Realtime publishers

The Shortcut Guide™ To

Smart Network Management for the SMB

sponsored by

IPSWITCH WhatsUpGold
Network Management Software

Chris Hampton

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: The Power of Intelligent Network Management through Discovery and Mapping

You are the owner of a new up-and-coming small business. After a long weekend of mapping out the final touches of your new marketing campaign, you enter the office with a sense of completion. You ask yourself, "What could possibly go wrong?" Before taking your first sip of coffee, you receive an urgent email from your marketing director stating that the company's new Web site is not responding. You promptly head over to IT and find your senior network administrator frantically rebuilding the configuration on the network load balancer—it seems the new network admin applied the wrong patch and did not save the configuration during Friday's upgrade.

It is later in the afternoon, and your Web site is up and running again. However, it is too late, the damage has been done. The new ad campaign ran, despite your marketing director's attempts to pull it from today's broadcast. Your receptionist tells you that she has been receiving a number of calls from customers complaining about the availability of the advertised Internet coupons. These same customers voiced concern over the reliability of your products—based on their experience accessing your Web site.

What went wrong and how can small and midsized businesses (SMBs) avoid these same pitfalls? Network management, and more specifically *smart network management*, can be the deciding factor. Through the selection and implementation of a smart network management solution, SMBs can gain the needed insight into network performance to proactively monitor the devices and systems within the network to avoid scenarios like the earlier example. Over the next four chapters, we will review the underlying features and benefits that a smart network management solution can provide.

Why Do SMBs Need Network Management?

In today's economy, large corporations are demanding more from their investment in information technology, and SMBs are no different. As an SMB owner, you have to keep an eye on the bottom line while *ensuring you are providing key innovations* that set your business apart from the competition. Often, information technology becomes that distinctive innovation, and your business' ability to efficiently manage and utilize a given technology can mean the difference between gaining market share and becoming yesterday's news.

Network management allows an SMB to efficiently control and monitor the network, which is the very foundation of the business' information technology. Stop for a moment and think about the importance of the network in relation to your business; email, order processing, Internet access, and critical communications with customers and partners represent the heart of your business operations. In fact, it is difficult to imagine your business operating without the use of technology tools such as these.

Your network is made up of a diverse set of technologies: devices such as routers and switches, server infrastructure systems such as Windows and Linux hosts, and critical business applications such as messaging and database applications. All of these technologies provide some level of management at the individual component level, but the real empowerment comes from the centralization of network management and broad visibility into each technology. A business that understands how to manage these technologies and how to provide optimal performance across all devices, systems, and applications has moved from simple network management to *smart network management*.

Consider the scenario presented at the beginning of this chapter; if this same business had previously implemented a *smart network management* solution, the unresponsive Web site could have been proactively detected. In addition, the failed upgrade of the network load balancer would have been quickly recovered by restoring the last known good configuration from a central device configuration backup.

What are the consequences of ignoring the need for a network management solution? The cost to an SMB is visible across many levels of the business from loss of sales and corporate or product image decline to loss of customers and an increased cost of supporting the network due to reactive troubleshooting. Take a look at how this network downtime affected a number of SMBs that were surveyed in 2007.

The data represented in Figure 1.1 was collected from a 2007 survey, sponsored by The Strategy Group, that included 173 SMB respondents from the Ziff Davis Enterprise database. The survey highlights the consequences of network downtime to an SMB. .After reviewing the data in Figure 1.1, the surprising conclusion is the large effect of downtime to loss of customers and decline in corporate image compared with the financial loss experienced. This shows the importance of minimizing downtime, as the effect to the business can be very broad.

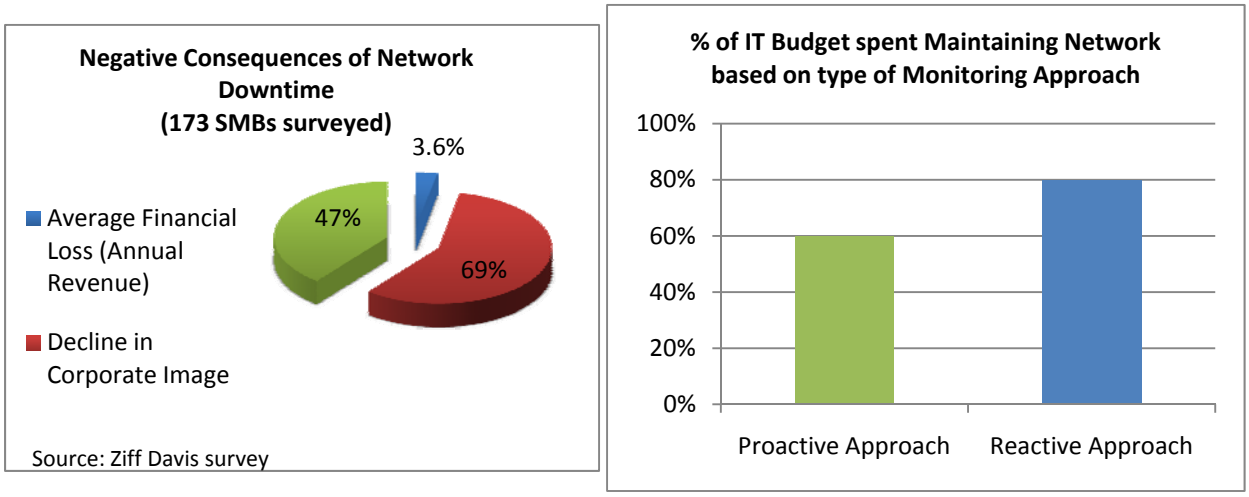

Figure 1.1: SMB survey data regarding network management.

