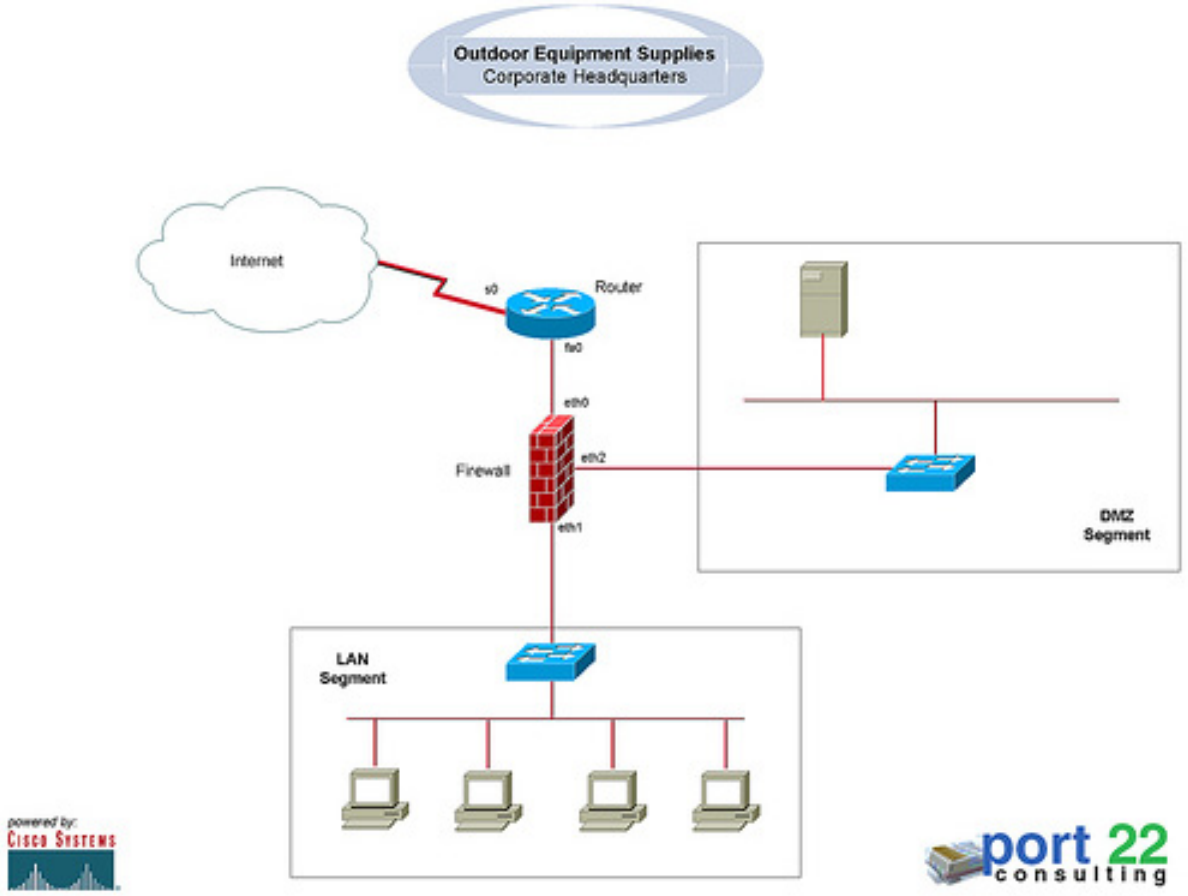

FIGURE 1. A simple, manual network map.

Why Bother with a Network Map? Building a manual network map for a modern, complex network can be time consuming, however, and because it's out of date nearly as soon as it's finished, many organizations don't even make one. However, *not* having a network map can cost your team a lot more time than it takes to make one.

In the past, I have stepped into management roles at several companies that either didn't have a network map or had an inaccurate and out-of-date map. Invariably, each time this happened, there was some kind of

issue that became much harder to track down and troubleshoot due to a lack of overall understanding of the network and its topology.

The best (or worst) example of this that I can recall was when a company I worked for was having intermittent DNS issues. The company hosted its own Internet-facing DNS servers, as well as the main application for the company. At one point, DNS resolution for the domains that we hosted began to fail—intermittently. However, the DNS servers worked just fine when they were queried from inside the network, behind the firewall. Connections that originated from outside the network and traversed the firewall were the ones that had issues—they'd timeout and fail, but at random-seeming intervals. After more than a week of suffering through these issues in production and losing revenue over it, we finally tracked down the culprit. The DNS servers were behind a pair of load balancers, and one of the load balancers was beginning to fail. None of us realized that the DNS servers were behind the load balancer—figuring that out and testing the load balancer would have been trivial if we had had a network map. A map could have reduced the discovery time from a week to less than a day, saving the company countless dollars in possible lost revenue.

