

Lucent Technologies
Bell Labs Innovations

Remote Network Management

HIGHLIGHTS

- Three-quarters of current remote network management users are satisfied with the service they are receiving. Respondents who do not currently employ remote network management are most likely to do so in the future on an ad hoc basis.
- The primary reasons that respondents either employ or will pursue a remote network management strategy are the complexity of managing an integrated voice, data, and mobile network, and to reduce personnel costs. Top reasons not to pursue this strategy are that the current network is running well and security concerns.
- For 83 percent of respondents, people and process issues are the biggest challenge to implementing or improving their remote network management. Only 17 percent identify technological issues as their biggest challenge.
- Two of the three top barriers to implementing or improving remote network management are money related – the cost of these services and justifying this expenditure to upper management.
- The most important functions respondents expect from a remote network management service are surveillance and control of network elements and devices, and diagnosis and analysis of alarms.
- When selecting a remote network management vendor, the top characteristics respondents look for are network expertise, real-time around-the-clock monitoring for proactive problem identification, and availability of performance reports.

CONTENTS

1 Highlights
2 About Lucent Technologies Worldwide Services
3 Introduction
3 The Bottom Line
4 Remote Network Management Strategies
8 Challenges and Barriers to Remote Network Management
10 Remote Network Management Environments and Functions
12 RNM Vendor Requirements
15 Respondent Demographics
16 Respondent Comments
17 About Lucent Worldwide Services Network Industry Surveys
18 Methodology

About Lucent Technologies Worldwide Services

Lucent Worldwide Services provides a full life cycle of services and solutions that help our customers plan, design, implement, and operate networks in today's rapidly changing and complex environment. We have a proven track record with the broadest cross-section of service provider and enterprise customers, evidenced by an extensive portfolio of more than 15,000 engagements worldwide. Our commitment to our customers' success includes a commitment to planning, designing, building, and operating successful networks. We operate 150 customer networks from our world-class Knowledge Centers around the world.

Lucent Technologies Worldwide Services' Remote Network Management Service was recently named "Outsourced Network Management Product of the Year" by *Network Magazine*. This global service offers best-in-class fault management, performance management, and configuration management for multitechnology, multivendor networks.

Lucent Technologies is headquartered in Murray Hill, New Jersey, USA.

Visit the Lucent Services Web site at http://www.lucent.com/businessunit/worldwide.html

For information regarding Lucent Services network services and solutions capabilities, call 1-888-767-2988 in the U.S., or 1-650-318-1020 outside the U.S., or email: networkcare@lucent.com.

For more information regarding this survey, please contact:

Rick Blum
Senior Research Programs Manager
(781) 848-5500, Ext. 320
Email: rickblum@lucent.com

Introduction

Network complexity and cost are rising rapidly in concert with the increasing reliance of business operations on those networks. This phenomenon is true for enterprises and service providers alike. But proactively managing large networks requires significant time, expertise, and staffing – which is why many IT organizations are evaluating the benefits of outsourcing or out-tasking some or all of their network management to a third-party provider that can manage the network from a remotely located network operations center.

From June 1, 2001 through July 12, 2001, Lucent Technologies Worldwide Services conducted a Web-based survey on remote network management, which was completed by 90 network professionals around the globe. The results of this survey yield valuable insights into the past, current, and future remote network management strategies of today's service providers and enterprises. Moreover, these results identify the significant barriers and challenges network professionals face as they plan, design, and implement remote network management strategies for their organizations. These results should enable networking organizations to better understand how their operations compare with others in the industry and identify possible areas for improvement. Complete results for all Lucent industry surveys are available at www.lucent.com/knowledge/resourcelib.

For the purposes of this survey, network management was defined as the set of controlling and automating processes and technologies required to manage networked systems (voice and data) and enable managers to maximize operational performance. Remote network management (RNM) is the use of an outside vendor to perform one or more network management functions, i.e., Fault Management, Configuration Management, Performance Management, Security Management, and Accounting Management. Out-tasked remote network management is the contracting of a vendor to provide one or more of these functions while retaining overall control of the network by maintaining ownership of network assets. Outsourced remote network management typically includes transfer of full operational responsibility and ownership of network assets and personnel to the outsourcing vendor. Ad hoc remote network management is acquiring a specific function from a vendor as required.

The Bottom Line

Remote network management services can provide significant benefits to network managers who are responsible for smooth network operations in complex environments, such as integrate voice and data networks, networks comprising multiple transport types, and multivendor/multiplatform networks. Many network organizations lack the necessary skills or manpower to adequately manage these networks and can take advantage of the technical expertise of remote network management vendors that have broad experience in many network environments.

Although cost reduction is also a frequent goal of a remote network management strategy, it can be difficult to demonstrate to upper management that the benefits will equal or exceed the cost, particularly for complete outsourcing of this function. More successful strategies can be out-tasking, where one or more functions are conducted remotely without giving up ownership and control of the network, and acquiring specific functions on an ad hoc basis.

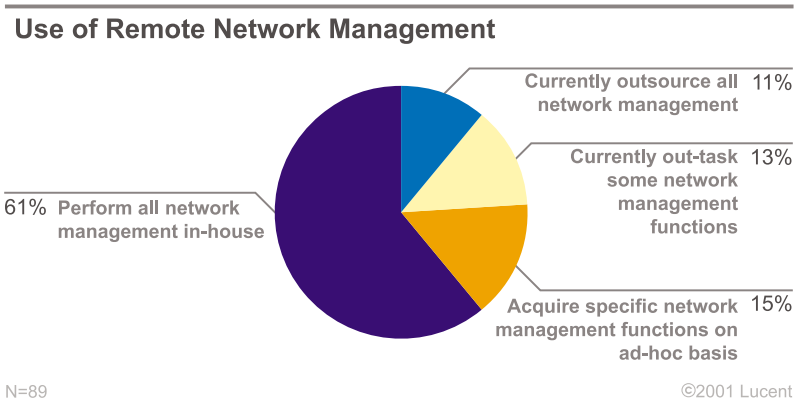
When considering a remote network management solution, network managers should consider each of the following points:

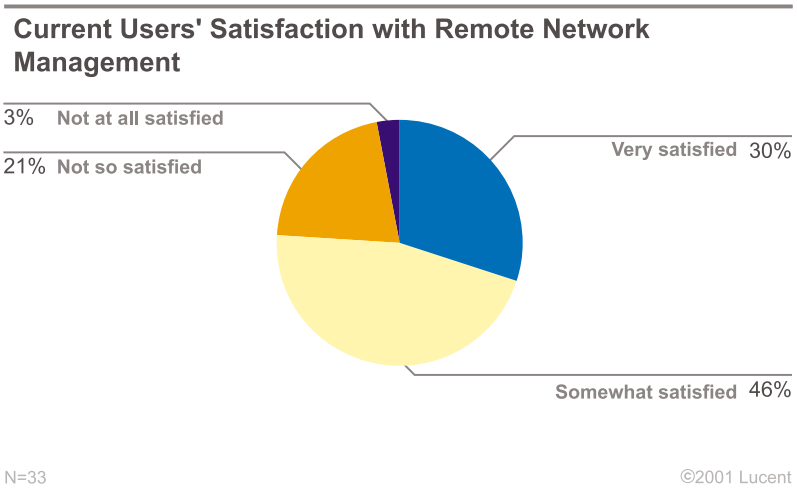
- The biggest challenge to implementing remote network management will be aligning internal processes with the remote service, and the people who will support those processes. Careful attention to issues such as problem escalation, documentation, training, and workflow will be instrumental to a successful outcome.
- Obtaining support from upper management will require a complete and detailed cost/benefit analysis. Quantifying the benefits, such as improved network performance, reliability, and time-to-market, in monetary terms will be essential.
- When choosing a remote network management vendor, seek out those that can help with the two previous points. That is, look for vendors not just with technical expertise, but those that recognize that establishing well-understood and documented processes is key. Vendors should be able to demonstrate the cost savings of their services by providing a thorough analysis of the network and its management requirements.

Remote Network Management Strategies

Thirty-nine percent of survey respondents currently employ some form of remote network management: 11 percent outsource all network management, 13 percent out-task selected network management functions, and 15 percent acquire these functions on an ad hoc or as-needed basis. The remaining 61 percent of respondents perform all network management functions themselves.

Of those respondents who currently employ remote network management services, the vast majority (76 percent) are satisfied with those services, with 30 percent saying they are very satisfied. Only a scant 3 percent of respondents are not at all satisfied with their remote network management services.

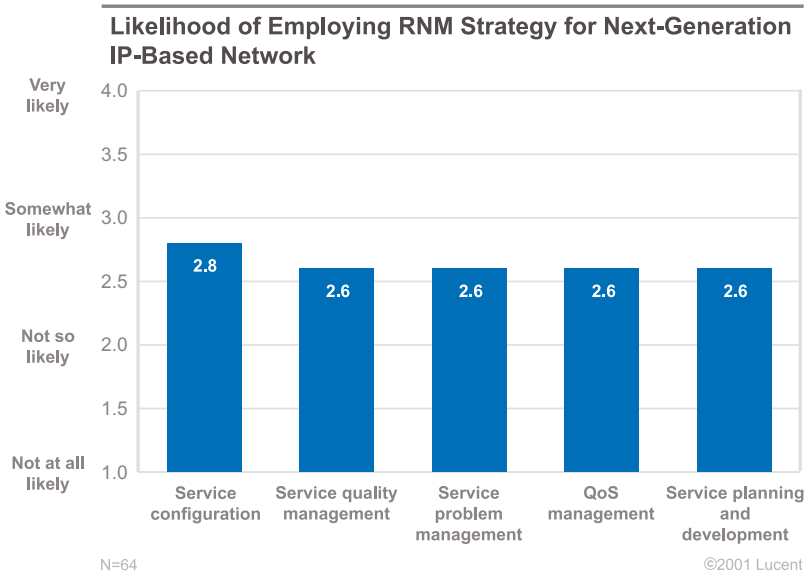


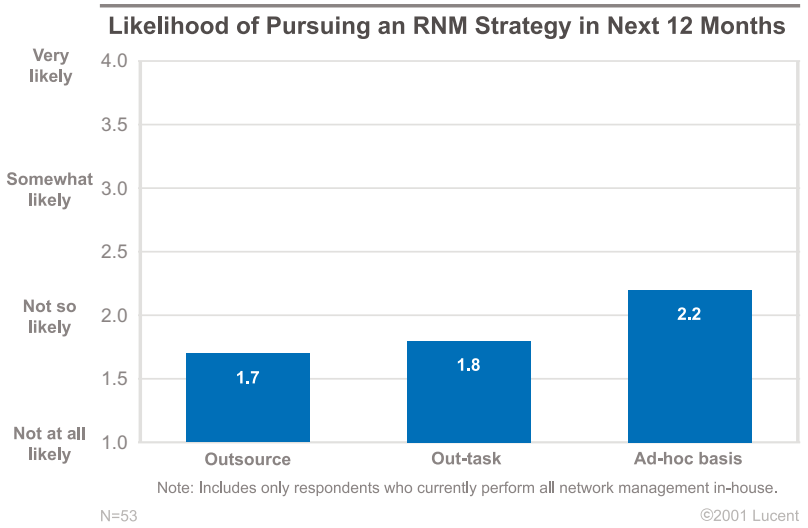


As respondents' networks move to next-generation, IP-based architectures, most will look at a range of network management functions as candidates to outsource or out-task. We asked respondents who either currently employ a remote network management strategy or would consider doing so which functions they are likely to outsource or out-task. The most likely is service configuration, which nearly three-quarters of these respondents indicated that they are likely to outsource or out-task.

Service planning and development garnered the highest percentage of respondents (25 percent) who would be very likely to employ a remote network management strategy. However, it also garnered the highest percentage of respondents (20 percent) who are not at all likely to pursue this strategy. The other three functions – service quality management, service problem management, and quality of service (QoS) management – fall between service configuration and service planning and development.

Of the respondents who currently employ an in-house network management strategy, nearly half (48 percent) are very or somewhat likely to pursue a remote network management strategy in the coming year. Using ad hoc services is the most common path for these respondents (42 percent), but out-tasking (23 percent) and outsourcing (17 percent) are also being considered by many.