The survey data also indicates that those SMBs that take a *proactive approach* to network monitoring versus a *reactive approach* see a significant reduction in IT spending. If you take a step back and look at this data from the perspective of an SMB owner, the picture becomes clear: With rising costs and ever-shrinking budgets, your revenue margin is becoming very thin. As an SMB owner, you have to minimize the exposure a network outage can cause to your business while keeping your IT budget under control.

The second portion of the survey indicated the cost benefit to a business of implementing a proactive monitoring approach. Together, this data clearly indicates the importance of minimizing network downtime, and the cost benefit of utilizing a smarter proactive solution for the management of all network-related devices and systems. The question is, What does a smart network management solution look like and how does it work? At a high level, a network management solution should provide a set of key features and benefits:

- Complete visibility—Before a business can manage the network, you first have to understand what devices, systems, and applications are on your network. Intelligent discovery and mapping is key to having the required visibility into your network.
- Sophisticated monitoring—To truly provide a proactive response to network issues, you need a solution that offers both active and passive monitoring. Simple ping test and Simple Network Management Protocol (SNMP) polling are fine for availability and fault management, but preemptive alerting of network device changes takes network monitoring to the next level.
- Integrated configuration and change management—Your network has many devices each with its own configuration files and passwords. A network management solution should provide the ability to centralize the management of these configurations and automate required changes.

- Real-time troubleshooting, trending, and traffic analysis—This is where the smart in smart network management really pays off. By providing a solution that enables the business to proactively detect and resolve network-related issues, user interruption and critical business loss will decrease dramatically. Add to this the capability of historical trending of system and application performance, and you have a powerful network management solution.

Together, these four high-level features form the foundation of a smart network management solution, as Figure 1.2 shows.

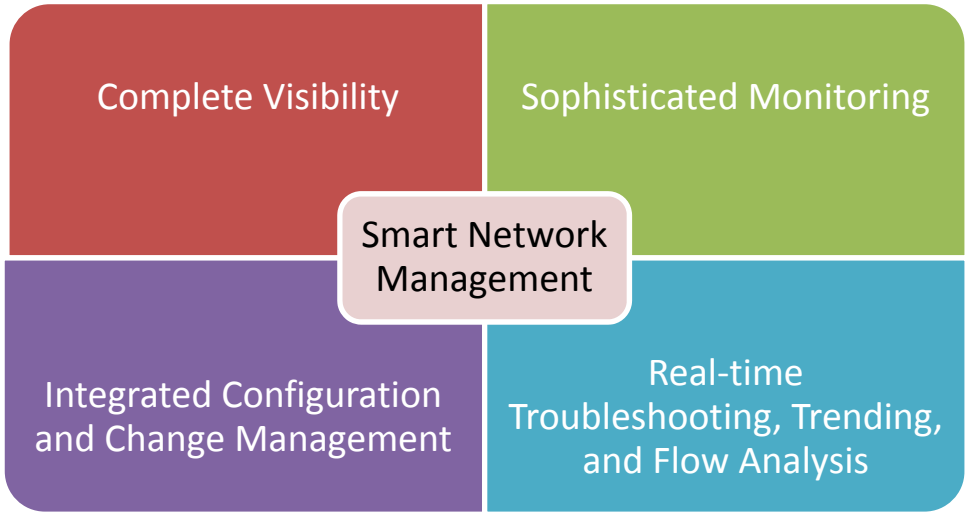

Figure 1.2: Foundation of a smart network management solution.

Let's break down each of these key features by starting with a detailed look at what is behind the desire to have *complete visibility* of the network.

Network Discovery

Before any monitoring, configuration management, or troubleshooting of the network can occur, you must have knowledge of the devices and systems that reside on your network. The importance of having complete visibility into the network cannot be stressed enough. No matter how good the network management solution, if you do not know the device or system exists, you cannot manage it. When looking at network management solutions, the first feature you should focus on is network discovery.

> **Note**
>
> Often overlooked are the prerequisites to a successful network discovery process. These include enabling key protocols such as SNMP and standardizing on the SNMP credentials across all network devices (including read community strings for SNMPv1 or SNMPv2 devices and SNMPv3 device usernames and passwords). Smart network management solutions incorporate a credentials library, which allows for centralized management of SNMP credentials across all devices.

Types of Discovery

The power of a smart network management solution lies in its ability to utilize multiple types of discovery methods. Basic network discovery begins at Layer 2 and Layer 3 of the OSI model—devices at these layers are responsible for providing reliable transit of data across physical links and routing of packets across the network.

Network management solutions must incorporate IP discovery protocols such as:

- Internet Control Message Protocol (ICMP)—This discovery protocol tests the IP address' active state and responsiveness.
- Address Resolution Protocol (ARP)—This low-level request and answer protocol is used at the Media Access level.
- SNMP—This protocol allows discovery of detailed device information from each SNMP-enabled device.

Smart network management solutions should also incorporate advanced methods of discovery such as

- Link Layer Discovery Protocol (LLDP)—This vendor-neutral protocol is used by network devices for advertising their identity.
- Proprietary vendor protocols such as Cisco Discovery Protocol (CDP) or Microsoft's Link Layer Topology Discovery (LLTD)

> **Note**
>
> The use of vendor protocols such as Cisco CDP and Microsoft LLTD provide a richer set of Management Information Database (MIB) attributes for the specific device. These advanced vendor-specific discovery protocols should be used in place of a general LLDP discovery if possible.

These advanced methods of discovery interrogate the device's MIB files and gather extensive information that helps build a complete picture of the network. Network vendors provide management information base (MIB) files with each of their hardware devices. A MIB is a type of database used for managing devices in a communications network. It comprises a collection of objects in a (virtual) database that can be used to manage entities (such as routers and switches) in a network.

