Managing the InteropNet™

Bobby Krupczak
Empire Technologies, Inc.
rdk@empiretech.com

Steve Hultquist
Worldwide Solutions, Inc.
ssh@wwsi.com

1 Introduction

The NetWorld+Interop trade show has grown from a small gathering of industry professionals interested in testing and evaluating their networking hardware and software into a full-blown industry event attended by over $50,000$ people. At the heart of the show is the InteropNet™, which interconnects the exhibitors, attendees, remote sites, and the Internet. The InteropNet emulates the complex networks found in large corporations and educational institutions. Furthermore, it often mirrors (if not magnifies) the challenges faced today when building such networks. NetWorld+Interop attendees can see, test, and inspect new and emerging network technologies and products functioning on a real, live network. The interconnection of all exhibitors, for instance, provides the opportunity for exhibitors to prove interoperability with other exhibitors during the show. The challenge of designing, building, and installing the InteropNet is immense. The task of managing its operation during the show is as well.

The InteropNet presents many unique and equally immense constraints and challenges due to its size, the fact that it must travel from city to city, the desire to encorporate new and emerging technologies, the lack of control over the equipment that is connected, and its dynamic composition. Although the InteropNet is more complex in size and scope, the experiences gained from it are most certainly applicable. An enormous amount of work goes into bringing the InteropNet to life, much of which goes un-recognized. The design, assembly, and deployment of a network this size would constitute at least three separate articles in and of itself.

The goal of the article is to articulate only one of those aspects – how we, the network operations center (NOC) team, collectively manage the InteropNet. We use the term “manage” somewhat loosely so as to incorporate the full spectrum of activities including management, operations, and administration. What differentiates this article from others is that we reflect on experiences and knowledge gained through the management of the InteropNet – a **very** large, dynamic, heterogeneous, multi-protocol network. We hope that the experiences and knowledge gained through this effort can be incorporated into the design of future network and systems management products.

The article is organized as follows: We present an overview of the InteropNet starting with its design and ending with its deployment at NetWorld+Interop, then we outline our management strategy and, lastly, present a discussion of the lessons learned from such an undertaking.

2 The InteropNet

In this section we present a brief overview of the InteropNet ranging from its design and installation to its deployment at show sights. Previous articles [Alm89, Kno90, Kno91, Cha92] document the InteropNet as it existed some time ago. Although still applicable, the dynamics of the InteropNet warrant periodic discussion. Pitsker [Pit93] documents the InteropNet as it existed in 1993 while a World-Wide Web page [ins95] expands and provides more updated information.

Over the years, an InteropNet design criteria has evolved which stresses flexibility, interoperability, modularity, and transportability. Flexibility is important for several reasons: First, the network design must be extremely flexible so to accommodate changing requirements and requests from users, component changes, and equipment failures. Second, flexibility is key due to the desire to incorporate the latest, emerging network technologies. Third, because the InteropNet is built almost exclusively from donated and loaned equipment, a design lacking flexibility may often fail to meet the requirements of a specific show given the available equipment.

It almost goes without saying that interoperability is an important criterion. Indeed, the original purpose of the Interop organization (and the very basis of its name) was interoperability testing. To that end, participating in the InteropNet is an important avenue for demonstrating interoperability and conformance to industry and organizational standards.

Modularity is becoming even more important as the NetWorld+Interop show expands; There are currently seven shows worldwide per year, with each show placing differing constraints and requirements on the InteropNet. One feature of this modular design permits sections of the network to be deployed and installed independently of one another. Lastly, transportability is obviously important because the network must be quickly shipped, deployed, assembled, and disassembled throughout the world.

Logical Design The design criteria above has led to a "backbone and rib" design whereby multiple, redundant backbone networks feed rib networks. Rib networks, in turn, feed exhibitors and users. Normally, there are at least two backbone networks (currently ATM and dual-ring FDDI). Rib networks generally are Ethernet with ATM, FDDI, 100BaseT and 100VG-AnyLAN added at the larger venues. ISDN is also a planned technology for 1996 or 1997. In addition to rib networks, the backbone interconnects special purpose networks in hotels, network application centers, and the Internet. For each, two separate, redundant routes are provided so that network connectivity can be preserved if failures occur.