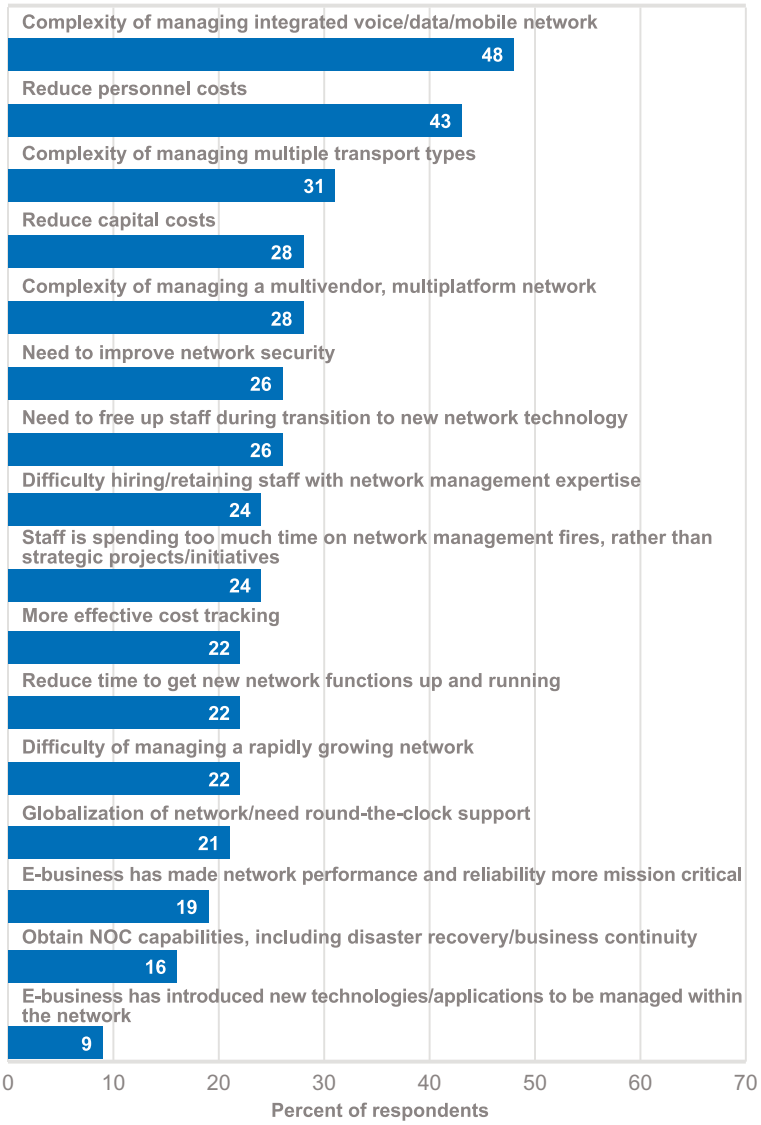


The reasons that respondents currently employ a remote network management strategy or are likely to do so within 12 months are many and varied. However, two reasons are considerably more common than the others: the complexity of managing an integrated voice, data, and mobile network, and reducing personnel costs.

The second of these two leading reasons should come as no surprise, particularly in today's belt-tightening climate. It should also be no surprise that networks are becoming more complex, and that this complexity raises the level of expertise and effort required to manage them. Remote network management providers that have been in the game for awhile have a wealth of expertise, and can alleviate the difficulty of allocating resources to never-ending network management tasks.

Interestingly, the next two most common reasons follow these same themes: complexity and cost reduction. For 31 percent of respondents, the complexity of managing multiple transport types is reason to pursue a remote network management strategy, while 29 percent of respondents want to reduce capital costs.

Primary Reasons for Pursuing an RNM Strategy



Note: Includes only respondents who currently use an RNM strategy or are likely to do so within 12 months.

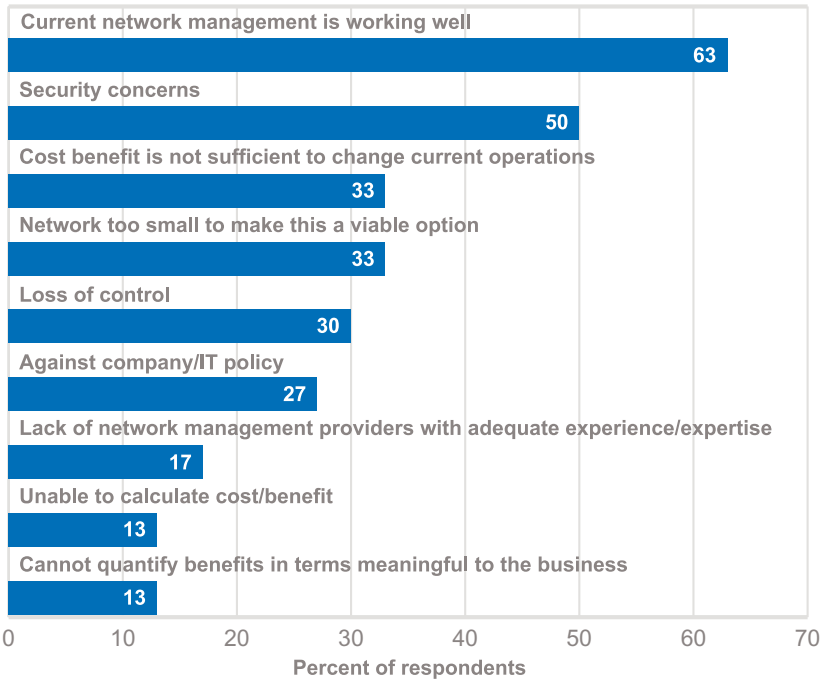
N=58

©2001 Lucent

On the flip side of the coin, respondents who currently perform all network management in-house and are not likely to change this strategy within the next six months have their own set of reasons. Again, two factors rise to the top. Most prominently, 63 percent of these respondents say that their current network management efforts are going well and so they don't see a need to make a change to the status quo. A primary consideration for half of respondents is concerns that remote network management will have an adverse affect on security, either because it will expose the network or that the remote network management vendor is not capable of maintaining adequate security levels.

Another one-third of respondents simply don't perceive that the cost/benefit ratio with remote network management will be acceptable. Given that cost is one of the primary reasons that the other respondents cite as a reason to move to remote network management, it is clear that the cost equation can vary widely depending on circumstances. It is possible, however, that some of those differences are in the calculation methodology, not necessarily in the actual cost.

Reasons for Not Pursuing an RNM Strategy



Note: Includes only repondents who currently perform all network management in-house and are not likely to change this strategy within 12 months.