One example of the use of these advanced methods is the ARP Cache discovery method. This discovery method is highly recommended due to the ability to utilize SNMP information from multiple network devices—it also incorporates the use of proprietary discovery protocols like those discussed earlier.

One remaining element of many SMB networks that cannot be overlooked is the *virtual machine layer*. Virtualization is one of the hottest technologies in the industry and many SMBs are taking advantage of this technology to dramatically reduce the number of physical servers in the data center. Market Research firms such as IDC and the Gartner are predicting rapid adoption of virtualization in the SMB space over the next few years. In a Gartner report from October 2009, Gartner analyst Tom Bittman stated "that SMB adoption of virtualization will drive growth in the virtualization space for the foreseeable future, resulting in more than 50 percent of workloads running on virtual machines by 2012." As more businesses port their server architecture to a virtual infrastructure, it becomes critical to have visibility into the virtual machine layer.

Smart network management solutions incorporate discovery at the virtual machine layer using protocols such as VMware's Virtual Infrastructure Management (VIM) or VMware's vSphere API structure. By utilizing SNMP v3 or SSH credentials, a secure connection can be made from the Network Management System (NMS) to the base ESX hypervisor and discovery can occur at all critical layers within the virtual infrastructure: base hosts, virtual switches, virtual appliances, virtual machines, and guest operating systems (OSs) as Figure 1.3 shows.

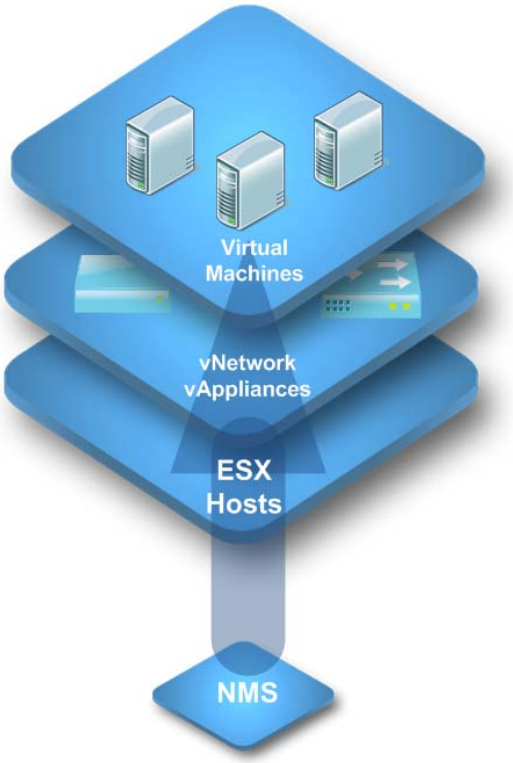

Figure 1.3: VMware (VIM) discovery.

The individual protocols and discovery methods discussed thus far are powerful in their own right. Team these with the ability to build a complete network picture through relationship mapping of each device, and you have yourself one very powerful network discovery solution. What is relationship mapping? Think of a discovery solution that can incorporate Layer 3 device and application mapping with detailed Layer 2 port-level relationship mapping. Now add to this the ability to gain visibility all the way down to the individual port level connectivity of each router, switch, and server interface on your network and you will begin to see the power behind this type of solution.

Power of Scheduled Network Discovery

If you think of network discovery as a one-time task that is undertaken when building out a network management solution, you are missing the boat. The real power in the use of network discovery tools comes in the ability to incorporate these tools on an ongoing basis. By scheduling a reoccurring network discovery, you will maintain a living picture of your network environment.

Your network is in constant motion: new devices and systems are added, existing systems are moved from one subnet to another, live migrations of virtual machines occur more regularly and older or obsolete devices are removed from the network. You need a way to keep track of these changes and ensure your monitoring is as accurate as possible. Tracking these changes is the goal of a scheduled network discovery.

When a new device comes on the network—let's say through a vendor demo or proof of concept project—you will immediately be aware of the device and have the ability to map the connectivity, establish monitoring, and manage the device. Equally important is the ability to know when a device or virtual machine is removed from the network. To ensure updated monitoring, and to maintain an accurate overview of the network status, device additions and removals must be captured.

Network discovery encompasses a wide variety of technologies and methods. When evaluating network management solutions, ensure that *network discovery* tops your list of important features. A rich set of discovery tools will give you peace of mind in knowing that you have a complete picture of your environment, and will bring you one step closer to achieving *complete visibility* of your network (see Figure 1.4).