Physical Design Groupings of equipment racks termed "peds" make up the entire InteropNet. Peds (short for pedestals, an historic reference) are advantageous for several reasons. First, they can be transported quickly and safely because all sensitive network equipment is mounted within and protected by equipment racks. Second, the pedestals can be assembled and configured off-site before they are deployed at a particular show. Two types exist: concentrator (or 'C') peds and router (or 'R') peds. Concentrator peds generally serve to aggregate traffic from ribs and network segments and connect to router peds. Router peds contain at least two routers and/or switches; their primary task is to route between rib segments and the multiple, redundant backbone networks.

Network Application Centers Dispersed throughout the exhibit halls and surrounding hotels are network application centers (NACs) which provide banks of computers and X terminals that allow attendees to access the InteropNet, the Internet, and the World-Wide Web. In addition, NACs often feature software and hardware from participating exhibitors and have become tremendously popular. Connecting off-site NACs with the InteropNet is accomplished using digital telephone lines, microwave transceivers, and point-to-point lasers at up to 155Mbps.

Network Operations Center The Network Operations Center (NOC) is the heart of the InteropNet. From the NOC, a team of engineers manage and troubleshoot the InteropNet. The NOC is also where all rib and backbone networks within the InteropNet come together and connect to the Internet through multiple, redundant links. For the Atlanta '95 show, two separate 45 Mbps links to two different providers were used.

Exhibitor Connectivity Each exhibitor is required to connect to the InteropNet, and many choose to connect at multiple points using Ethernet, Token Ring, FDDI, or ATM. Further, some vendors require special connectivity to other exhibitors as part of special demonstrations and interoperability testing. These connections, called "specials", are installed specifically for requesting exhibitors and usually require a separate cable run between booths. Requests for "specials" occur up to and throughout the show.

Building the InteropNet Building the InteropNet is an immense effort involving hundreds of individuals. A smaller, core group of individuals (termed the "NOC team") is responsible for the design, deployment, and management of the InteropNet. Scores of additional volunteers (InteropNet team members or "ITMs") help in this giant effort. The NOC Team is a group of highly skilled engineers with broad technical expertise, a commitment to open standards, devotion to the success of the InteropNet and the ability to lead the corps of volunteers who help with specific elements of the network. The NOC Team includes premier network engineering talent from industry, academia, government and the NetWorld+Interop staff. This team spends thousands of hours developing the network design and sleepless nights constructing a working version of the InteropNet during hot staging in NetWorld+Interop's facilities. They, along with the help of ITMs, set it up, operate it and tear the InteropNet down at each NetWorld+Interop World Tour location.

3 Network and Systems Management

Managing the InteropNet is a very challenging task due to its size, its rapid deployment and installation, changing requirements, open connectivity, and it heterogeneity. Network and systems management of the InteropNet is crucial to the success of the show. Vendors invest a substantial amount of money and time to attend a trade show and have come to expect a fully-operational, production show network on which to base their marketing demonstrations. In this section, we first elaborate on the term "management" and then discuss the overriding goals and methodologies we use to manage the InteropNet.

The phrase "network management" is a somewhat loose term with widely varying definitions. While some separate the day-to-day tasks of running the network from its management, others bundle the entire spectrum of operations, administration, maintenance, and planning as network management. Further, some taxonomies separate the management of the network from management of connected systems. Our definition of network management has evolved over time to include the operations, administration, maintenance, planning, and troubleshooting of almost all facets of the InteropNet including network components and critical systems.

Management Goals The overriding goal of network management of the InteropNet is the provision of network connectivity to exhibitors and attendees. That is, first and foremost, full connectivity must be provided between every exhibitor, the Network Application Centers, and the NOC. Secondary goals include connectivity to the outside world (via the Internet), network security and integrity, and the provisioning of a minimum level of network quality-of-service to all devices. Unfortunately, some goals may never be fully realized (e.g. network security and integrity) while others may not be feasible given current network architectures (e.g. IP and Ethernet and reliable quality-of-service guarantees for the fair allocation of network bandwidth.) Further, we differentiate between the management of the "core" InteropNet with management of exhibitor equipment.

Our management goals differentiate between exhibitor equipment (termed "non-core" equipment) and InteropNet (or "core") equipment even though all are interconnected. This differentiation is based primarily on the fact that we (the NOC team) cannot provide network and systems management for every single device (e.g. exhibitor equipment) attached to the InteropNet. The distinction is often based on who maintains administrative control. Unfortunately, failures and errors in non-core equipment can and do have a tremendous impact on the correct functioning of the InteropNet. For those cases, we must be able to identify, isolate, and recover from such problems.

