Ascend

WHITE PAPER

A New Era in Network Management

Table of Contents

NETWORK MANAGEMENT: TODAY'S CHALLENGES

The Internet has introduced fundamental changes in the way people communicate and the way networks are built. The traditional dedicated network infrastructure has been replaced by a more dynamic, connection-by-demand architecture that is growing at a staggering rate. Scalability requirements of the management system are no longer measured in a few hundred elements, but in multiple thousands of elements: huge numbers of access ports, an array of access and backbone transmission services, and a heavy concentration of switches and routers (Figure 1).

But with all this growth, the network management paradigm has not shifted from the element-oriented network management schemes which break down when faced with densities of this magnitude. One-device-at-a-time management is impossible, and dependency on SNMP alerts and network polling to monitor thousands of devices could bring the network to its knees. Furthermore, the major growth area of the network — at the access and switching layers — is not even visible to IP-based network management platforms. You can't manage what you can't see.

A new kind of application is needed to manage the network as it exists today. Network management can no longer focus only on the element, but must globally manage the environment, while understanding the complex relationships between elements.

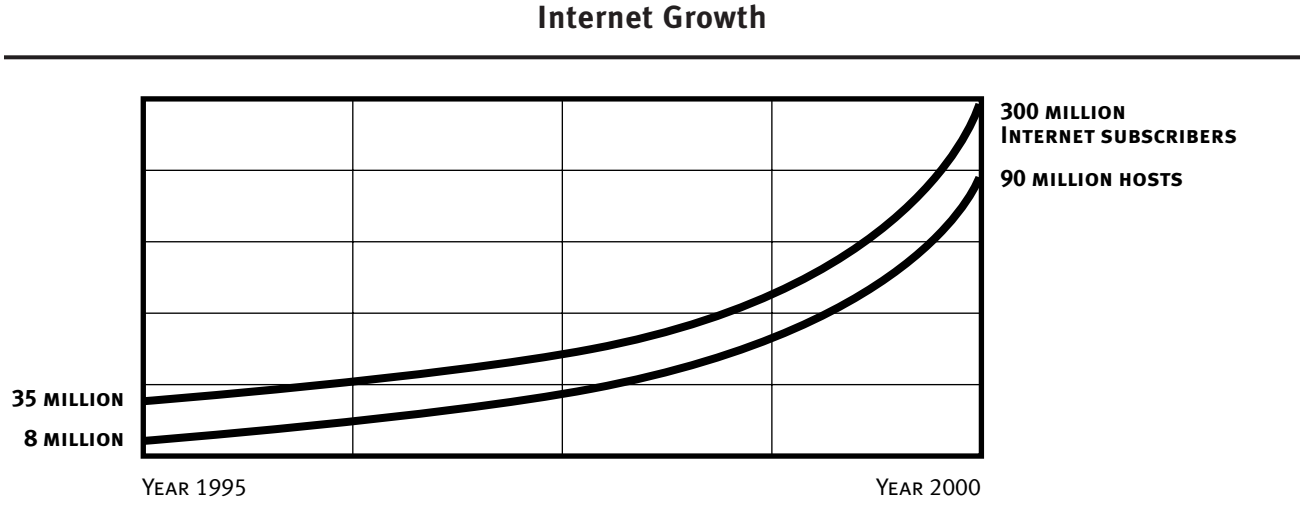


Figure 1. The growth in numbers of Internet subscribers and host systems has created the need for a new type of network management tool, one that can combine clients in logical groups and incorporate access devices into network views.

Beyond Traditional Approaches

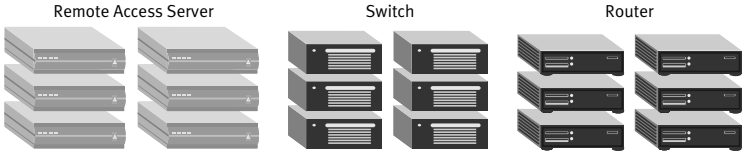
Traditional network management tools were designed to meet the demands of networks which were IP-based and contained comparatively few devices, and they did so with varying degrees of success. These applications could be launched from a network management platform, but there was no integration of the disparate solutions. Information could not be shared, and there was no common database to consolidate the information on network performance.

Today's complex network cannot be managed effectively with the old tools. Network growth is taking place predominantly at the access and switching layers, and traditional management platforms not only cannot manage access and switching devices, they can't even see them. As the network grows, more and more of it becomes invisible to traditional management tools, meaning more and more is out of your control.