N=30

©2001 Lucent

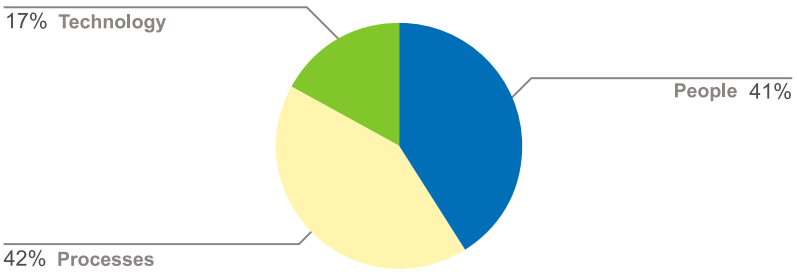
Challenges and Barriers to Remote Network Management

Unlike many other issues network managers have to deal with, when it comes to implementing or improving a remote network management strategy, technology is rarely the biggest challenge. Instead, either people (e.g., training, recruiting, roles and responsibilities) or process (e.g., troubleshooting, change management, documentation) issues are the main sources of concern, with a virtually equal percentage of respondents choosing each. For network professionals whose work experience has been primarily dealing with technical issues, overcoming these other two issues in order to attain their remote network management goals can be a big challenge indeed.

While people and process issues are a challenge, there are a number of other barriers that must also be overcome to meet remote network management goals. For 63 percent of respondents, the cost of services is a hurdle. Interestingly, 43 percent of respondents previously identified reducing personnel costs as a primary reason for pursuing a remote network management strategy, so it appears that these are the ones who have calculated a favorable cost/benefit ratio, while the remainder are still struggling to make the numbers work.

Even when the number make sense, justifying the cost of services to upper management remains a barrier to overcome for more than half of respondents.

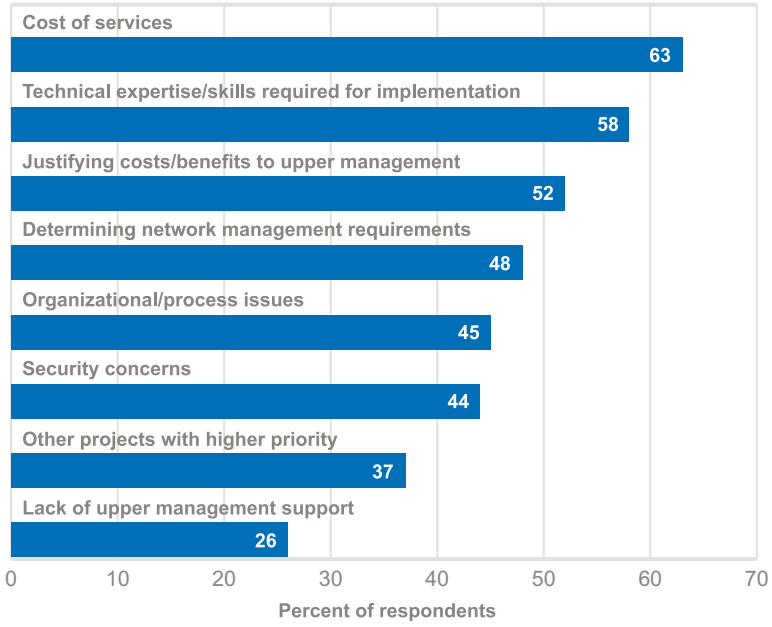
Area That is Biggest Challenge to Implementing/Improving RNM Strategy



N=59

©2001 Lucent

Significant Barriers to Implementing/Improving RNM Strategy



N=62

©2001 Lucent

For 58 percent of respondents, obtaining the technical expertise and skills required to implement remote network management is an obstacle, despite the promise of remote network management vendors to supply many of those skills.

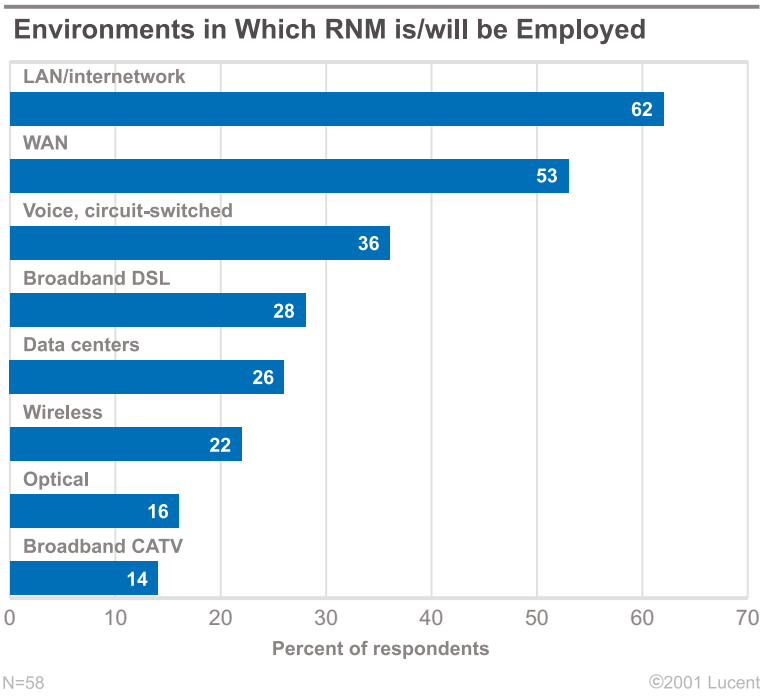
Remote Network Management Environments and Functions

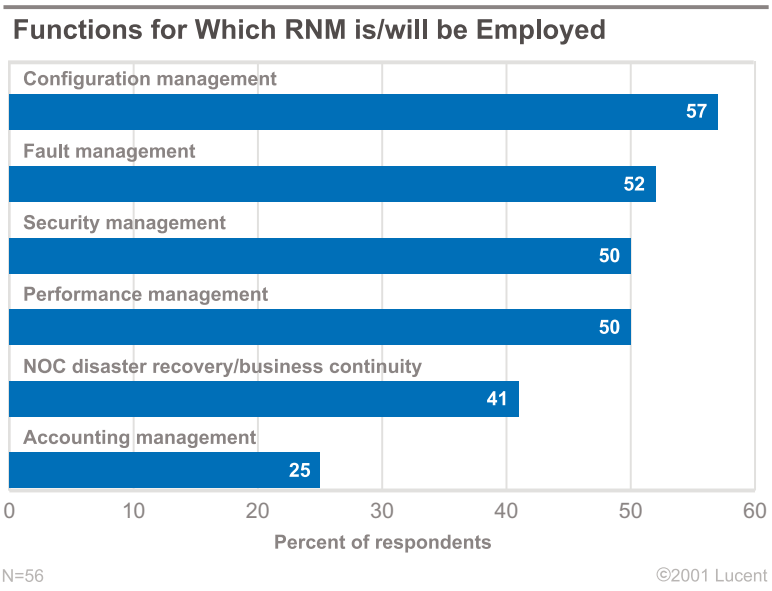
The two most common environments in which respondents have deployed or are considering deploying a remote network management strategy are local-area networks (LANs)/ inter-networks and wide-area networks (WANs), with both being chosen by more than half of respondents.