Management Strategy The overall management strategy we use evolves over time as knowledge is gained and new management technologies appear. However, first and foremost, our management strategy is shaped by and is no better than the very hardware and software tools and technologies at our disposal. Indeed, we often find it necessary to augment commercially available tools with those developed expressly for use in managing the InteropNet. Nevertheless, our management strategy is centered around detecting and correcting faults before they impact network connectivity. As can be expected, this goal may not always be realized. Further, no single network and systems management technology can suffice for all management needs.

Not surprising, however, the overriding management technology used on the InteropNet is the Simple Network Management Protocol (SNMP [CFSD90, RM90]). Although not exclusive, SNMP is a major component of our management strategy, providing a foundation for system and network management. Virtually all equipment used in the InteropNet is SNMP manageable – even the uninterruptible power supplies (UPSs) contain SNMP agents. Despite its ubiquity, SNMP is no substitute for hand-held analyzers and administration tools like *ping*, *traceroute*, and *telnet*. While early shows functioned without SNMP [Cha92], the InteropNet of today would not be manageable without it. Lastly, despite its lowly status in the SNMP community, SNMP Trap messages are an extremely important part of our overall management strategy, providing trigger alarms and active warnings as well as exception-based management.

Our management architecture (built to realize the management strategy articulated above) has been simultaneously developed from the top down as well as from the bottom up. It is a relatively flat hierarchy consisting of roughly four layers and mirrors our overall network design. Those four layers are: ribs, backbone and external connectivity, systems/NOC, and management operations. The various management technologies are then deployed according to how they help us manage each of the layers.

Rib Management Because exhibitors and network application centers are connected to the InteropNet through ribs segments, their management and monitoring is the first component of our management architecture. We wish to be able to detect and recover from hardware and software failures, configuration errors, as well as failures in any non-core equipment which impacts the rib or InteropNet. To that end, we deploy a host of equipment to remotely monitor and troubleshoot ribs. First, we utilize RMON [Wal91] probes and RMON agents for statistics collection and event generation. Second, we monitor MIB-2 [edi91] and private-enterprise MIB statistics for each router interface attached to each rib. Third, we often have distributed protocol analyzers attached to each rib that permit us to remotely capture and analyze rib packets. Fourth, we utilize hand-held portable and wireless tools to spot-check and troubleshoot ribs. Lastly, a special “spy” network can be used to actively monitor any rib from a physical location in the NOC.

The spy network is a series of point-to-point fiber links used in conjunction with optical/electrical switches that enable network managers to place workstations, hand-held analyzers, and other management devices in the NOC onto a rib segment without the need for network-layer routing. The spy network can be thought of as providing the ability to virtually patch any NOC machine directly onto any rib.

Backbone Management Managing the InteropNet backbone is crucial to the success of the show because without its proper functioning, little network connectivity would exist. In some respects, backbone management is simpler than rib management because only core equipment is ever directly connected to it. However, an exhibitor’s mis-configured router can cause routing problems on the rib it is connected to. One common problem is “black-holing” a rib. This occurs when a mis-configured router advertises that it has the “best routes” on the rib. Consequently, all exhibitor traffic on that rib goes to that router and disappears. The InteropNet insulates itself from such problems by configuring its routers to only exchange routing information with other InteropNet routers. However, these kinds of problems can appear and will affect exhibitors. We have developed a number of techniques for detecting black-holes, including the active monitoring of RIP packets.

Our major backbone management tasks include the collection of statistics, route management, and detection and recovery from hardware and link failures. Backbone and router management are so important to the InteropNet that a small, separate group with the NOC team devote the entire show to that task. Router monitoring and backbone statistics collection are performed using SNMP, MIB-2, and private-enterprise MIBs. Indeed, SNMP is ideally suited for this kind of monitoring. Route management is performed differently using a variety of techniques. First, management software periodically polls a set of dispersed machines in order to test network connectivity and reachability. This periodic polling enables us to detect link and hardware problems as well as routing protocol failures. However, this technique alone is not sufficient because the inability to reach a node may be due to a variety of problems. To perform route management, we have experimented with a specialized route verification tool that monitors OSPF [Moy94] and RIP [Hed88] routing protocol messages; this tool tracks the topology as constructed via routing protocols and compares it against a pre-programmed topology. When topology changes occur, the route verification tool sends event messages and raises alarms. To detect hardware and link failures, we rely on hand-held analyzers as well as SNMP Trap messages.