The element-oriented nature of traditional tools is also the most severe limitation in today's environments. Element management applications with a "box at a time" approach may be adequate for legacy router networks consisting of several hundred devices. Faced with an environment of 10,000 or more port POPs, these tools are simply unable to cope (Figure 2).

Element Management

Figure 2. Traditional network management tools see only individual devices and are unable to handle today's network challenges



The new network demands, above all, the ability to manage the complete environment, not just the elements. Management-by-element will be replaced by tools that can see the entire enterprise at a glance and implement actions based on group definitions and group requirements (Figure 3).

With this paradigm in mind, we will examine several areas that are critical to managing the network:

- Enterprise discovery and mapping
- Enterprise configuration management
- Performance
- Fault monitoring
- Security and Accounting
- Scalability
- Quality of Service

Managing the Environment

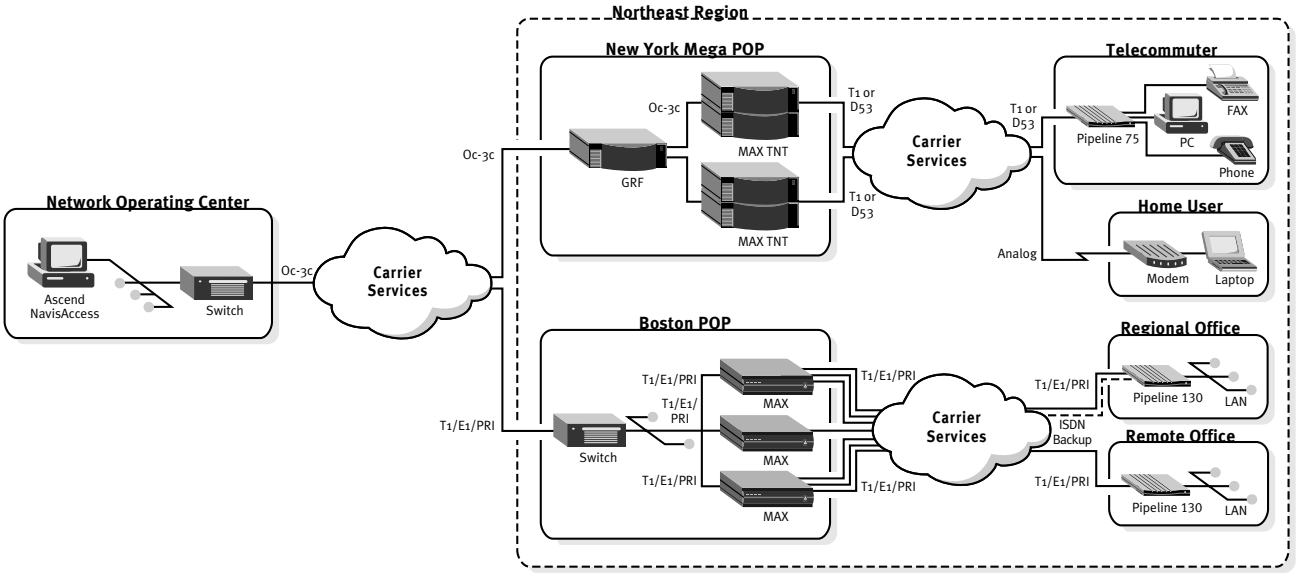


Figure 3. Next generation network management systems consolidate large, multiservice networks into easily manageable logical entities.

Enterprise Discovery and Mapping

The key to enterprise discovery and mapping is the depth of vision provided by the network management tool. Typically, network management tools map only the IP Layer (OSI Layer-3) and can not discover the Link Layer (Layer-2) and the Physical Layer (Layer-1). Yet it is precisely at the Link and Physical layers that network growth is most rapid and management needs most extreme.

Layer 1 discovery allows you to manage your physical interfaces (T1, DS1, E1, etc.) and trace precise element-to-element connections. Without a Layer-1 view, you cannot manage access devices and are not provided with a view of what is happening at the point of connection between you and your users. Layer-2 mapping and discovery depicts the virtual network level and lets you manage the wide array of network services (Frame Relay, ISDN, ATM) as well as the devices (switches, hubs) used in your network.

Combined with the IP Layer, a three-layer map provides an end-to-end depiction of your network that lets you view and understand the complex, inter-related nature of the different devices and services in your network. Without discovery and mapping of the network connections at all three layers, the network manager's ability to troubleshoot connectivity problems and monitor performance and Quality of Service are seriously impaired.