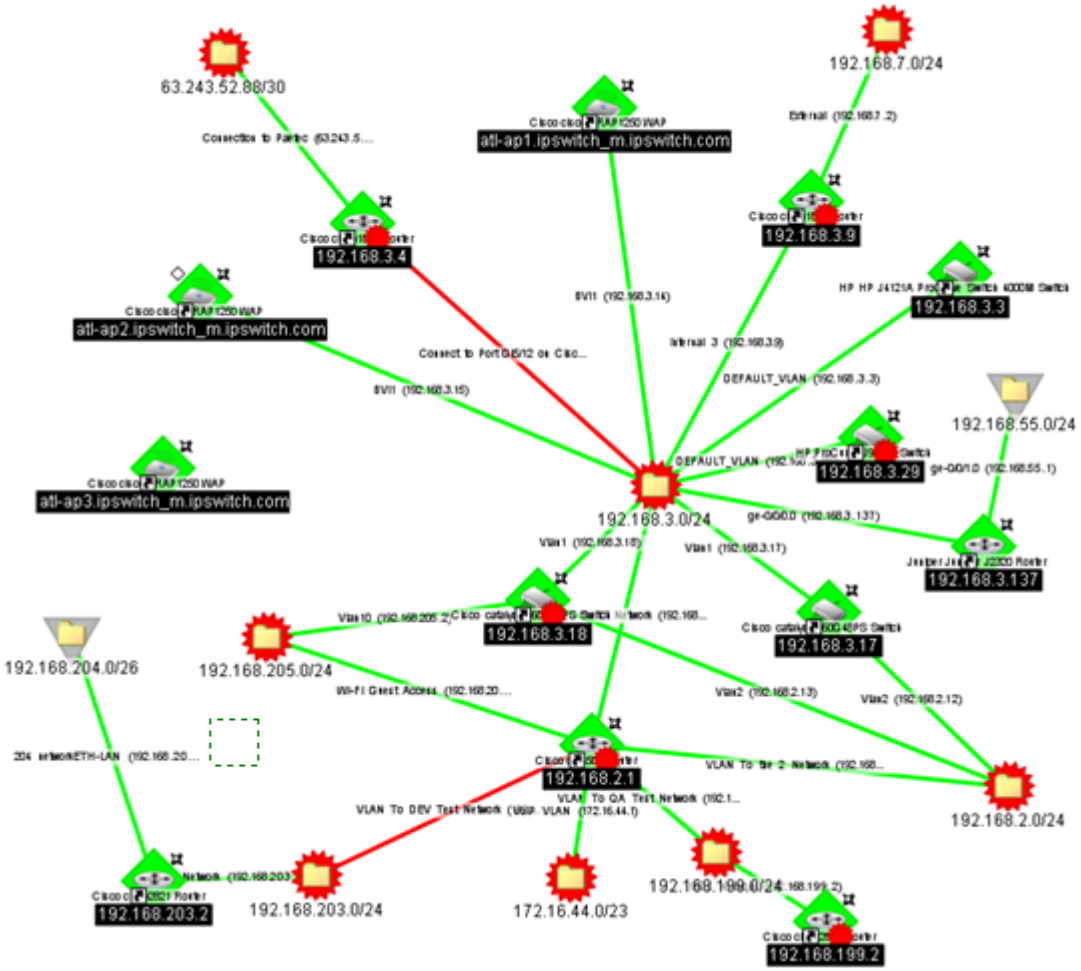

Figure 1.4: Smart network management solutions offer a rich set of discovery tools to accurately identify, map, and represent your network—devices, interdependencies, and locations.

Network Mapping

When Google released Google Maps in 2005, they provided a rich mapping tool that could be used to quickly locate business and residential addresses at the click of a search button. Just like those old paper maps we all have in our glove compartments, Google Maps helped us understand a specific location in relation to a larger geographical context. Google Maps provided us with a wealth of information about our chosen location: hours of operation, points of interest, and local phone numbers, to name a few. Most importantly, a detailed route to our location was provided showing us how to get from point A to point B.

Think of your network as a vast land of locations—let's call these devices. When it comes to network management, you need a tool much like Google Maps that can provide a location-based context for your devices. You also need quick access to each device's discovered information, such as type, manufacturer, model, CPU, memory, and so on. Finally, you need to understand how each device is connected in order to develop a complete context for your network. In network management, we call this process *network mapping*; it is critical to understanding your network.

Creating Topology Maps

When looking for a network management solution, SMBs must focus on those tools that provide the ability to create detailed network topology maps. Network administrators are being asked to do more with less in today's economy; with so many resources vying for their attention, they need tools that provide a comprehensive view of the network with minimal effort to create. Smart network management solutions incorporate the ability to port the data, from the discovery tools and methods discussed earlier in this chapter, into a detailed hierarchical map of the network.

Remember, within our discovery data we captured full addressing information for each device and system as well as the connectivity between each device at the subnet, virtual LAN (VLAN), and port level. This rich data set when ported into the network mapping tool becomes a detailed network map containing a complete and accurate representation of the live network and application environment.

Once the topology maps are created, they become a central point for visibility into the network. These maps also allow the network administrator to dynamically drill down into specific subnets and VLANs for additional management. Network mapping tools should also provide the ability to drag and drop discovered devices within the map in order to update device positions or create additional relationship mappings. Gaining visibility into the network by using a *visual representation*, such as a topology map, allows the network administrator to quickly see what is happening and how each device and system is inter-related. This ability reduces the amount of time needed to troubleshoot issues and helps the network administrator become more proactive.

Power of Auto-Created Mapping

As great as network topology maps are, if it takes a lot of effort to create these maps, the value is diminished over time because the maps will age and the data will become irrelevant. That's where auto-creation comes in. Smart network management solutions must have the ability to integrate the captured network discovery data into the mapping process with little effort. By utilizing a topology mapping tool, within the network management solution, the discovered network data can easily be exported into other network management tools or documentation applications. This enables the network administrator to auto-create topology maps and detailed hierarchical views in a short amount of time.

Earlier, the power behind scheduled network discovery was discussed; this process becomes even more powerful when combined with the auto-creation mapping feature. With this powerful combination, network administrators can keep critical network maps updated and truly rely on them for accurate visibility into the network.

Adding to these processes, smart network management solutions provide the ability to intelligently match the discovered devices with a prebuilt library of role-based templates such as routers, switches, Web servers, and email servers. Role-based templates provide an accurate and less time-consuming method for developing a network topology map of your environment, allowing critical monitoring to be up and operational in a much shorter timeframe. Finally, support for porting of the detailed auto-created Layer 2 topology maps directly into the integrated monitoring software allows for rapid deployment. With all of this, the network administrator has more than a detailed, accurate network topology map with dynamic drill-down capabilities; the administrator also gains a real-time visual troubleshooting tool that provides full monitoring and alerting of all discovered devices and systems within a single pane of glass.

