Alternatives to clearVISN IntraNet Manager for Managing a Multivendor Switched or Routed Network

Introduction

StonyBrook Software's Router Manager, later renamed IntraNet Manager, was one of the first "non-platform" or "value-added" network management products to provide detailed information on routers from multiple vendors. Router Manager configured and managed routers from a variety of hardware vendors. IntraNet Manager added Layer 2 switches to the set of managed devices, and it also added several features already found on all Enterprise Management platforms. Since many clearVISN customers had routers and switches from a variety of vendors and had expressed the need for a single product with which to manage them, IntraNet Manager was incorporated into the clearVISN product suite.

Many of the features in IntraNet Manager V2.0, however, overlap with those of the leading Enterprise Management platforms. Functions such as Autotopology, Alarm Handling, and MIB browsing are integral to all Enterprise NMS platforms. The Enterprise NMS platforms are all much more feature rich and mature than IntraNet Manager in these areas. In other areas such as Performance Reporting and Path Tracing, IntraNet Manager is somewhat equivalent to the platforms. On the other hand, IntraNet Manager has a slight advantage in switch and router status and performance displays for specific vendor devices when compared to most Enterprise Network Management Systems. This is because IntraNet Manager has built-in knowledge of switch and router devices from several leading vendors. Only one of the leading Enterprise NMS, Cabletron's SPECTRUM, contains intelligent device models for many devices from a number of vendors.

This paper explores the relationship among Element Managers, Mid-level Managers, Enterprise Managers, and so-called value-added applications like IntraNet Manager. It reveals that the majority of IntraNet Manager features are duplicated in one way or another on the Enterprise Management platforms. These features were incorporated into IntraNet Manager to aid the user who wanted to use IntraNet Manager without an Enterprise NMS. If the user also has an Enterprise NMS, and most IntraNet Manager users do, then these duplicate features will not be used since the Enterprise NMS products provide a more advanced solution. Examples from SPECTRUM Enterprise Manager are used to illustrate the overlap, but many of these functions are also available on other Enterprise Network Management Systems.

Categories of Network Management Tools

Element or Device Managers

IDC defines network element managers as “software products that enable IS to remotely configure, monitor, and support devices (hub, router, switch, or sets of those devices) using SNMP MIB data.”

Element Managers are primarily configuration tools, although some products have evolved to include NMS functions such as autodiscovery, MIB Browsers and alarming. Almost all Element managers can be run standalone with the appropriate Operating System, although some have an NMS as a prerequisite. Some vendors bundle mid-level or even Enterprise Management System software with their element managers at an appropriate price. Virtually all Element Managers are produced by the vendor whose hardware is covered by the Element Manager.

Mid-level Managers

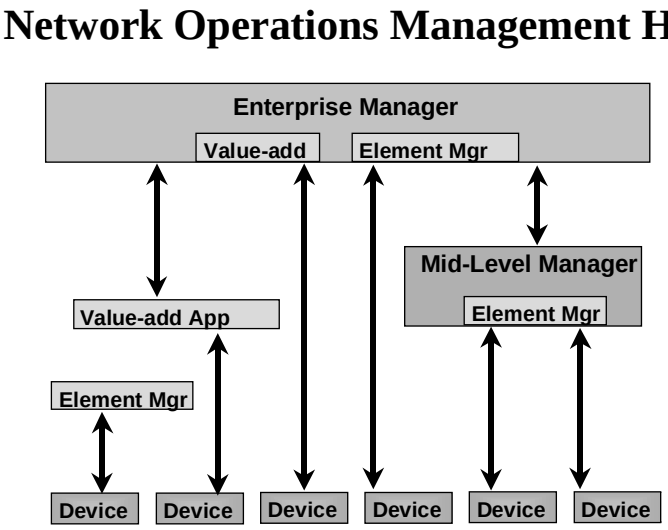
Mid-level Managers have the same base level features as an Enterprise Manager, however Mid-level Managers run on a lower end machine, and differ in scalability relative to the Enterprise Managers. They have IP Autotopology, alarm handling, and MIB browsing capability. They also cost about 1/10th the price of an Enterprise Manager.