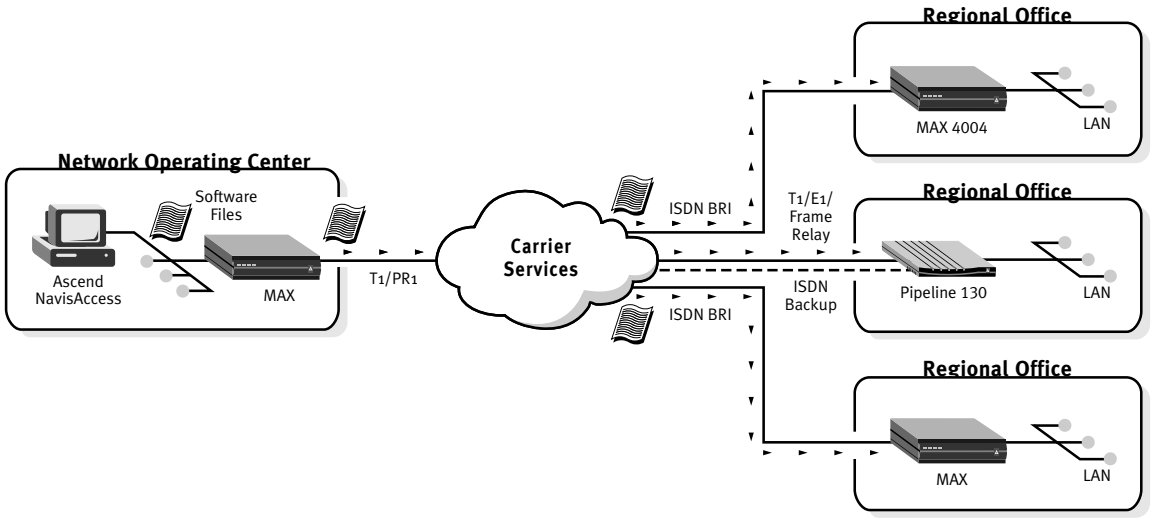


Figure 4. To manage today's complex and large-scale networks, network management software must support remote software upgrades and validation for multivendor equipment on remote LANS.

Enterprise Configuration Management

The largest cause of network failure is faulty device configuration. Network management applications must offer capabilities that make configuration easier and less error prone.

As a first step, network management applications should allow you to view the physical configuration of all equipment on the network remotely. The operator needs the ability to see precisely what is on each box — cards, interfaces, operating system software and configuration files. Further, information must be retrievable at an enterprise level via ad hoc queries, for example, "list all the ABC boards plugged in to my Ascend MAX access switches," or "list all the routers running version 4.6 software."

The operating software running on the devices in the network needs frequent upgrades. As devices grow in number, upgrading one device at a time becomes a cumbersome process, and doing so during high-usage hours can also drag down performance. Remote, scheduled software upgrades across multiple devices let you pre-schedule upgrades during non-peak hours, significantly decreasing operator hours and performance degradation (Figure 4).

Also, your management system must validate the software upgrade. For example, if an operator inadvertently sends Device A software to Device B, the management package must be intelligent enough to refuse this task and return an incompatibility warning. When the correct software is uploaded, the management system validates the delivery, making certain the software is not only delivered, but made active. Without the appropriate verification mechanisms, your first indication that a mistake has been made will be your network crashing.

Most importantly, the management software must handle configuration file change control. Change control encompasses many features, starting with automatic configuration file diffing. Since the majority of network disasters stem from errors in configuration changes, it is vital that the database keep a record every time a change is made. Configuration files should be automatically downloaded and compared to the file stored in the database, with alerts sent any time a parameter change is discovered. As a complement to this function, configuration file archives are maintained, allowing the operator to immediately drop back to a working version should any new changes prove problematic. When disaster strikes, the first priority of the management software is to return the network to an operational state. Time for testing and checking the faulty configuration updates must be postponed until after the network has returned to operation.

New device installation is facilitated by maintaining a set of configuration templates which can, with minor changes, be uploaded to the new equipment, eliminating the need to completely recreate configuration files every time a new box is installed on the network.

Finally, as configuration files contain security-sensitive information, file encryption is a key feature needed to ensure that files sent over the wire do not fall into the wrong hands.