At this point, full addressing and connectivity discovery data has been captured and auto-creation tools have been utilized to produce a detailed network topology map. However, you may be wondering, "Where is the *smart* in the smart network management solution?" The real intelligence in these network management solutions lies within the deep integration between features. Chapter 2 of this guide will explore the breadth of network monitoring, but you can already begin to see how the integration of discovery and mapping build a foundation for an intelligent network monitoring solution.

Relationship Mapping and Layer 2 Visibility

Relationship mapping was discussed earlier in the chapter, but let's take a closer look at this process and focus in on the key benefits. Think back to the Google Maps analogy—when we need to travel from point A to point B, we need to understand the route to follow. Within network management, relationship mapping is the tool that provides route information between devices and systems. With the ability of a smart network management solution to provide visibility at Layer 2 down to the individual port level, intelligent network topology maps can be created with detailed connectivity routing.

The immediate benefit of this ability is visibility into the connectivity and routes between devices and systems. When a device or system reports a network error, the network administrator can step beyond individual device troubleshooting and look at the issue in the context of the entire network (see Figure 1.5). In our introductory example of the SMB business owner and his troubled ad campaign, had the business acquired a network management solution that incorporated relationship mapping and Layer 2 port discovery, the day may have gone much differently: Before the SMB business owner arrives in the office Monday morning, the senior network administrator would have been notified that the Web servers were not responding to an HTTP get request for the new ad campaign Web page. The administrator could have opened the real-time topology map and saw the failed load balancer appliance interface, including the visual route between the Web servers and the load balancer's virtual IP address. Proactive steps could have been taken to correct the load balancer's configuration and reestablish network communication to the Web servers all before Monday morning.

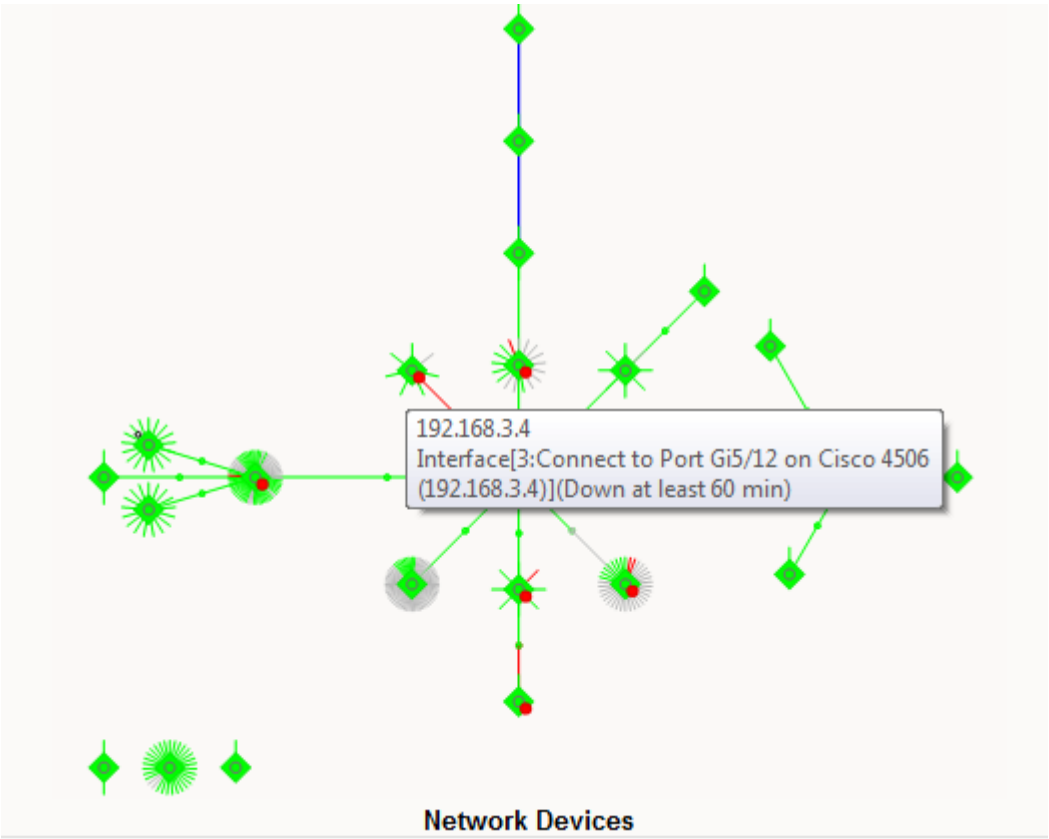

Figure 1.5: Smart network management solutions also offer a high-level view of errors and problems, so you can quickly ascertain the overall impact of a failure.

Building Device Inventories

Often overshadowed by other features such as monitoring and alerting, device inventory management is a key feature when looking for a network management solution. The goal of a device inventory management system is to have a complete, up-to-date, and accurate view of all network devices, including routers, switches, hubs, systems, printers, and software. At minimum, a device inventory management system should provide basic device class information and capture what is installed on the device through a Layer 3 discovery process. Taken a step further by utilizing a rich data set captured during additional Layer 2 discovery processes, device inventories become an integral part of the overall network management solution.

Without a network management solution, building and maintaining an inventory and asset database is a daunting task involving complicated login scripting, additional vendor software to install and maintain, and more time away from other tasks for your network administrator. Through the integrations of the device inventory management system into the overall network management solution and fully automating the capture, categorization, and reporting of all network assets, the task becomes much easier.