Automated Network Mapping

As I stated above, having a current network map is a huge benefit to your organization. Although you can get away with making a static, manual network map, there is an easier

While a software solution like InterMapper provides both network mapping and monitoring, it can also be used to complement other network management products to improve your overall reach and network monitoring experience.

way. Network mapping software, such as InterMapper from HelpSystems (http://www.helpsystems.com/intermapper), can automatically create a network map and keep it up to date for you, so that you and your team can spend less time documenting the network and more time improving the infrastructure and executing on projects.

Network Mapping and Network Monitoring: While a software solution like InterMapper provides both network mapping and monitoring, it can also be used to complement other network management products to improve your overall reach and network monitoring experience.

Where a network monitoring system typically works by polling each device for operational status and other statistics, a network mapper focuses on the way the devices interact and interconnect. More important, the network mapper will watch the network continually and notify you and your team of changes in the environment.

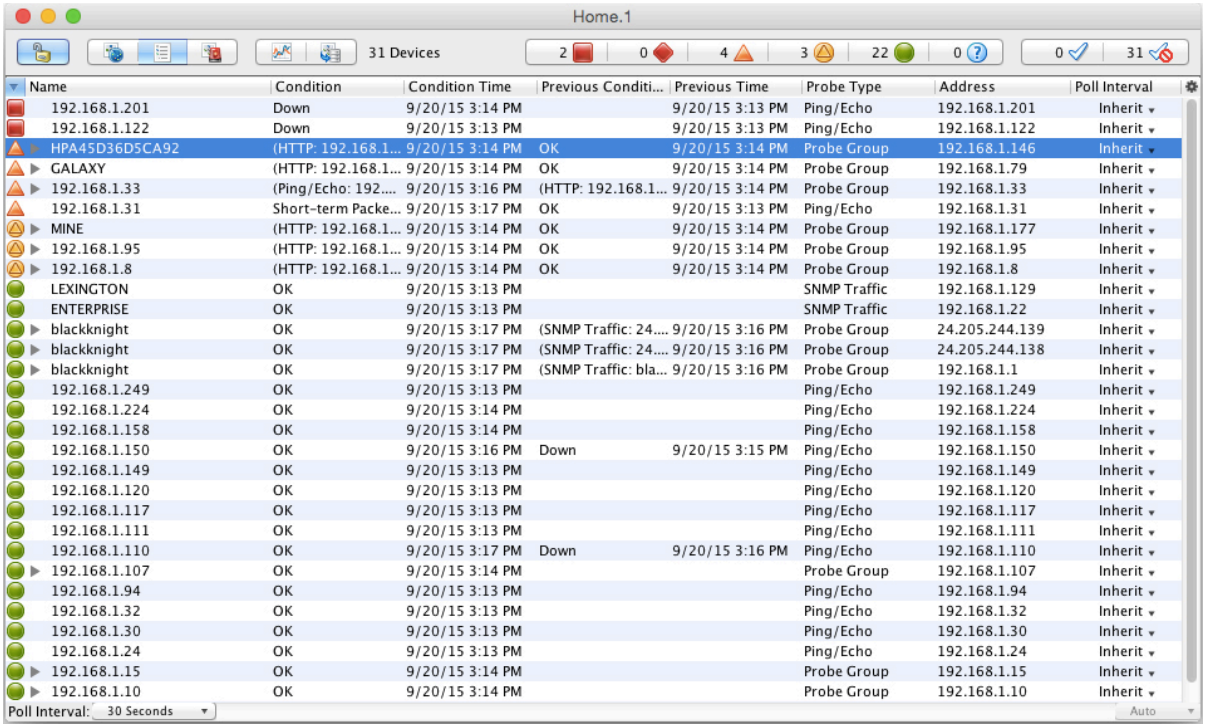

FIGURE 2. **InterMapper doing its thing! (Wow, I have a lot of devices at home.)**

One of the great strengths of a network mapping tool is its ability to draw links between systems and keep them up to date automatically. The map shown in Figure 3 is the same data presented in the table shown in Figure 2, but it's drawn automatically by the mapping tool and kept up to date. Here you can see quickly that all of these devices reside in the 192.168.1.0/24 network, for example. A picture is worth a thousand words, and having a solid picture of your network at any given time will give you and your staff a better understanding of the network, the hosts that reside in it, and how all the pieces interconnect.