Historical Trend Reporting

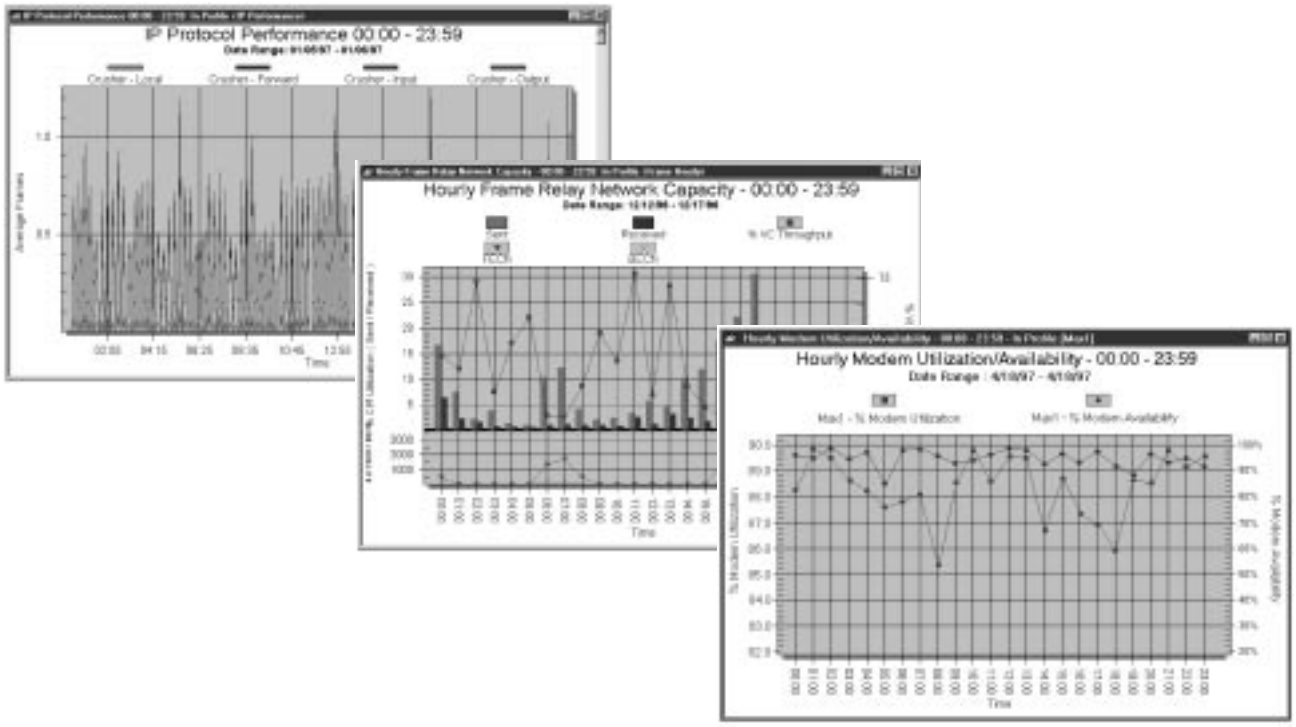


Figure 5. Aggregate performance reporting allows network managers to better understand usage patterns and conduct capacity planning.

Performance

If there is one word that has become inextricably linked with Internet and intranet, that word is “growth,” in terms of both user numbers and bandwidth demand. A key feature of any management tool is the ability to gauge performance — both as it impacts today’s business, and what it implies for tomorrow’s needs.

The basic performance management question has always been simple enough: how am I doing? Is performance up to par? Do I have excess capacity or am I pushing the limit? In legacy, router-based networks, the standard element-by-element, link-by-link view of performance made sense. Now, faced with an order of magnitude change in the number of devices, plus the additional complexities of mixed services, monitoring performance statistics one element at a time is an exercise in futility. Performance management must take place at the level of the environment, however defined, be it a POP, a region, a VPN, or network-wide.

In other words, network managers are no longer monitoring elements, they are monitoring aggregates. From a pure performance perspective, what an individual element or interface does is for all practical purposes meaningless. The element as such ceases to exist in the larger scheme, having been incorporated into the mass of elements that comprise the group. As a simple example, consider a POP running with 10,000 access ports. Is it worthwhile to view each connection as a separate entity? Of what use would such information be, assuming you had a staff large enough to view 10,000 ports, one at a time?

To be equal to the real-world tasks facing it today, the network management package must provide aggregate performance data, both in real-time and via historical trend reporting. It must supply detailed statistics such as: number of access ports that are being utilized in a POP measured every 15 minutes; average connect time for all calls; distribution of the speed at which the users are connecting; utilization by connection type; average number of calls per modem pool or hunt group. All this information is available for pre-defined periods of time and represented both graphically and numerically (Figure 8).