Systems/NOC Management The importance of systems management is becoming more important as the correct functioning of networks increasingly relies on the health of key systems. For example, in many networks today the operation of key services like DNS [Moc87], NIS, and Web [BL93] servers are crucial to the health of a network and the services it provides. Not surprising, the correct functioning of many NOC systems is crucial to the overall operation of the InteropNet. To better manage critical systems, we utilize SNMP agents supporting the Host Resources [GW93] and systems management [Kru95, Kru93] MIBs. These agents allow us to monitor critical processes, track system resources, and monitor the overall health of systems so that we can detect and prevent systems-related problems before they occur.

Management Operations The last layer in our management architecture is that composed primarily of SNMP management software and management data manipulation tools and scripts. Our SNMP management software is composed of enterprise management platforms, element managers, special purpose software, and SNMP browsers [Ros93].

We use enterprise management software quite extensively for statistics collection, basic polling and reachability testing, and the graphical depiction of the InteropNet. Although we distribute enterprise management across the InteropNet, manager-to-manager communication (at present) is almost nil for a variety of reasons. First, manager-to-manager communications is still proprietary, although some SNMPv2 work [CMRW93] has addressed this problem. Second, we desire management autonomy for increased robustness. Third, we are not entirely convinced that manager-to-manager communications adequately addresses many of our network and systems management problems.

We make heavy use of element managers as well as vendor-specific and special purpose management software. Element managers provide increased management of classes of devices (e.g. hubs or routers) while vendor-specific management software is often used because general purpose and element software often lack sufficient semantic understanding of private-enterprise MIBs. Unfortunately, the insistence by many companies to use private MIBs for functions available in public MIBs and other issues render vendor-specific element managers a requirement.

We make heavy use of specialized management software to “fill the gaps” left between general purpose, element management, and vendor-specific software. One example is our development and use of a “Trap exploder”. The Trap exploder is a software tool that allows us to receive SNMP Trap messages on a single system, log them to file, and forward them to other management stations, element managers, and vendor-specific software. The Trap exploder greatly reduces configuration overhead because we can designate a single InteropNet machine as a recipient of all SNMP Trap messages. We also use customized software and scripts to count the number of devices connected to the InteropNet. Lastly, one of the most commonly used SNMP management tools is a graphical MIB browser which diagrams MIB modules in a point-and-click interface. This type of tool provides a common interface for accessing any standard or private-enterprise MIBs without requiring specialized vendor-specific management software, provided the MIBs are available and can be compiled using standard MIB compilers. When troubleshooting, we often do not have the time to invest in learning vendor-specific management software.

4 Reflections and Lessons Learned

The development of a management strategy and architecture as well as its use on the InteropNet has provided a tremendous opportunity to learn the art and science of network and systems management in addition to providing us the opportunity to thoroughly test management software, practices, and accompanying frameworks. In this section, we articulate some of the important lessons we have learned over the course of the past few years. We hope that some of these lessons can be incorporated into future product design and implementation. Our observations range from product and framework deficiencies to more general industry observations.

Framework Deficiences Our experiences have highlighted what we feel our deficiencies in the Internet Management Framework (SNMP) when applied to a large, dynamic, and heterogeneous networks such as the InteropNet. One problem we have frequently encountered revolves around the looseness of SNMP MIB specifications. This looseness, and differences of interpretation, has led to interoperability problems between management and agent implementations from different vendors. For example, we sometimes find management software designed to work with a standard MIB often is incompatible with another vendor’s implementation of that MIB. This incompatibility prevents us from using a single management application; consequently we must often install numerous, overlapping management applications, which increases our configuration overhead and resource usage. Another problem involves the lack of semantic expressiveness of SNMP MIB specifications. The current standard SNMP MIB format [Ros91] does not permit the expression of causality between and among managed objects. For example, MIB specifications should to permit the linking of managed objects and managed object values to other managed objects as well as Trap messages. Lastly, the lack of security within the current framework hinders some of our SNMP-based management to monitoring only. However, to increase the security of InteropNet devices, we install a special Ethernet segment (called “ access ether”) over which most management traffic is routed. This segment is not accessible by exhibitors or attendees.