More than one-third of respondents employ RNM for their voice, circuit switched networks, while more than one-quarter do so for broadband digital subscriber line (DSL) and data center environments. Optical network and broadband cable TV (CATV) environments are less commonly found and, therefore, only a few respondents have or will employ an RNM strategy for these.

Respondents indicate a wide variety of broad functional categories that they get from using RNM. Configuration management leads the pack, employed by 57 percent of respondents. Fault management, security management, and performance management are all functions performed by RNM for 50 percent or more of respondents.

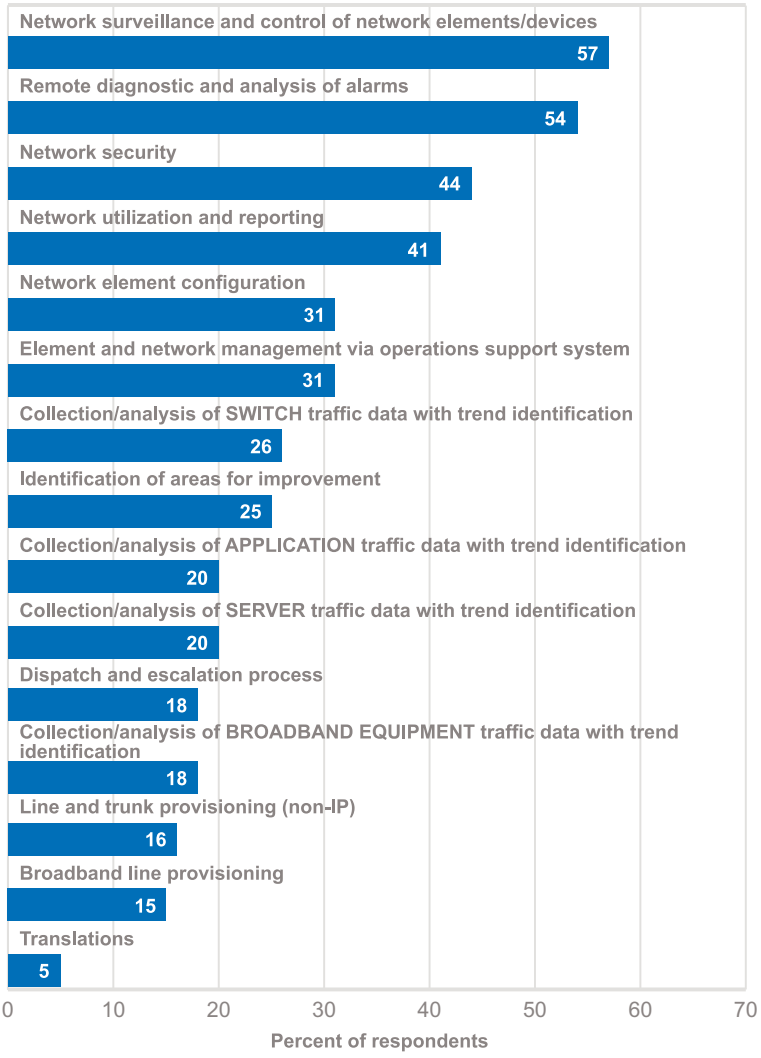
A sizable percentage of respondents (41 percent) uses RNM to provide disaster recovery and business continuity for the network operations centers (NOCs). Only one-quarter of respondents choose RNM for accounting management.





We asked respondents to identify the most important specific functions that they will have accomplished by employing RNM. Two functions were chosen by more than half of respondents: network surveillance, including control of network elements and devices, and alarm diagnosis and analysis. Two others were chosen by more than 40 percent of respondents: network security and network utilization and reporting. A third set of functions was chosen by more than 30 percent of respondents: network element configuration and element and network management via operation support system.

Most Important Functions of RNM



N=61

©2001 Lucent

RNM Vendor Requirements

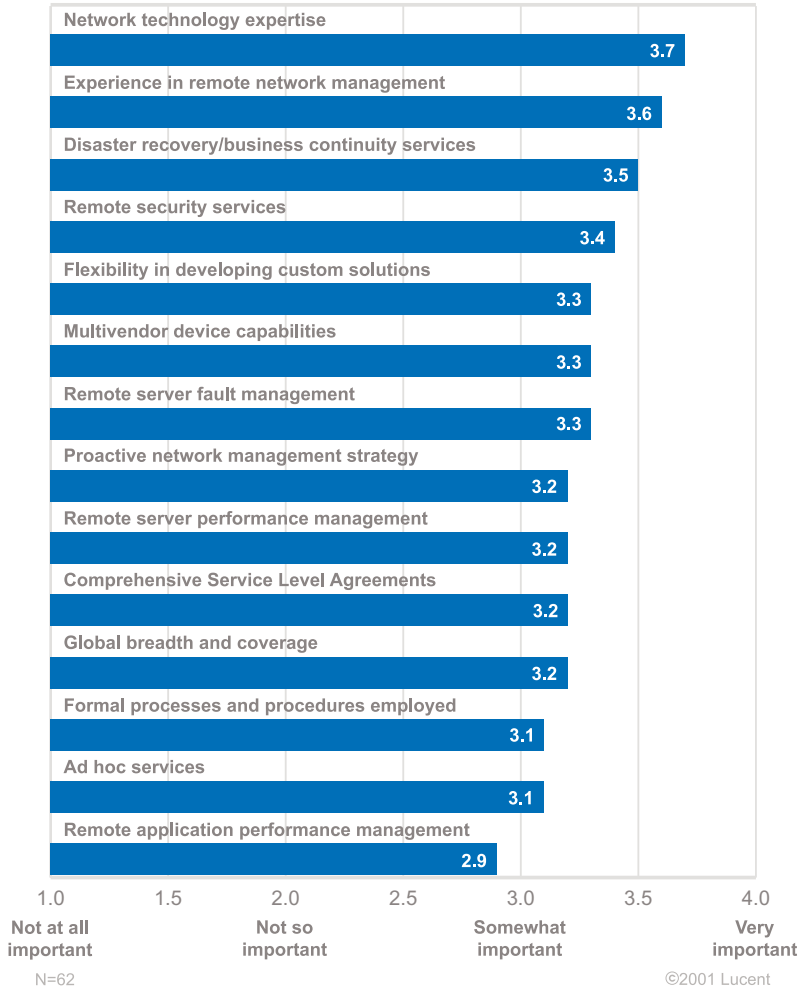
When a decision has been made to follow a remote network management path, choosing a vendor with the right mix of capabilities becomes the critical next step. The first capability that respondents look for goes without saying, that is, network technology expertise. Three-quarters of respondents consider expertise very important when evaluating an RNM vendor, and all but a handful consider it at least somewhat important.