Enterprise Managers

The Enterprise Managers’ claim is that they can manage systems as well as networks. They have advanced IP Autotopology, and numerous add-on’s are available from third parties. These EMS typically have umbrella names and include multiple products.

Another common feature of Enterprise NMS is that most functions are at least partially customizable by the user. The user can tailor features to suit their needs. A downside to all this flexibility though, is the need for extensive training in order to put it all to effective use.

Hierarchy Picture



Value-Added Tools

Value-added tools differ from Element Managers because they are not usually provided by the hardware vendor for a specified set of that vendor's devices. These tools are primarily network monitoring applications with a minimal set of configuration functions. They are geared toward monitoring a specific aspect of a network as opposed to in-depth management of a particular device type. Such tools often apply expertise targeted at solving a specific network management problem area that is not solved by Element Managers, Mid-level Managers, or Enterprise Managers. Industry standard MIBs, such as RMON, are often used to cut across vendor differences.

IntraNet Manager Feature Comparison

IntraNet Manager performs most of its functions through “applets”, or sub-applications of the main framework. Applets exist to set up thresholds and monitoring, to collect and view performance and fault data, for changing device configurations, and for viewing device status. One of the early aspects of IntraNet Manager that attracted network managers was its unique ability to monitor a routed network well from a PC. Now, however, several Enterprise NMS offerings run on Windows NT, including SPECTRUM, CA Unicenter TNG, Tivoli NetView, and HP OpenView. The fact that IntraNet Manager runs on a PC is no longer a differentiator.

Autodiscovery and Mapping

The combination of these functions discover SNMP and IP-only devices on the network, including how they are linked at the network layer. Then, a map can be automatically drawn by the application to display the discovered devices and the IP subnet topology. When this map is drawn automatically, the function is referred to as Autotopology. In IntraNet Manager, these functions are represented by the Explorer and by Device Discovery. The map is constructed with hierarchical views of the network, the top level showing just the routers and subnets. The map displays how devices are connected from an IP Routing perspective. Hierarchical navigation of the topology and “Find” or jump-to navigation is also included.

All Enterprise NMS platforms provide this functionality, and, in all cases, the Autotopology provided by these platforms is more evolved and mature than that of IntraNet Manager. Furthermore, the platforms can not only discover, but manage servers and end nodes. Enterprise NMS vendor and/or third party add-on applications are available for in-depth management of the systems and the applications that run on them.

The user can click on a map icon representing one of the network devices, and launch device-specific views or applications for more detail about that device. IntraNet Manager and SPECTRUM both have integral device-specific models for many different device types. With all other Enterprise NMS platforms, the user will typically launch the hardware vendor-provided element management application, as the platform only includes a generic MIB II device model.

Trap Handling and Alarming

These functions involve receiving SNMP Traps from network devices, logging them to a file, assigning a severity level to the event and appropriately highlighting the problem device(s) on the topology map. There is usually provision, as well, for notifying the user audibly, or via email or pager.

The general category of alarming is encompassed in IntraNet Manager by multiple features and applets, each having a different name – Threshold Manager, Alarm Monitor, Incident Monitor, Event Viewer, Alert, System Log Monitor, and Trap Forwarder. Following is a brief explanation of what each applet does:

- Threshold Manager is used to set alarm thresholds for a predefined set of error classes including protocol, system, interface, MAC, and Bridge objects.
- Alarm Monitor polls a single device or a group of devices for status and errors; it works in conjunction with the Threshold Manager to determine whether a given error condition is acceptable.
- Incident Monitor allows the user to select a device or group of devices and to display an Event report for that device or group. Events are classified according to severity. The report can be re-sorted by any column.
- Event Viewer is a background application that captures the SNMP Traps and other events. When active in the foreground, it also displays pie charts of event breakdown by severity and by family.
- Alert activates interface status fault detection on devices or groups. Interface status thresholds must be pre-configured using the Threshold applet. The Alert report contains a summary of events per device and interface.
- System Log Monitor is analogous to the UNIX “syslog” function, and uses service port 514. The report is similar to other event reports, but only contains messages sent by devices to the syslog port.
- Trap Forwarder forwards all events received by the application to a maximum of twenty IP addresses.

