GENERAL DATACOMM

ProSphere NMS

Managing Multiservice Networks

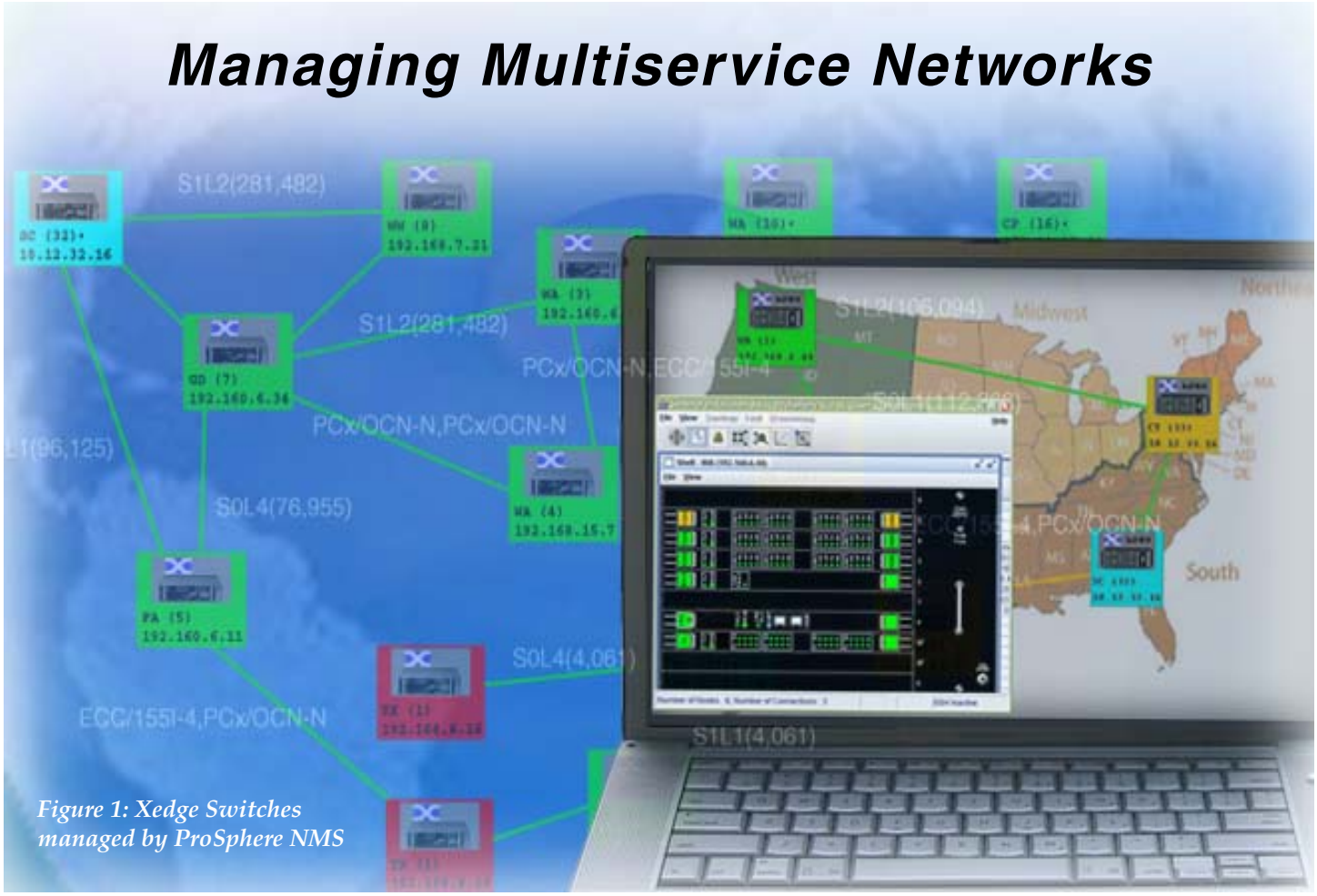

Figure 1: Xedge Switches managed by ProSphere NMS

The Multiservice Challenge

Managing diverse protocols, applications and topologies can be a challenge for operators of multiservice networks. Network managers require the tools that make the tasks of operating and maintaining such networks more efficient, secure and reliable.