The second most important capability also goes without saying: experience in remote network management. Being able to demonstrate this experience with current customer lists and references will be critical for vendors to secure business.

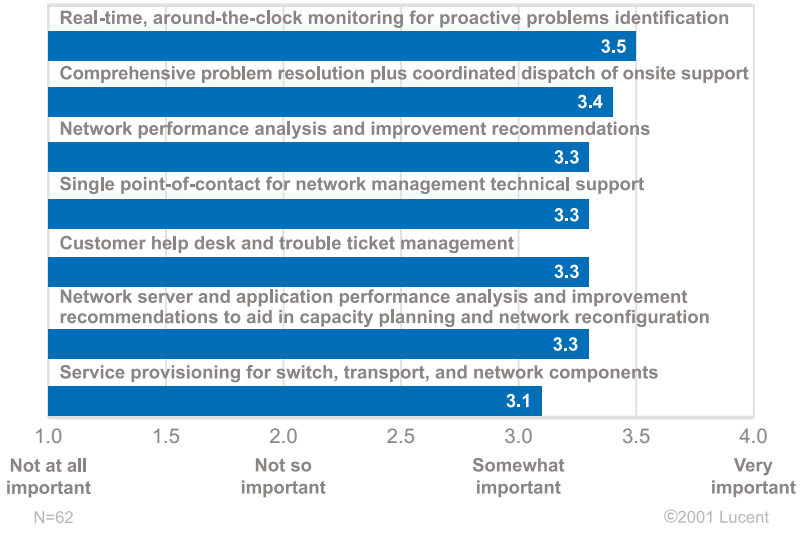
The third most important capability is not as easily anticipated as the first two. But nearly nine out of ten respondents say that business continuity and disaster recovery services are important capabilities of RNM vendors. Clearly, maintaining network uptime is a critical reason for choosing an RNM strategy. Remote security services is the fourth capability that at least nine out of ten respondents consider important when evaluating RNM vendors.

Even though these four capabilities rate higher than the next 10, the most striking thing is that the expectations are universally high. Even for the lowest rated capability – remote application performance management – more than 70 percent of respondents make this an important part of their evaluations of RNM vendors.

Importance of Capabilities When Evaluating an RNM Vendor



Importance of Functional Requirements When Evaulating an RNM Service



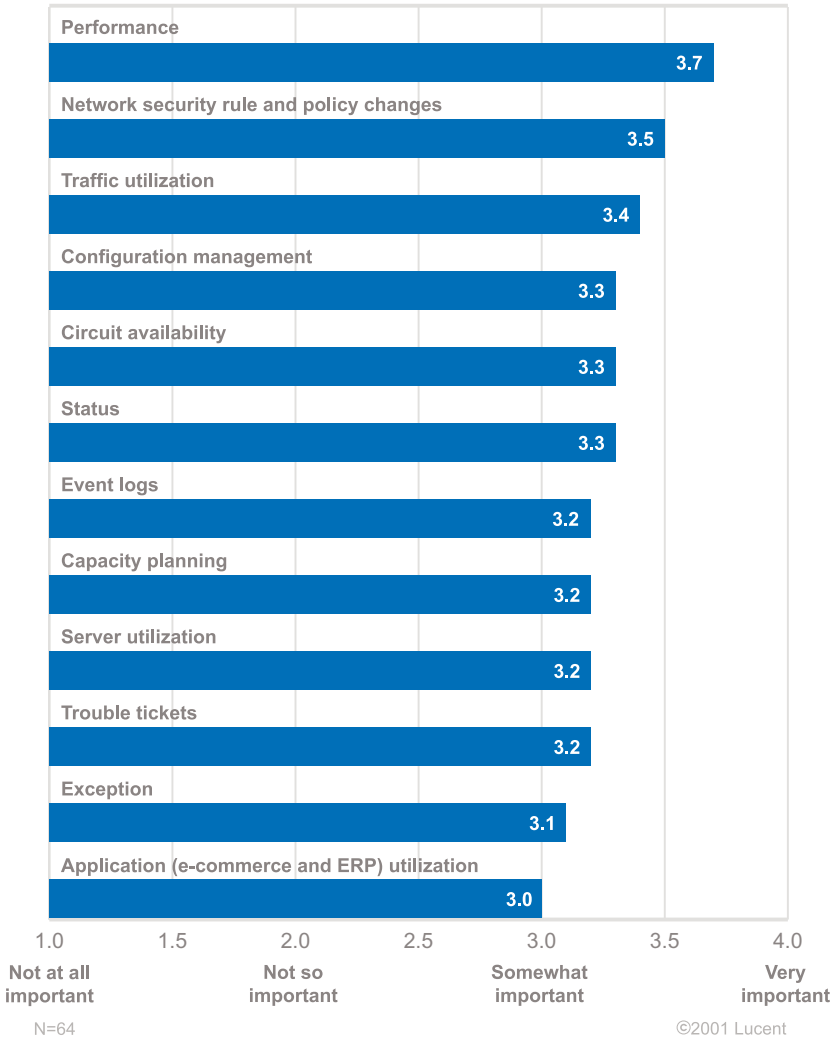
Similar to the high importance placed across the entire range of capabilities, respondents consider a broad range of functional requirements to be important, from real-time, around-the-clock monitoring for proactive problem identification to service provisioning for switch, transport, and network components. This shows that potential users set the bar for RNM vendors very high, and that they must be competent at a wide range of functions in order to win and maintain clients.