Autodiscovery

Wouldn't it be great to have your network map just made *for* you, without tying up you or your team's time? A solid network mapper can do that for you! Intelligent network mapper tools can "walk" your network, not only pinging hosts, but they also can do port scans of them and see what services are running on each host. In some cases, you can feed SNMP, SSH or WMI credentials to these tools, and they will add the information they pick up from each host to the map, creating a much richer informational context that gives your team even greater visibility into what's going on at any given time.

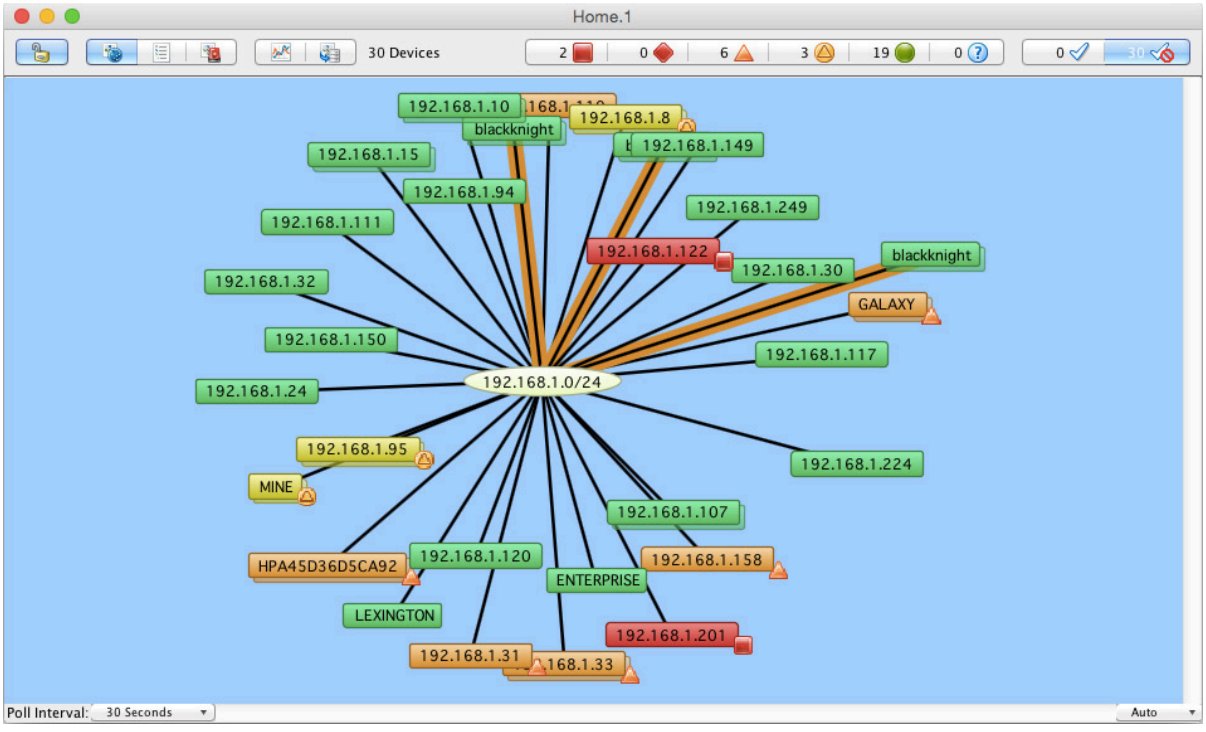

FIGURE 3. A very basic, but automatic network map.

Where a conventional network monitoring system generally alerts you only in the case of trouble with a host, a network mapper can alert you as a threshold begins to be reached, so you can take action to fix issues before they turn into problems, thereby preventing network outages and downtime.

Since the network map is constantly being updated by the tool as services are brought on-line, your team stays notified and aware. This is a great benefit—in the event a rogue operator makes it into your network and starts a service, like a Web server, mail server or file-sharing server—you can be notified, investigate and take appropriate action.