ProSphere Network Management System (NMS) for the Xedge family of Multiservice switches provides a cost saving toolset to enable any service (TDM, ATM, IP, Ethernet, VLAN) over MPLS, ATM or Ethernet networks. End users transparently send and receive services and ProSphere simplifies the provisioning, monitoring, and securing of multiprotocol operations and maintenance.

ProSphere NMS is a suite of application tools that collectively provide a total network management system for enterprise or service provider networks. ProSphere supports the TMN/ITU 3010 standards according to the FCAPS (Fault, Configuration, Accounting, Performance, and Security management) model. ProSphere applications share status information and a common database so that alarms, for example, can be propagated from one user application to another, allowing the visualization of critical operation information at all times.

Feature & Benefits

- Smart graphical user interface
- End-to-end service provisioning for any service over any (IP, MPLS, ATM, VLAN or Ethernet) transport
- Status monitoring with global views of alarms and faults via polling or traps
- Automatic discovery and topology management with map views
- Element management with Explorer Views to facilitate node-slot-link and other object-oriented configurations
- Performance management with trend analysis to predict problems before they occur with automated-custom report generation
- Administrative-security management for operations
- Routing management
- SNMP-JAVA for platform independent-standard based communications
- Scalable client-server architecture to manage very large networks

Figure 1 (above) shows multiservice switches deployed in the Xedge network, managed by ProSphere NMS.

Topology Management

ProSphere provides automatic discovery of the SNMP based Xedge Multiservice Packet Exchange family of switches. As part of the topology manager, the automatic discovery process also helps enable the topology map where Xedge nodes can be displayed. The Topology manager discovery process also automatically populates the "Explorer View" window, the interactive graphical display and center piece of the Element Management application.

- Certain nodes can be filtered out during discovery.
- Nodes and connections displayed with link types and remaining bandwidth.
- Nodes are colored according to alarm severity.
- Nodes can be displayed with node names, IP addresses and/or icons.
- Configurable background image.

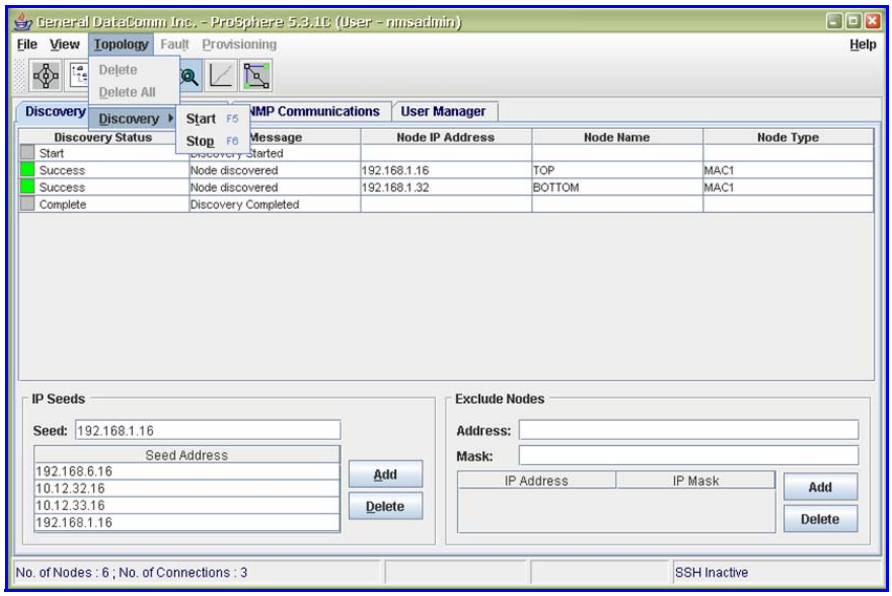

Figure 2: ProSphere AutoDiscovery

Element Management

The ProSphere Element Manager allows users a graphical means of modifying network elements in a given network by adding nodes, slots, cards, links and connections by means of the Explorer Tree view and associated menu-toolbar options. Users can also apply simple wizard processes to add and modify existing configurations.