All of the Enterprise NMS platforms do a respectable job in this area. They also tend to scale better and to offer more in the way of alarm notification. SPECTRUM, by way of example, converts SNMP Traps from devices into Events, which are logged, and can be viewed in the Events View. Events can be filtered to only display events for particular devices or device types. Various events can also notify the appropriate device model, which can, in turn generate an alarm. Alarms are logged in both the Event Log and the Alarm Manager log. In the Alarm View, a user can be assigned to troubleshoot the problem.

SPECTRUM goes further in Fault diagnostics by analyzing the topology in order to distinguish where the fault actually lies versus where its effect is propagated. It can do this because of the intelligence built into the device and topology models.

Another SPECTRUM feature is the ability for the user to customize the way that alarms roll up the topology view. In other words, how does the composite severity of the alarms at one level in the topology hierarchy affect the alarm conditions at the levels above? SPECTRUM also includes an application called WatchManager, which allows the user to easily add thresholds and log historical data for any model.

MIB browsing

IntraNet Manager includes a basic MIB Browser and MIB Compiler. It also has many of the vendor-specific MIBs already compiled for routers and switches. It has the flexibility to allow user-created MIB “profiles” to be created for a particular device type.

Again, all Enterprise NMS platforms have full-featured and robust MIB Compilers and Browsers. SPECTRUM’s MIB Tools include a browser and editor; the editor allows you to customize a particular vendor’s MIB to your own device’s configuration. You can also set up a database of quicklinks to MIB Browse specific devices. SPECTRUM offers greater flexibility and more features than does IntraNet Manager for browsing MIBs. It has a “radar” view for faster navigation of large MIB Trees as well as an ASCII string “Find” feature. But SPECTRUM offers real power with its ability to let the user create new model types by editing a similar model type and importing the MIBs for the new device. This allows the user to organize the MIB information in a way that makes sense for that device type.

Performance Reporting

IntraNet Manager's Schedule Wizard is key to its ability to do performance monitoring and reporting. The user must first select the days and hours during which the monitoring is to take place, the application to be run, and the devices on which a particular schedule is to operate. Data collected is stored in the "historical database", where it can later be retrieved during report generation. Data is only stored in the historical database when it is collected by a scheduled task. Schedules can be stopped or resumed by the user at any time. When you go to generate a report in the Device DB program, you select a schedule that you created by name as the data source for the report. You can also schedule reports to be generated at preset times. Background applications that can be scheduled include performance by protocol, by interface, by device CPU, and by CIR for switched services.

In addition to historical reporting, IntraNet Manager has numerous interactive performance trending applets. Many of these applets generate charts that break down performance by traffic as follows:

- Input – the traffic level(s) on the Receive side of the device or port
- Local – how much traffic the device generates vs. forwards
- Forward – how much of the traffic is forwarded by the device or port
- Output – the traffic level(s) on the Transmit side of the device or port

There are numerous performance applets for reporting on a great variety of router parameters. The device(s) must support the appropriate MIBs for these applets to work; therefore some are vendor specific. Some of these applets are

- Performance Distribution – breaks down traffic by protocol for each of the four charts above
- Top 10 Utilization – displays the utilization in a bar chart for the 10 busiest ports; the graph automatically adapts to devices with fewer than 10 ports
- Protocol performance – for IP, IPX, and AppleTalk
- Virtual Circuit Utilization – for Frame Relay DLCI
- Ethernet and Token Ring Statistics – for 3COM only
- Mean Packet Size Distribution – for Cisco only
- Output Queue Length

- X.25 Statistics
- ICMP and SNMP Statistics

Many SPECTRUM views contain charts, graphs, or tables which display data related to the view. For example, a Performance view uses the multi-attribute line graph to track frame rates, errors, collisions and load. The Device view uses bar gauges to indicate port activity and status. A detail view within the Performance view uses pie charts to depict frame breakdown and errors. Many applications have information views containing tables. The particular attributes presented in the charts, graphs, and gauges are specific to the particular device.