Implementation Flaws Our experiences have also highlighted what we feel are product implementation deficiencies when applied to networks larger than a single, small, isolated LAN environment. Because software bugs are an unfortunate fact of life and are fixable, we will only focus on design issues. One major problem we encounter is the lack of flexible element management software; this deficiency has led to the balkanization of many management tasks. Hub management, for example, is very difficult. When a hub-specific trap is received, we must first determine which vendor manufactured the hub and then navigate the appropriate vendor-specific hub management software. We currently cannot use vendor B's hub management software with vendor A and vice versa. Poor integration of element and management station software only adds to this problem. It is clearly in the best interest of both the industry and individual vendors to solve these problems and enable interaction and interoperability between element managers, and integration with enterprise management systems. The lack of integration is an embarrassment to the industry and clearly a concern for all network managers.

Interoperability and Robustness Concerns Another category of implementation deficiencies centers around interoperability concerns. One huge problem we encounter at every show is MIB compilation problems. Vendors continue to ship pre-Concise-MIB specifications as well as MIBs so filled with syntax errors that they are unusable. While it is tempting to categorize this class of problems as implementation bugs, we feel that it occurs with such regularity as to constitute either a design flaw or an intentional oversight. It seems vendors generally never use, attempt to compile, or test their own MIBs with other management software. We regularly encounter a problem with management software reliance on the functioning of systems-related services like DNS, NIS, and NFS [SM89]. When management software unnecessarily relies on the correct operation of system services, and those system services become unavailable, management software ceases to be functional and only aggravates the problem. For example, many management station implementations rely on DNS and NIS address lookup despite the fact that we have configured network layer addresses into their management databases. When DNS services are unavailable, the management station software becomes unusable.

Software Configuration Management software is often so complex and difficult to operate that misconfiguration itself can lead to network problems. One more humorous example involves the development of the trap-exploder software. We were seeing exceedingly large numbers of traps early in a pre-show environment, many coming from core equipment. We struggled with the problems in an effort to correct what appeared to be catastrophic meltdown of the entire network. It turns out that we had configured the trap exploder machine as a receiver of traps from the trap exploder, thus creating a trap delivery loop. When this occurred, the trap exploder would forward received trap messages back to itself, resulting in almost instant implosion of the underlying machine! Another common problem involves the immense configuration overhead necessary to use most commercial management stations. Although this problem may be more specific to the fast-paced, short-lived environment like NetWorld+Interop, the daunting task of configuring management station software limits its usefulness.

Lastly, we have observed a general trend towards poor “factory” configuration of most management and agent software. For example, many hubs are configured by default to send trap messages at such a high rate (say one per minute or more frequently) so as to inundate a high-powered workstation and render all Trap-based management useless. Further, most devices are configured to send authentication failure traps by default and many do not support the ability to change this behavior via an SNMP SET request. In addition, private-enterprise MIBs are often written such that read-write community strings are contained within tables that can be queried using read-only permissions. Consequently, any browser can discover read-write community strings and compromise any management security that may exist.

An Industry Trend We have also noticed a general industry trend forming which we term “open proprietary computing” or “OPC”. The oxymoron is intentional and is used to describe a practice becoming increasingly common. For example, many vendors encode their private-enterprise MIBs within their management software, but do not distribute the MIB specification to users of their products. This situation prevents network managers from picking and choosing the best management software independent of network hardware. This practice, which greatly disturbs us, is tantamount to product tying as well as the closing of an open standard.

Another example of open proprietary computing can be found in vendor’s minimalist implementations of standard MIBs, which they then augment by full-featured private-enterprise MIB implementations tied to their own management software. This implementation strategy is similar to bait-and-switch selling. These trends are accelerating and appear to be aimed at creating a new paradigm for “golden handcuffs.

Positive Trends We also have noticed many positive developments in the network and systems management arena. SNMP’s successful deployment and near ubiquity have greatly enabled the remote monitoring of network equipment and systems. New private-enterprise and standard MIBs are emerging that will greatly enhance our management ability. The SNMPv2 process is addressing and improving the expressiveness of MIB specifications, addressing some of the root causes of interoperability problems, as well as addressing scalability issues. Lastly, new management software appears to be improving in several key areas: it is providing increased integration as well as the ability to be “programmed” with or learn the knowledge of its operators.

5 Conclusion

Building and installing the InteropNet presents many challenges due to its size, its dynamism, and its heterogeneity. Managing such a network presents tremendous problems, but also provides for unique insights into the strengths and weaknesses of current network management practices and products. We have articulated the network and systems management goals of the InteropNet NOC team as well as the basic architecture we use to fulfill them. We then discussed a few weaknesses of the components that make up our management architecture and hope that our experiences will guide future design and development. Although we tended to focus on many of the problems, many things do work and do work very well. As Dave Clark has said: keep the faith.