Respondents also expect that RNM vendors will be able to provide a plethora of reports on their networks as part of the services. Performance tops the list of reports, being named as very important by nearly three-quarters of respondents, and somewhat important by another fifth.

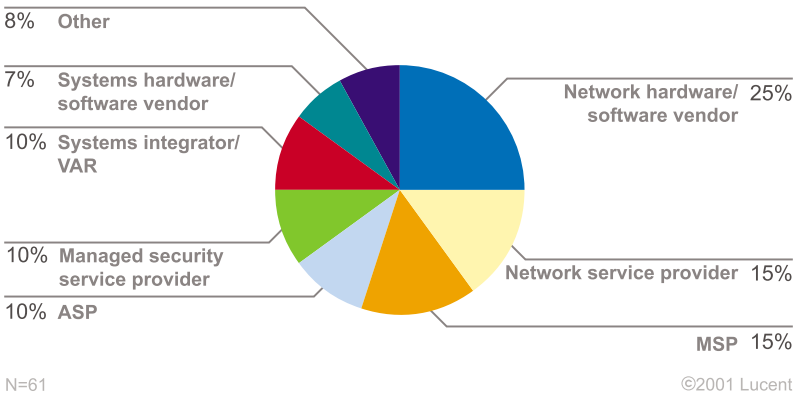
Reporting on network security rule and policy changes is second in importance, followed by traffic utilization. Again, though, the most striking aspect is that the importance rating of all 12 reports is universally high.

Taking all the capabilities, functions and reports into account, we then asked respondents which type of vendor they currently use or would be most likely to use. The results did not point to any one winner, although network hardware/ software vendors were chosen significantly more often that the next vendor type, network service provider. Still, only one-quarter of respondents would go in this direction. The clear message is that many different types of vendors can play in this field, as long as they meet the stringent requirements expressed previously.

Importance of Reports on Various Aspects of RNM



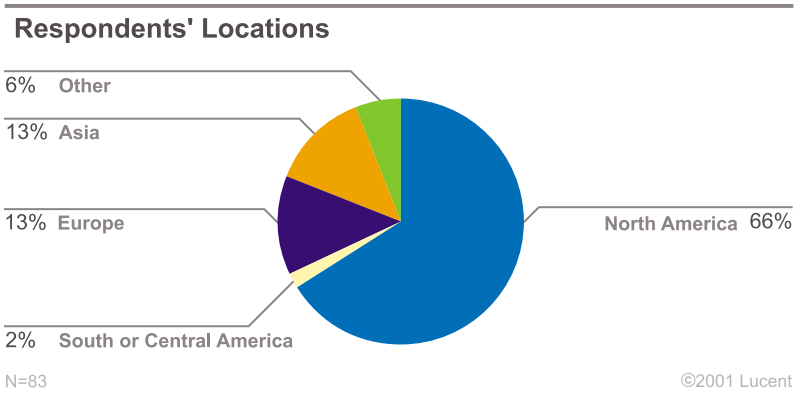
RNM Vendor Type Most Likely to be Used

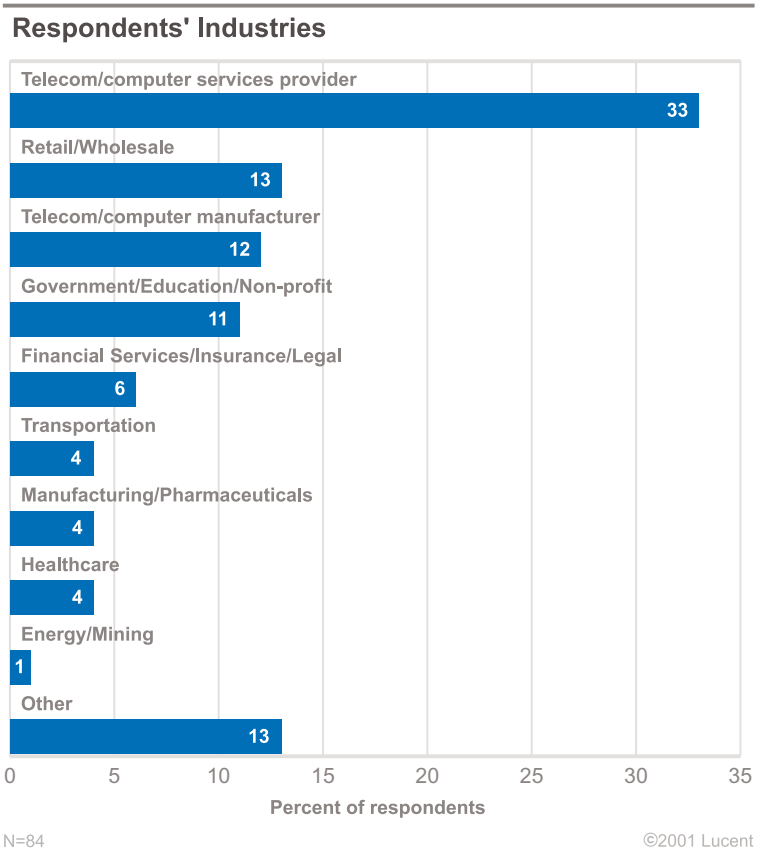


Respondent Demographics

Nearly two-thirds of respondents are located in North America, while Asia (13 percent), Europe (13 percent), and South or Central America (2 percent) account for most of the remaining respondents. The "Other" category includes respondents from Australia and New Zealand.

Survey respondents represent a fairly broad cross section of industries, led strongly by telecommunications/ computer services providers, which represent one-third of respondents. Other well-represented industries include retailers/wholesalers (13 percent), telecommunications/ computer hardware and software manufacturers (12 percent), government/education/nonprofit organizations (11 percent), and financial services/insurance/legal firms (6 percent).