Access to device performance information can be accessed in several ways. From the device model icon, you can go to Device View and access performance information tailored to the device. Typical performance views will include current, average, and peak values in a tabular fashion in addition to a graph that starts at time zero with the opening of the screen. You can also go directly to a device performance view by double clicking on the performance zone of the device model icon.

The Reports application lets the user specify a variety of historical reports including Alarm, Event, Inventory, Relational, Statistical, and Up/Down. In the category of Statistical, you can specify frame rate, error rate, collision rate, utilization rate, and hard error count reports. You can even derive calculated fields based on a variety of expressions. Output formats can be specified as tabular ASCII, tabular postscript, graphical display, graphical postscript, and GIF. The tabular reports can be sorted by various criteria, and reports can, of course, be scheduled for generation at specified times.

Configuration Management

IntraNet Manager does not have applets other than the MIB Browser for direct manipulation of specific MIB objects, but it does allow the user to upload configuration files from routers, edit them and download the edited configuration. It also has a wealth of configuration monitoring applets for routers, switches, and switched services.

The uploading or downloading of configuration files for routers can be scheduled using the Schedule Wizard. The uploaded file is automatically compared to the master configuration file for that device; an alarm is generated if a mismatch is found.

Just like there are numerous applets for monitoring performance statistics, there are applets for the interactive collection and display of configuration information. Some of these applets only rely on MIB II information, while others rely on specific vendor MIBs. Some of these applets are:

- Route table, Address table, and Translation table display – for IP, IPX, and AppleTalk
- Interface table display
- X.25 circuits display
- X.25 Administrative table and Operation table display
- Neighbor table for ISDN
- Frame Relay Interface Configuration
- Bridge Learned addresses display
- Source Route Bridging display
- Chassis View display – shows the number and type of interfaces on the device

In SPECTRUM, there is a "device topology" view that shows the configuration and connections of a device. It will display the slots, if the device is a chassis, or just the interfaces when the device is a single box. It will also show the device icon for the device attached to a port on the device.

In addition, SPECTRUM has an application called Enterprise Configuration Manager (ECM) for managing multiple device configurations. The associated SPECTRUM device model must be installed prior to using ECM. ECM is designed so you can divide the tasks of network management between the network experts who set policy and create the configurations for the network and the system administrators who manage day-to-day operations. SPECTRUM has built-in security to allow the administrator to only allow certain operations for some users and all operations for others.

ECM allows you to create configurations with templates or manually without templates. A template is a list of attributes for a specific device. You can use templates to capture the configuration of a device. When you use templates to capture the configuration of an existing device, ECM captures the instance IDs, if any, and the values of the attributes listed in the template. The attributes listed in the template plus the instance IDs and attribute values captured by ECM make up the new configuration.

You can compare the configuration of one device to a master configuration file, compare the configurations of two devices of the same type, and schedule configuration loads. The chief difference between SPECTRUM and IntraNet Manager is that IntraNet Manager lets you capture only the non-SNMP configuration of many different routers, while SPECTRUM allows you to capture the SNMP configuration of any device plus the non-SNMP configuration of most Cisco routers.

Path Tracing

This is called the PathFinder tool in IntraNet Manager. It allows you to trace the route forward and back between any two IP devices. PathFinder is launched from the map by selecting the source and destination devices. A round trip path is drawn on the screen showing each device that forwarded packets from the source to the destination and back. The type of each link along with error and utilization percent at the input and output ports of each device along the path is displayed. The link is colored green, blue, or red according to how the error and utilization thresholds compare to the actual values.