The context sensitive Explorer tree allows appropriate configuration menus per object type. The element manager provides a hierarchical framework for organizing Xedge configurations including the enabling of source and destination ports as well as required signaling options.

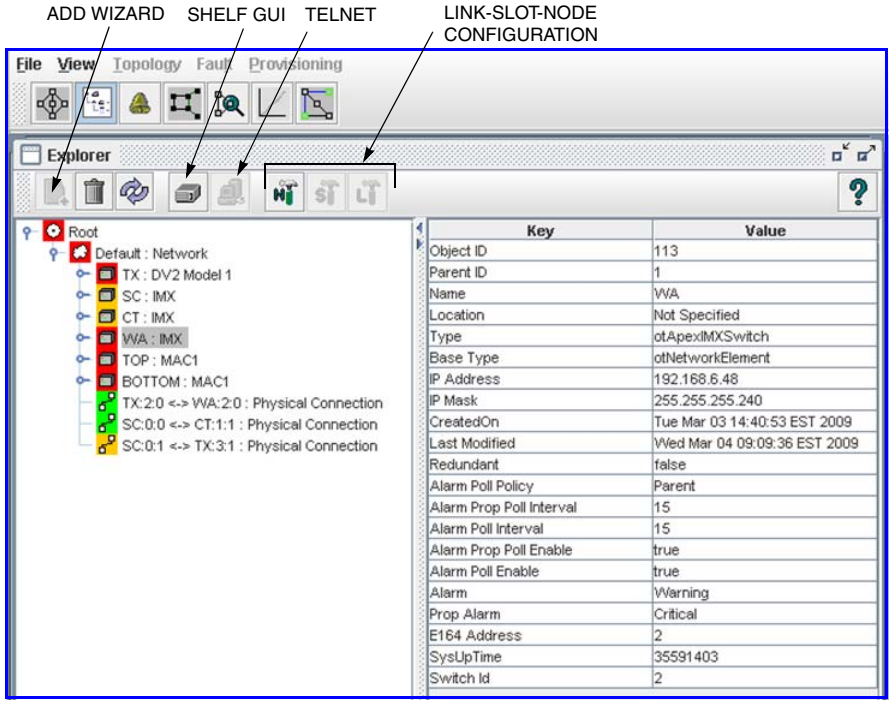

Figure 3: Configuration via ProSphere Explorer Tree

Fault Management

ProSphere Fault Manager provides comprehensive fault and status monitoring for the Xedge switch family. The Alarm View window displays active or historical alarms. The alarm status includes information that is acquired by a polling process or via SNMP traps.

Fault Manager includes a programmable alarm configuration tool that allows users to modify alarm severity, to mask alarms not to be displayed on the management alarm window, and to edit the alarm message descriptions suited to operator requirements. An alarm polling editor allows users to change the polling interval or disable polling for a node. The flexibility of the Fault manager allows operators to drill down and isolate faults and solve problems quickly. *Figure 4* shows an example display of the Active Alarm screen.

ProSphere also provides an email notification feature that automatically sends an email regarding specific events to remote analysts/technicians. Operators can select which type of event would send email notification to targeted users.