Network Mapping Is Proactive Monitoring

Network mapping tools are great at helping you and your staff get ahead of the curve and be proactive. Where a conventional network monitoring system generally alerts you only in the case of trouble with a host, a network mapper can alert you as a threshold begins to be reached, so you can take action to fix issues before they turn into problems, thereby preventing network outages and downtime.

Capacity Planning

Capacity planning can be a daunting task at times. In

order to plan for the future correctly, you've got to know where you are and the state of your network and systems today—and this is another place where an accurate and up-to-date network map shines. Without a network mapper, in order to plan for the future, you have got to take a global assessment of your network—manually. This is a tedious, time-consuming process, and it can tie up your staff, keeping them from implementing new projects. Once you've got a network map, capacity planning can be as simple as running a report, looking for the usage trends across your network and extrapolating what pieces need upgrading, and how much. Tools like InterMapper can provide access to the data, and capture and parse that data in an external program with minimal effort.

Monitoring

A static, manually generated network map doesn't give you one of the biggest advantages that a tool like InterMapper can provide: real-time monitoring and alerting of changes in your network, as they happen. A good network mapper can act as your watchdog on the network, keeping an eye out for anomalies and reporting them to you in real time, as they occur.

If you have to maintain maximum uptime, you simply can't have too much monitoring. A network mapper fills the gaps that an ordinary network management and monitoring system has, giving you a 360-degree view of your entire network deployment. Proactive monitoring is the key to maintaining uptime—being on top and aware

of situations before they become problematic will allow you to maintain the highest possible service level for your organization.

Speaking of service levels, do you have service-level agreements (SLAs) that you need to maintain? Usually not meeting those service levels results in credits to your customers, which means a loss to your business. Naturally, you and your staff want to prevent that situation from occurring, and a network mapping package is another tool in your toolbox to achieve that end. A good network mapper can keep an eye on your systems, switches, routers and interconnects, and warn you at a predetermined level *before* you saturate your capacity. Although this ties into capacity planning, it also allows you to maintain your service levels, keeping upper management happy and avoiding fire-fighting operational issues for your staff.

And, with respect to fire-fighting, we all face an ever-looming threat: external intrusion by malicious operators—in other words, attackers. Having that 360-degree view of your network helps you shine a spotlight on malicious activity when and where it occurs. Tools like InterMapper can help you establish a baseline level of activity for each device on your network, and then alert you when devices deviate too far from the baseline. In addition, a network mapper can monitor the flow of traffic in and out of the network, using NetFlow or sFlow protocols. This adds to the overall 360-degree view, giving you and your team insight not only into the state of devices on the network, but also the data those devices are transmitting and the destination of that data.

Troubleshooting

When the fire has broken out, and the chips are down, you need every tool you can have at your disposal, ready to go and provide information. Troubleshooting a problem on a complex network today requires that you have both a high-level picture of what's going on in the entire system, as well as a low-level view from each host and device. A network mapper, in conjunction with other tools, can give you that perspective, letting you hone in on issues and resolve them quickly.

Earlier in this ebook, I described a real-life troubleshooting situation where the time to resolution of that problem could have been dramatically reduced by having a solid network map and mapper tool—and that 360-degree view of the entire network. When your team is forced into troubleshooting and fire-fighting mode, situational awareness is critical. Analytical troubleshooting techniques, applied correctly, can reduce the problem space by half every time you iterate through the issue, but *only* if you have good information upon which to base your decisions and troubleshooting direction. That's why having an up-to-date network map and good tools is so critically important. It can keep you from heading down a troubleshooting dead end and forcing you to retrace your steps back to an earlier point, thereby beginning the process over again.

Minimizing time to resolution and restoring service to expected levels is what it's all about when you're in troubleshooting mode, and tools like InterMapper

Minimizing time to resolution and restoring service to expected levels is what it's all about when you're in troubleshooting mode, and tools like InterMapper give you the information necessary to zero in on issues and drive them to completion.

give you the information necessary to zero in on issues and drive them to completion.

Conclusion

Any team responsible for maintaining network health and performance needs every possible tool that will provide a comprehensive view of the network. Monitoring, capacity planning and troubleshooting activities all benefit greatly from the use of a network mapping tool like InterMapper. Whether you manage a large enterprise network or a smaller network, the benefits of having a network map are clear for you and your team. Your team members will thank you for implementing a mapper, because they'll get better information and can respond more appropriately, and management will be pleased when SLAs are maintained and predictable capacity planning and growth can be projected. Every network deployment can benefit from having a tool like InterMapper in its toolbox.■