Only by delivering such information can the management application be a tool for capacity planning. Again, knowing that modem A is running at 50% of capacity, modem B at 80%, and so on, gives no indication of your real POP/network status. However, an aggregate view of all modems showing, for instance, 90% utilization during peak hours, is a clear indication that more capacity needs to be added if you expect to grow the user base. Breakdown by connection type is also important, because while dial-up utilization may be reaching full capacity, ISDN usage may be very low. Successful performance monitoring lets you pinpoint bottlenecks and areas of high utilization, ensuring that critical dollars are spent where they are most needed.

In terms of functionality, performance reporting is both automated and unattended. While spur-of-the-moment reports are needed from time to time, the bulk of performance reporting is done at regular intervals (such as daily or weekly). The reporting tools, therefore, only have to be configured and started once. Reports are accessible locally from the reporting tools and remotely via the web.

Service providers can also provide the reporting package to their customers so that they can monitor the performance of their piece of the network themselves. This way the service provider and his customers are looking at the same information as they discuss issues related to network performance and quality of service.

Fault Monitoring

A key feature of the network management system is the ability to make sense of the countless SNMP-based error and warning messages sent by network devices. At the most basic level, the management tool recognizes problems and provides visual alerts for the operator. Once an error is flagged, you can then easily drill-down through the network to locate the cause of the problem.

But alerting the console operator is not enough. Message volume must be dealt with as well. All network devices produce errors, which may or may not have serious consequences, and they often report hundreds of non-critical informational messages as well. Manually sorting through these thousands upon thousands of messages is impossible. Instead, management software correlates the events it records, and it identifies multiple messages which in fact refer to the same event, finally reporting one consolidated message rather than the dozens of individual events the network may have produced.

Message volume is also reduced using error threshold management. Threshold management allows the operator to monitor normal operating conditions in order to establish baseline error levels. Monitoring can be done by group, by device, by protocol, by interface, and so on. Once the typical error rates are known, the fault management tools are set to send warnings only when a dangerous threshold level is breached. This effectively filters out the numerous messages that are generated which are of no real concern.

A key means of tracking down errors is tracing paths between elements. With no more user input than the selection of a start and end point, the software traces the full, round-trip path between the two elements, showing all the links and devices traversed along the way, along with performance and error information. Clear indications are given for every point on the path where performance is degraded, routing loops exist, or errors are being generated.

Finally, support for multi-vendor device MIBs is necessary, as is support for other MIBs, such as those for protocols (IP, IPX, AppleTalk), services (Frame Relay, ATM), and interfaces (DS1, ISDN, T1/E1, OC-3c, HSSI).

Security and Accounting

Access to the network management application has to be limited to the personnel with the authority and the necessary skills to make changes, therefore several levels of access are available to the operations staff. The administrator has full rights to all devices and management functions. But not everyone should be granted that level of access. Other levels of operators, with admin-defineable rights, are also permitted. These rights are granular enough to grant access not only based on operator name, but also based on specific devices, device-groups, geographic domains and business domains. Flexible password and lockout options help refine your security options. And once operators log in, an audit trail feature keeps track of exactly what critical actions they take when logged on the system.

The management tool must also integrate with the security procedures you already have in place. Since RADIUS is the de facto standard in dial-up authentication, the management platform should work seamlessly with your RADIUS implementation.

Strong user accounting is essential to any business plan. As the flat-rate model for user billing gives way to higher value added services at premium rates, keeping track of user information is essential for proper billing and reporting. User accounting tracks not only connect time, but also the quality of service, making sure that high-tier customers are getting the extra performance they have contracted for, and that lower tier users are not drawing on resources for which they have not paid.