Smart network management solutions capture a wealth of information from every device and system on the network during the discovery process. To do so, they use SNMP queries of the device-specific MIBs and advanced discovery methods such as Link Layer Topology Discovery (LLTP). In addition, the ability to use intelligent matching against a pre-built library of vendor-specific device templates and attributes enhances the inventory management system. The following list highlights key device categories to look for in a network management solution:

- Networking devices including routers, switches, hubs, and wireless access points
- Server OSs including Windows, Macintosh, Linux, and Unix
- Virtualization infrastructures including VMware vSphere 4, Microsoft Hyper-V, and Citrix XenServer
- Printers including network printers, multifunction copiers, and plotters
- IP phones including Cisco, Nortel, and Avaya
- Power/UPS including APC, Belkin, and Liebert

Once a device or system is categorized, additional attributes are captured and tracked. When used in conjunction with *scheduled network discovery,* an automated, complete, and accurate inventory of each device and system on the network can be easily maintained.

Searching the Network

The usability of a network management solution is just as important as the powerful discovery tools or advanced monitoring options. Let's face it, if you have a system that can capture detailed device information including vendor-specific attributes and can track connectivity for every device down to the port level but you cannot easily interface with or use this data, then what is the point? Smart network management solutions must provide an intuitive interface and dynamic tools to interact with the captured data (see Figure 1.6).

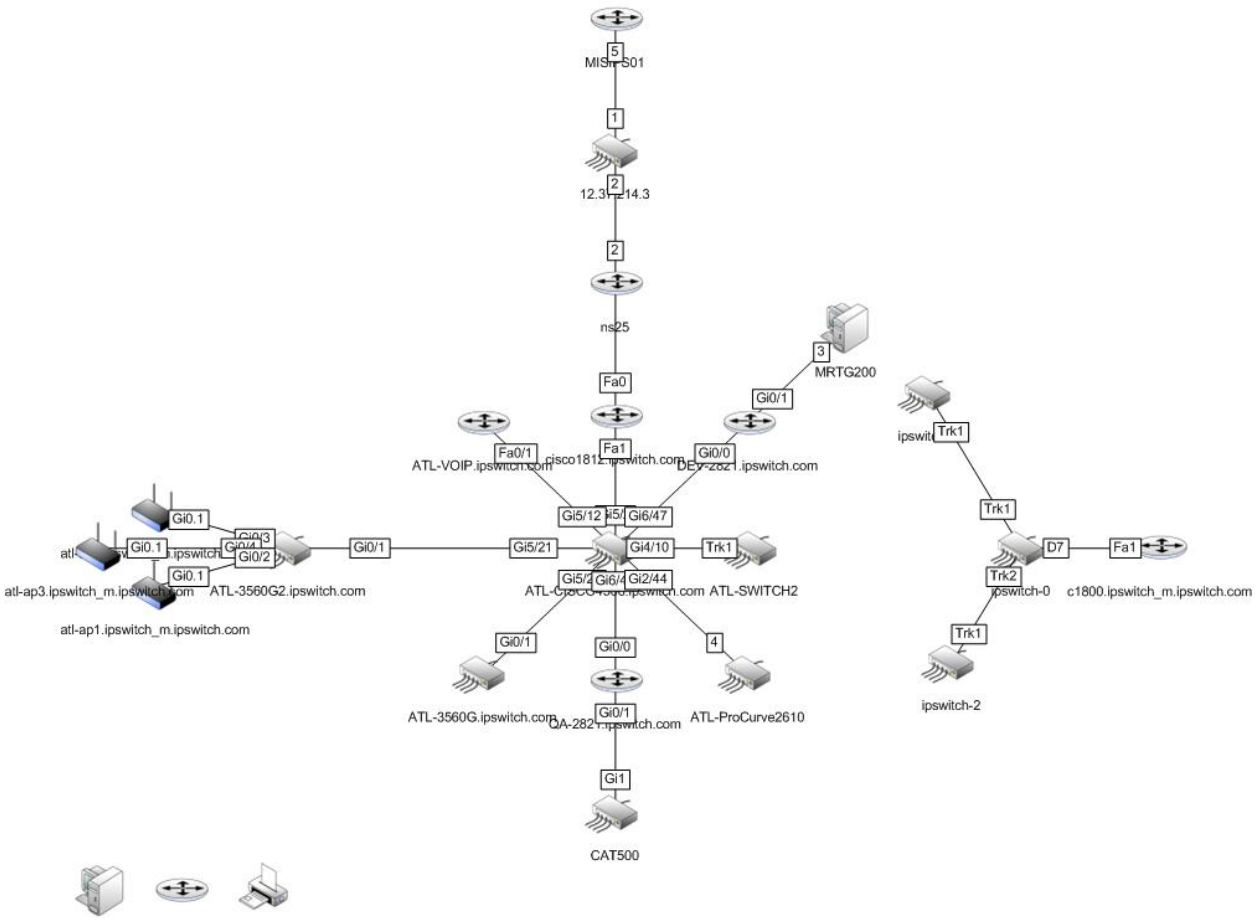

Figure 1.6: Look for a smart network management solution that will enable you to document and publish your network topology views to external applications, such as Microsoft Vision, for future use.

One key point to focus on is the ability to search the network; the network management solution must have the ability to reach into the network and quickly find specific device information and report back using an intelligent interface. Among the many search features, it is important to have wild card search capabilities for device configurations, inventory categories, and device-specific attributes. This feature simplifies the process of finding devices or systems quickly, especially in network environments that are constantly changing. Two additional search-based tools are Layer 2 traces and IP/MAC filtering. These tools provide key insight into device connectivity and addressing that can be used by network administrators during troubleshooting.

To see how these tools work in the real world, the following section offers a short troubleshooting scenario that uses the Layer 2 trace. Additionally, the IP and MAC filtering tool is highlighted for it's ability to resolve IP addressing issues.

Layer 2 Traces

Network administrators often need immediate route information between network devices when troubleshooting connectivity issues. Having a tool that provides a visual reporting of the network data path is critical. Layer 2 traces allow the administrator to input a source and destination device, by IP address or hostname, and the tool will actively trace the network path. A visual representation of the network path is displayed showing each device, IP address, and interface name along the path.