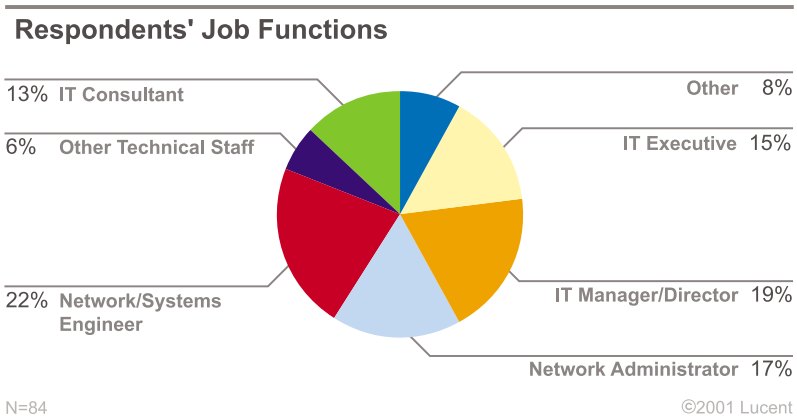


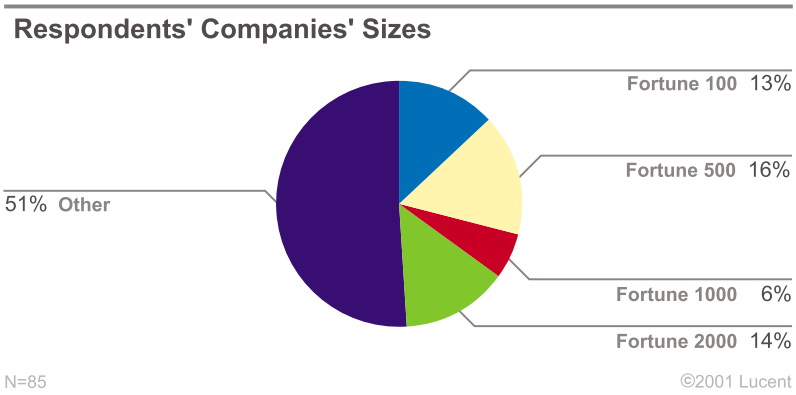


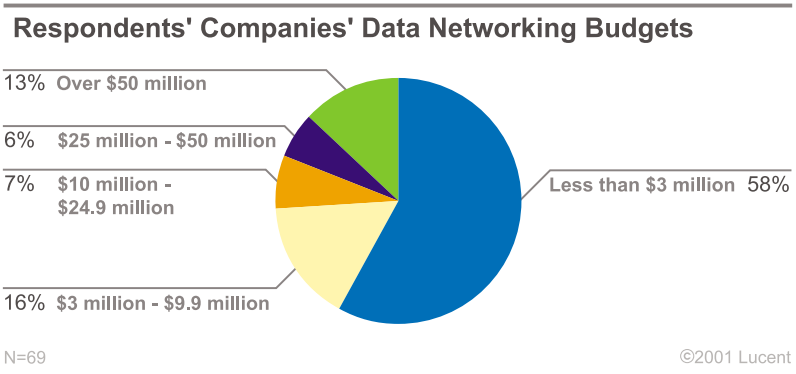
The highest percentage job title/ function category is network/systems engineer (22 percent), followed by IT manager/director (19 percent), network administrator (17 percent), and IT executive (15 percent).

Nearly half of respondents' companies are in the Fortune 2000, and 13 percent fall in the Fortune 100.

At the high end, 13 percent of respondents' companies budget in excess of $50 million annually for data networking. The majority of respondents' companies work with budgets of under $3 million.







Respondent Comments

- As a longtime IT professional, I have seen outsourcing in action. All too often it was to bring in a bunch of products that never worked as advertised, compromised our security, cost an arm and a leg before all the dust had cleared, and left us with huge problems migrating our data to their products . . .
- Most outsourcers would try to take away our Linux workstations and replace them with Win2000 and various other changes . . .
- I can't see any MSP (at least in Europe) who could succeed in functionality, skills, service level management, etc.
- I use an ASP to monitor servers, analyse data, and recommend actions to improve network operations.
- Use of Internet in a secure way would be very effective for managing organisations like ours.
- We are a bank and we externalized our IT department to an outsourcing company. We are bound to use them, no matter what level of services, what services, or what expertise they have.

About Lucent Worldwide Services Network Industry Surveys

Lucent Worldwide Services conducts monthly industry survey projects intended to provide IT managers with insight into key issues impacting the ability to develop and deploy network-centric business applications. Previous survey reports include:

- ASP Network Infrastructure
- Convergence and New World Services Providers
- E-Business Network Architecture/Infrastructure
- Enterprise Operating Systems and Directory Services
- Management Intranets
- Network and Systems Management Total Cost of Ownership
- Network Challenges and Opportunities in Uncertain Times
- Network Operations Centers
- Network Professionals Job Satisfaction
- Network Quality of Service
- Network Security
- Performance Management and Engineering
- Remote and Mobile Network Access
- Service Level Management
- Virtual Private Networks

To see the results of these surveys or to participate in the latest Lucent Technologies network industry survey, visit our web site at:

http://www.lucent.com/businessunit/worldwide.html

If you would like to learn how Lucent can help you implement or improve your networking capabilities, please call us at 1-888-767-2988 in the U.S., or 650-318-1020 outside the U.S., or email: networkcare@lucent.com.

Methodology

This survey was conducted over the World Wide Web from June 1, 2001 – July 12, 2001 at:

http://www.lucent.com/contact/current_survey.html

All Web survey responses were automatically collected into a survey tool. Any questions skipped or incorrectly answered by survey respondents were not included in the tabulations. Not-applicable responses were also not included in the tabulations. Each chart includes the number of valid responses for that particular question (e.g., N=100 indicates 100 responses). Percentages shown in charts may not equal 100 percent due to rounding.

For additional information, please contact your Lucent Technologies Sales Representative or your Lucent Advantage Reseller. You can also visit our web site at www.lucentservices.com or call 1-888-4LUCENT in the U.S. or 1-650-318-1020 outside the U.S.

Lucent Technologies
Bell Labs Innovations



VitalSuite and VitalQIP are trademarks of Lucent Technologies Inc. All other trademarks and registered trademarks are properties of their respective holders. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to Lucent Technologies products or services. ©2001 Lucent Technologies Inc. All rights reserved. Printed in U.S.A.Lucent Technologies Inc. Marketing Communications IS.NWKMGMT.8091.0801

1213 Innsbruck Drive
Sunnyvale, CA 94089

Bulk Rate
US Postage
PAID
Permit No.426
Sunnyvale, CA