Scalable Network Management Architecture

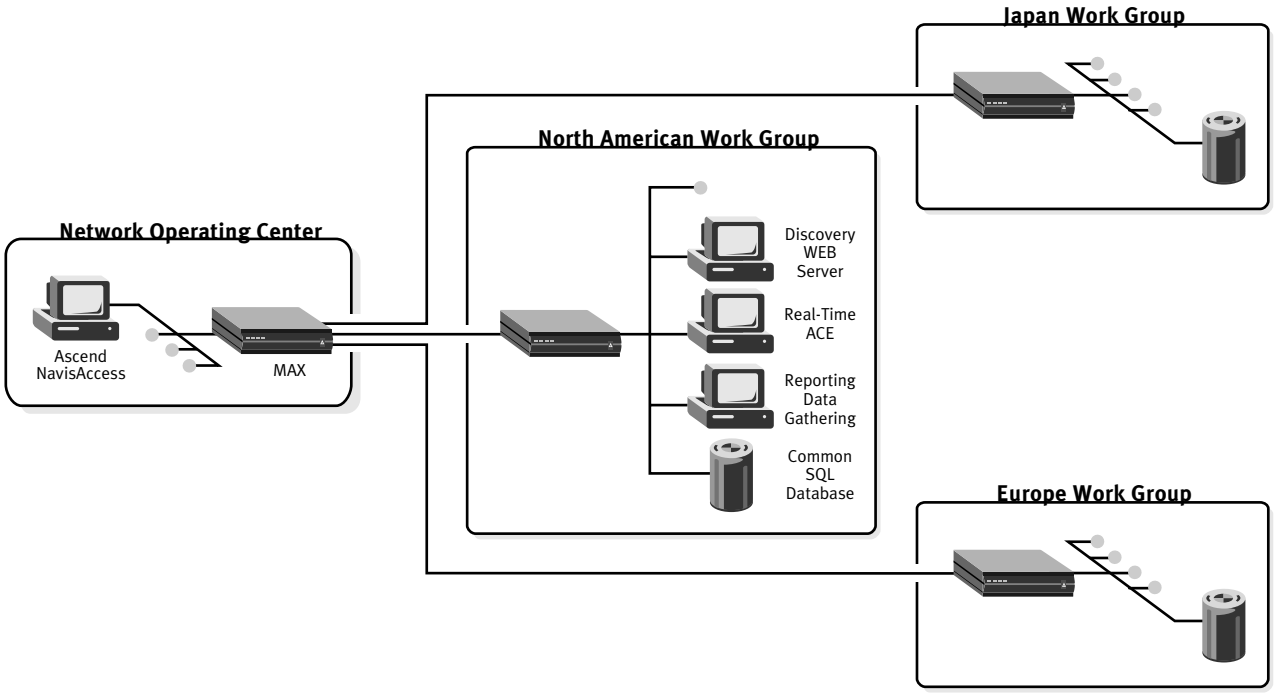


Figure 6. Distributed databases and multi-user console access allow delegation of management tasks according to business and staffing needs.

Scalability

As networks grow, the management functions need to be distributed. A centralized, single console management tool is not adequate to the task. Management systems must be able to support a client/server architecture, with distributed databases and division of tasks by console or work group. Such a system is configurable based on business needs, allowing separate business units to monitor their own network segments or, if preferred, one central data center to monitor the entire enterprise. Similarly, information gathering and reporting is available at any level: a single work group, multiple work groups, or the full enterprise. Within a work group, it is possible to distribute responsibility by console. For example, one workstation may be used for configuration management, another for performance reporting, and a third for fault monitoring, with all three working concurrently from a common database located on a server.

Quality of Service

Service providers must deliver on quality of service commitments. Premium prices can be charged for higher level services, such as resource reservation, priority service for time sensitive traffic, guaranteed delivery time, and committed bandwidth for value added services like Frame Relay. Network management software provides the data needed to verify that your clients are getting the services they have contracted for. Network management also allows the operator to understand the impact that resource reservations are having on the overall network capacity.

Ascend Network Management

Current generation management tools, designed for legacy router and shared hub networks, are not able to provide the power and flexibility you need. Ascend's NavisAccess™ delivers the next generation of network management: fast, flexible, able to grow with your network and able to manage that growth. NavisAccess lets you globally manage the environment while understanding the relationship between elements. It offers:

- Enterprise Discovery and Mapping
- Enterprise Configuration Management
- Performance management
- Fault Monitoring
- Security and Accounting
- Scalability for adding elements
- Quality of Service

Complete, end-to-end management software that leaves nothing to chance, that sees your network as a single entity and lets you manage it as such, that makes sure the bottom line is never compromised, and that brings a wealth of real-world network management experience to bear on your very real-world needs.

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

European Headquarters
Aspen House
Barley Way
Ancells Business Park
Fleet
Hampshire GU13 8UT, United Kingdom
Tel: +44 1252.360000
Fax: +44 1252.360001

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Asia-Pacific Headquarters
Suite 1908, Bank of America Tower
12 Harcourt Road
Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2669

15-03-WP