By using a Layer 2 trace, the network administrator can easily build a complete picture of the current network connectivity between devices and see in a single view the status of each point in the connection path. Figure 1.7 shows a simple network configuration between two server devices. Without a Layer 2 trace, it would be hard to see that the communication issue was a failed port on the workgroup switch on the destination LAN.

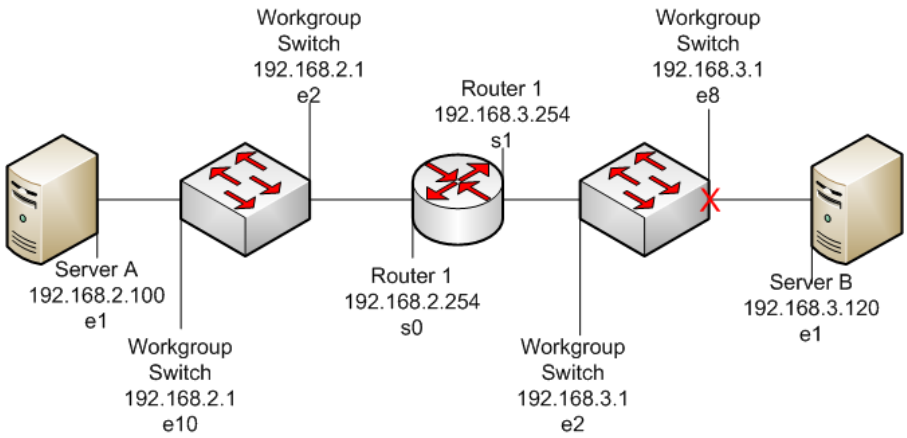

Figure 1.7: Basic network diagram.

Table 1.1 shows the output from a Layer 2 trace clearly indicating the failed switch port. This capability to quickly see the status across all connectivity points is very powerful.

Device	IP Address	Interface Name	Status
Server A	192.168.2.100	e1	Up
WGSW1	192.168.2.1	e10	Up
WGSW1	192.168.2.1	e2	Up
Router1	192.168.2.254	s0	Up
Router1	192.168.3.254	s1	Up
WGSW2	192.168.3.1	e2	Up
WGSW2	192.168.3.1	e8	Down
Server B	192.168.3.120	e1	Down

Table 1.1: Layer 2 trace report.

IP and MAC Address Filtering

Another key search tool to assist the network administrator is IP and MAC filtering. Often, within network environments, the assignment of IP addressing is not carefully managed. This may be caused by inefficient practices or shared management of large IP address ranges. This problem manifests itself in the form of duplicate IP address assignments, thus causing network conflicts as multiple devices are responding on the same IP address.

Network management solutions that incorporate an IP and MAC address filtering tool allow the administrator to query the discovered network devices and list each device that has reported associations with the specified IP address or MAC address. The returned data should include the device name, IP address, and interface name. In addition, the filter can list those devices that are currently linked to the IP or MAC address. This ability allows the administrator to quickly narrow in on rogue IP addresses and resolve network conflicts. Search tools such as Layer 2 tracing and IP address filtering enhance the network management solution, giving the administrator additional troubleshooting capabilities.

Documentation, Documentation

Documentation conjures up negative thoughts in the minds of most network administrators. Memories come rushing back of late nights in a cold data center tracing cables and logging port numbers. Those of us that have spent time working in large IT organizations understand the importance of documenting the network. Networks are becoming more and more complex, involving multiple layers of devices and systems. Having up-to-date and accurate documentation for the entire network—from edge network devices such as routers, firewalls, and gateway appliances to core server network devices such as layer 3 and layer 2 switches, and finally the systems themselves and their associated applications—is critical. Add to this the complexity of virtual infrastructures including their own switching, systems, and applications, and the importance of having good documentation becomes even clearer.

If documenting the network is so important, why do many organizations fail to produce or refresh their network documentation? The problem is that documentation is usually an afterthought in many organizations; most network administrators do not have the time to capture all the required device information, network connectivity, and relationship mapping to properly document their network. Within today's SMB network environments, there is no less complexity and the need for documentation of the network is just as relevant.

Smart network management solutions can solve this problem by addressing two core issues: discovery of network devices and documentation of the network. Let's take a look at how a network management solution solves these issues.

Automating Network Discovery

This chapter discusses the features and benefits of automated discovery of network devices. The ability to discover Layer 3 and Layer 2 devices and systems on the network has been highlighted. Also, the ability to provide a complete picture of the network by using relationship mapping and Layer 2 port-level connectivity discovery is detailed. Finally, we explored the power behind a scheduled network discovery process through which, on a regular basis, the captured network device data can be updated to account for device adds and removals. When looking at these features again from a documentation perspective, you can see how the same automated discovery process and collected data that is easily ported into detailed network topology maps can benefit the documentation process. The key here for network administrators is that smart network management solutions automate this entire process and simplify the collection of the required network information to complete their documentation initiatives.

Publishing Discovery Maps

With the ability to automatically discover a wide variety of network devices, classify these devices, and port the discovery data into highly detailed topology maps, there is only one step remaining for completing documentation. Network management solutions that incorporate the ability to automatically generate network maps or custom map views and publish these maps into popular documentation tools, such as Microsoft Visio, help achieve that final step for network administrators.

The added benefit of running scheduled discovery allows administrators to easily refresh their network documentation. They also gain insight into the impact, if any, that design changes or device additions had on the network.