Acknowledgements

A great many people participate in building, designing, deploying and managing the InteropNet. So many, in fact, that we cannot individually acknowledge them. All contribute greatly; without all their help, the InteropNet would not exist.

References

[Alm89] P. Almquist. The INTEROP 88 network – behind the scenes. *ConneXions: The Interoperability Report*, 3(2):2–9, February 1989.

[BL93] Tim Berners-Less. Hypertext transfer protocol (HTTP), November 1993. Internet Draft.

[CFSD90] J.D. Case, M. Fedor, M.L. Schoffstall, and C. Davin. Simple network management protocol. Anonymous FTP, May 1990. RFC 1157, obsoletes RFC 1098.

[Cha92] B. Chapman. Building & managing the INTEROP 91 fall shownet. *ConneXions: The Interoperability Report*, 6(6):18–21, June 1992.

[CMRW93] Jeffrey D. Case, Keith McCloghrie, Marshall T. Rose, and Steven L. Waldbusser. Manager-to-manager management information base. Anonymous FTP, April 1993. RFC 1451.

[edi91] Management information base for network management of TCP/IP-based Internets: MIB-II. Anonymous FTP, March 1991. RFC 1213, obsoletes RFC 1158.

[GW93] P. Grillo and S. Waldbusser. Host resources MIB. Anonymous FTP, September 1993. RFC 1514.

[Hed88] C. Hedrick. Routing information protocol. Anonymous FTP, June 1988. RFC 1058.

[ins95] Pocket guide to the INTEROPNET: NetWorld+Interop 95.
http://www.interop.net/interopnet/brochure.html, 1995.

[Kno90] S. Knowles. The INTEROP 89 network: from one of its builders. *ConneXions: The Interoperability Report*, 4(2):10–17, February 1990.

[Kno91] S. Knowles. Building the INTEROP 90 show network. *ConneXions: The Interoperability Report*, 5(9):36–39, September 1991.

[Kru93] B. Krupczak. Unix systems management via SNMP. In *Proceedings of the IFIP TC6/WG6.6 Third International Symposium on Integrated Network Management*, April 1993.

[Kru95] Bobby Krupczak. Systems management and the Internet management framework. *ConneXions: The Interoperability Report*, 9(8):2–9, August 1995.

[Moc87] P. Mockapetris. Domain names - implementation and specification. Anonymous FTP, November 1987. RFC 1035.

[Moy94] J. Moy. Ospf version 2. Anonymous FTP, March 1994. RFC 1583.

[Pit93] Bo Pitsker. Insights into the INTEROPnet. *ConneXions: The Interoperability Report*, 7(3):2–8, March 1993.

[RM90] M.T. Rose and K. McCloghrie. Structure and identification of management information for TCP/IP-based Internets. Anonymous FTP, May 1990. RFC 1155, obsoletes RFC 1065.

[Ros91] M. T. Rose. Concise MIB definitions. Anonymous FTP, March 1991. RFC 1212.

[Ros93] Marshall T. Rose. Network management: Status and challenges. *ConneXions: The Interoperability Report*, 7(6):11–17, June 1993.

[SM89] Inc. Sun Microsystems. NFS: Network file system protocol specification. Anonymous FTP, March 1989. RFC 1094.

[Wal91] Steve Waldbusser. Remote network monitoring management information base. Anonymous FTP, November 1991. RFC 1271.

Bobby Krupczak is Chief Scientist at Empire Technologies, Inc. where he designs and implements intelligent network and systems management agents and managers. He regularly participates on the InteropNet NOC team where has gained valuable insight into the art of network and systems management of large, heterogeneous networks. He can be reached at **rdk@empiretech.com**. For more information, please consult Empire's homepage at **http://www.empiretech.com/empiretech/**. For a copy of the Trap-exploder, send email to **info@empiretech.com**.

Steve Hultquist is President of Worldwide Solutions, Inc. in Boulder, Colorado, which specializes in helping organizations design and deploy technology-based business solutions. Steve has an extensive background in information technology, from application development to outsourcing, and he has a special interest in designing, building, and deploying networks. He regularly participates on the InteropNet NOC team. He can be reached at **ssh@wwsi.com**. For more information, please see Worldwide's home page at **http://www.wwsi.com/**.