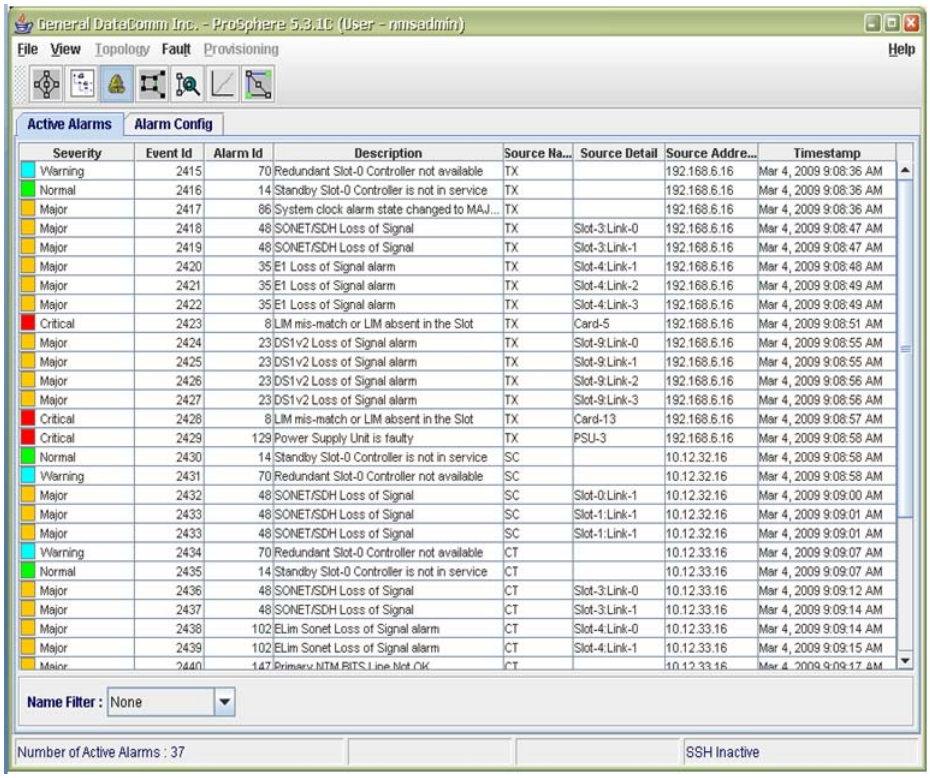

Figure 4: ProSphere Active Alarm Screen

Service Provisioning

ProSphere's Service Provisioning Manager (SPM) eases the management of multiple services over any transport. Using a variety of techniques including wizards, users can select a service to match with a desired transport type. All packet-based connections (for example, Pseudowires) can be mapped according to a policy-based quality of service via a Frame Transport Specification or TSPEC.

ATM connections are specified by ATM forum based parameters for Virtual Paths and Virtual circuits with appropriate QoS for CBR, VBR real time, VBR non-real time, or UBR. *Figure 5* shows an example ProSphere SPM screen being used to manage Pseudowire connections over MPLS.

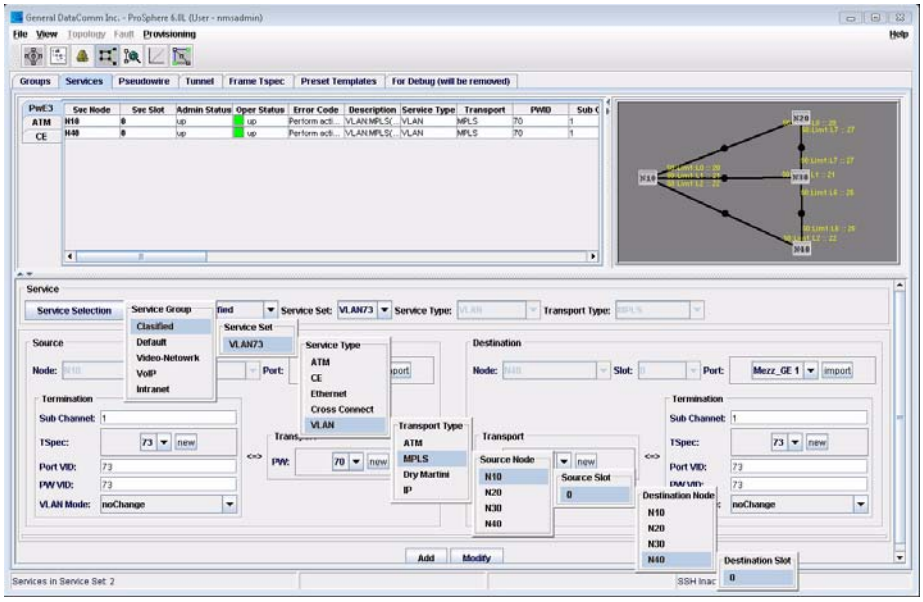

Figure 5: ProSphere Service Provisioning Manager (SPM)

Performance Monitoring

ProSphere's Xedge Performance Monitoring (XPM) allows operators to proactively intervene in network operations based on performance trends. XPM employs SNMP polling of the Object Identifiers (OIDs) associated with the measurement of statistically significant Xedge parameters.