Asset and Device Inventory Tracking

Another important area of documentation revolves around asset and device inventory tracking. Many businesses are under a mandate to keep close records of their computing and network resources for accounting purposes, such as depreciation tracking. As with general network documentation, the process of gathering asset information is very labor intensive if not automated. Network management solutions that provide the ability to automate the collection of asset information and then export the collected device inventory information gathered adds significant value. Through support for export to either CSV or Excel formats (see Figure 1.8), the inventory data can be easily imported into other inventory-tracking systems. By integrating the scheduled discovery process into the asset and inventory management tracking, inventory databases will be kept current and accurate.

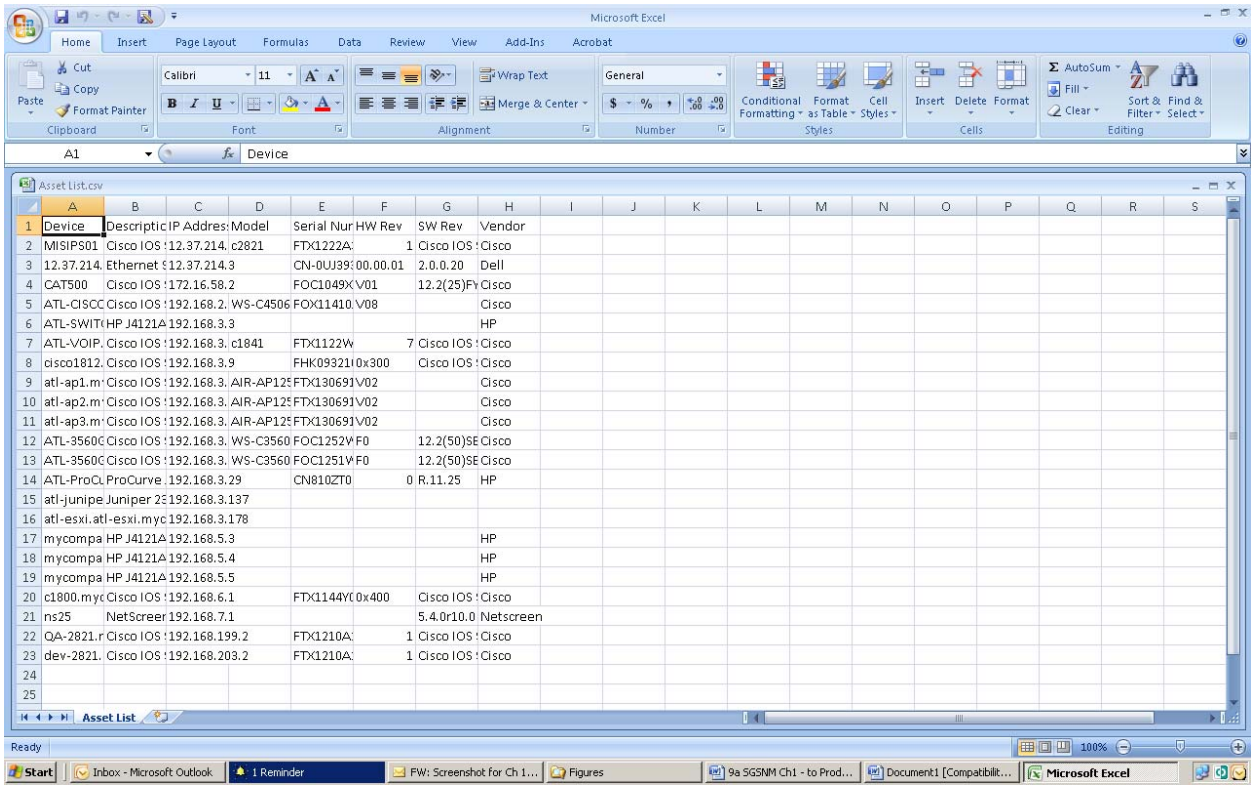

Figure 1.8: With smart network management solutions, you can collect and export network asset information in CSV or Excel formats to seamless integrate with other inventory-tracking systems.

Just as important as data collection is the data itself. If the network management solution only provides very basic information, the inventory tracking system will be limited in value. Smart network management solutions must incorporate platform identification and vendor-based classification. These two methods within the discovery process provide the rich set of device-specific data that a good inventory management system needs. When looking for a network management solution, make certain that the inventory discovery capability provides platform identification and classification for devices across the following areas:

- Vendors including Cisco/Linksys, Foundry, HP, Nortel, 3COM, Extreme, Netgear, Dell, SMC, VMware, and Alcatel
- Device types including routers, core switches, distribution switches, firewalls and servers
- Hardware specifications including model, CPU, memory, and network interfaces
- Software information including OSs, applications, and service packs
- Network including ports and VLANS

Smart Network Management Empowers an SMB

This first chapter outlines the value that a smart network management solution provides to an SMB through intelligent network discovery and mapping. This chapter introduces the first foundational feature, *complete visibility*, and highlights that through the use of key features such as Layer 2 port-level discovery and virtual infrastructure discovery you can build a complete picture of the network. In addition, this chapter discusses detailed topology mapping and asset inventories that capture the discovered information.

Chapter 2 covers the second foundational feature, *sophisticated monitoring.* In this chapter, we go into detail about the importance of proactive monitoring and alerting, provide insight into the most desired monitoring technologies, and review the useful reports to look for in a network management solution.

Chapter 3 continues the conversation by discussing the third foundational feature, *integrated configuration and change management*. Here, we cover the benefit of centralizing device configuration and password management. Chapter 3 also takes a look at the ability to compare device configurations and recover from failed device configurations.

Chapter 4 concludes the discussion by focusing on the final foundational feature, r*eal-time troubleshooting, trending, and network traffic analysis.* This is where the *smart* in smart network management really pays off. By providing a solution that enables the business to proactively detect and resolve network-related issues, you will dramatically reduce user interruption and critical business loss. With the addition of historical trending of system and application performance, you will have a powerful network management solution.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.