ProSphere XPM collects and displays two types of statistical data:

- Error Statistics (physical/logical)
- Utilization Statistics (physical/logical)

Examples of collected data include: bandwidth, errors, lost cells, number of retires, cell and frame counts, number of collisions, and utilization at the link, pseudowire, packet and ATM VC statistics. *Figure 6* shows a ProSphere XPM report on utilization and errors.

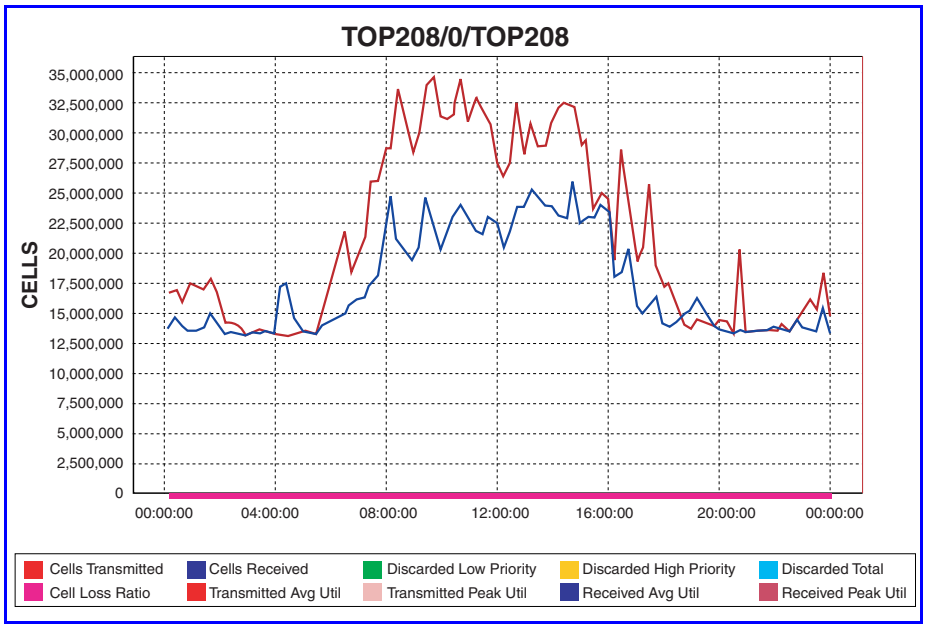

Figure 6: ProSphere XPM Report (graphical format)

SNMP polling intervals for performance monitoring are user-configurable for real-time monitoring and historical trend analysis. Users can view the collected statistics in graphical or statistical formats, as well as in a variety of standard or on-demand reporting schemes.

Routing Manager

For wide area networks where operators wish to define static routes for ATM based networks, ProSphere provides an automatic route generation tool that uses a map-based GUI to generate and manage static routing tables when there are SVCs or SPVCs in the Xedge network. The ProSphere Routing Manager (RTM) simplifies the setup of static routes and the calculation of backup routes from assorted menus and screens.

Route calculations can be based on node and link cost, on number of hops or bandwidth availability. Views of routes generated and active can be visualized from a source or destination perspective.

The Xedge platform also supports automatic route calculation and generation using the PNNI, RSVP-TE, and OSPF protocols. *Figure 7* shows a ProSphere RTM display.

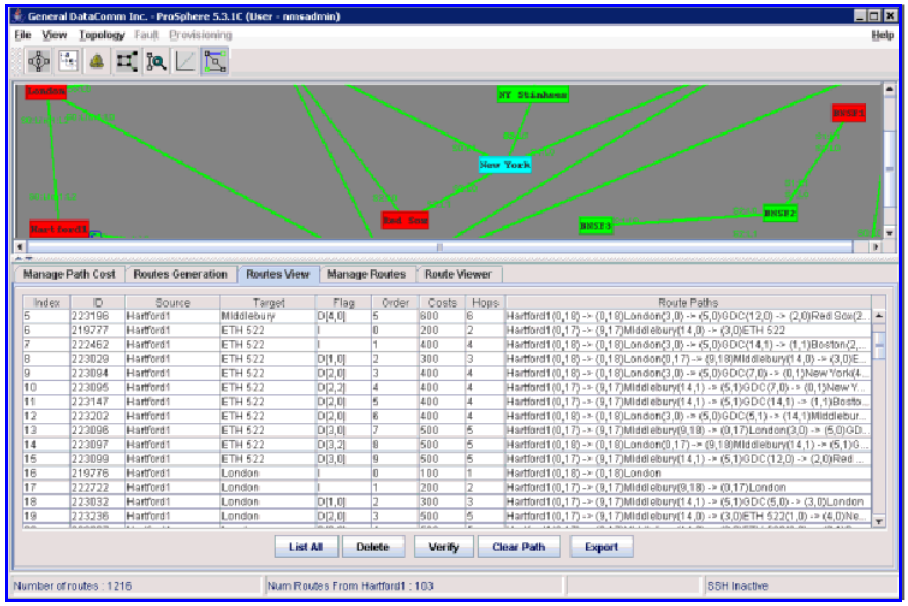

Figure 7: ProSphere RTM Routes Display

GENERAL DATACOMM

ProSphere NMS

Secure Management

ProSphere provides comprehensive user access management tools for secure network operation. Four user types are supported: Monitor, Operator, Admin, and Super User. Each type has distinct permissions that access given ProSphere applications. Users can only be created and assigned access privileges by a Super User. *Table 1* defines access permissions associated with each user type.

A User Manager GUI in the ProSphere Client application allows the addition and removal of users and the changing of passwords for existing users. User profiles are maintained on a ProSphere Server so that all clients communicating with the server have access to the same set of user profiles.

Table 1: User Types & Permissions

SUPER USER	Super Users have all network management privileges, including user management.
ADMIN	Admins have all network management privileges, but cannot create or delete users.
OPERATOR	Operators have all alarm and circuit privileges, but cannot change configurations or network topology.
MONITOR	Monitors have read-only access to ProSphere applications.

Secure Access

For non-secured installations, communication between Xedge MPSx nodes and ProSphere is accomplished using standard protocols such as FTP, TFTP, SNMPv1 and Telnet.

For secure installations, communication between Xedge MPSx nodes and ProSphere NMS is accomplished using the following security protocols:

- SCP (Secure Copy) is used in place of FTP and TFTP to transfer files.
- SSH (Secure Shell version 2) is used in place of Telnet to access the Xedge node menus.
- SNMPv3 is used in place of SNMPv1 to set and read variables within the nodes.

Secure installations of ProSphere NMS with SSH, SCP and SNMPv3 security protocols can protect management access and operations across the Xedge network.

When SNMPv3 is used for authentication, the encryption method used is MD5 or SHA. When SNMPv3 is used for data, the encryption method used is DES or AES.

Audit Trail

ProSphere's Audit Trail supports logging, tracking, monitoring and timestamping of both completed and attempted user logins as well as any modifications of provisoning or system configurations.

Audit trails allow the operator to trace the transactions that affected the network management system. Audit Trail stores information on such key events as:

- successful and unsuccessful logons.
- denial of access resulting from excessive number of logon attempts.
- privileged activities and other system-level access.
- session logout, lockout, or timeout.
- deletion/adddition of networks, nodes, slot controller, LIMS, and links.
- deletion/addition or modification of services (PVC's, SPVC,s, LSP Tunnels, PWE3, etc.

Specifications

- Platform Requirements
  - Database: MYSQL 5077
  - PS Server: Windows Server 2008 R2
  - PS Client: Windows 2008 Server, Windows 7
- Hardware Requirements
  - Processor: 2 Gig minimum
  - Memory: 2 Gig minimum per 50 nodes
  - 32 or 64 bit machine
- Scalability:
  - Supports up to six concurrent client sessions
  - Supports very large networks
- Northbound Interface: JAVA RMI
- Device Communication: SNMP V1, SNMP V3
- Conforms to RFC 1884 IPV6 addressing schemes.

0155_pros_ds05Dec15