Typically, Enterprise NMS systems can do a path trace from one IP device to another across the routers in between. There may be slight deviations in how the path is displayed and what kinds of errors get detected along the path. Most do not automatically display the return path. SPECTRUM's path tracing application is called PathView, and it gives the user a choice of discovering just the router portion of the path, or all the devices along the path. A status window is opened displaying activity and progress; this information can be printed or saved to a file. It allows you to specify a maximum number of router hops to reduce the search time when the destination is unreachable. Alternatively, you can specify a timeout value after which the search will stop. It is best to have run Autodiscovery prior to running PathView, as the devices between the routers will have already been discovered. PathView does not diagram the return path, nor does it provide performance information on each link in the path.

Special Considerations for Switched WAN Services Management

IntraNet Manager has the ability to model a switched carrier-provided service "cloud" as a virtual element, so that many of the common applets will function on the virtual element as well as on a real device. Virtual elements represent dynamic groups of devices connected through a switched service. The user can view alarms, interfaces, and Top 10 utilization on the cloud just as if it were a device. For example, the Virtual Elements Group Interface Table feature allows you to view information for each interface of every device that makes up the virtual element.

The map can show subnet information and a circuit map for virtual circuits in the cloud. It works for Frame Relay, X.25, and ISDN as long as the devices attached to the switched service support the proper MIBs.

Frame Relay virtual circuits can be defined, then data can be retrieved from the linked devices about the circuit. This information includes the DLCI, or Data Link Connection Identifier, the state of the DLCI, the CIR, or Committed Information Rate, the utilization threshold, and a throughput threshold for the virtual circuit. You can use the Virtual Circuit Utilization applet to view utilization by DLCI on an interface.

Applets also exist for X.25 and ISDN. For X.25, there is a Circuits applet and a Statistics applet. The Circuit applet reports 20 different parameters for the virtual circuit, while the Statistics applet reports values for 24 different counters per interface – the aggregate total for all the virtual circuits on that interface. The ISDN applet reports 17 bits of Neighbor Table data.

All Enterprise NMS are not created equal when it comes to managing a switched WAN network. However, there are add-on packages from other vendors, who are considered “partners” with the Enterprise NMS vendor, that do an excellent job of monitoring Frame Relay, X.25, or ISDN networks. Some of these products use hardware instruments or probes for collecting detailed data. Some example products include NetScout Systems’ WAN Probe coupled with NetScout Manager Plus, Visual Networks’ Visual UpTime coupled with their probes, and Concord Communications’ Network Health.

Cabletron offers ISDN management features as part of the core and a separate add-on module called Frame Relay Manager. The ISDN features really pertain to “non-persistent connections”, so dial-up analog modems are included as well. Three categories are covered – dial backup links, dial on-demand links, and bandwidth on-demand links.

The Frame Relay Manager module supports any device that uses the RFC 1315 Frame Relay MIB. You can monitor down to the PVC level and generate statistical reports such as throughput and congestion per PVC. Alarms can be generated when a given PVC, as opposed to the whole interface, is experiencing congestion or failure. In a topology view, you can see all devices that are part of the Frame Relay cloud. Autodiscovery will resolve connections down to the Data Link Connection Management Interface (DLCMI) level.

Summary and Conclusion

IntraNet Manager provides many focused features for management of a routed network, however, Enterprise Network Management Systems provide most of these features and a lot more. Many of IntraNet Manager's features are redundant to those provided by an Enterprise NMS, and therefore actually get in the way of effective management of the network. When a network manager attempts to perform the same function using two different tools, he or she is less proficient on either tool than if only one tool was being used. It also requires more time to keep two tools updated with changes on the network.

IntraNet Manager provides a slight edge over Enterprise NMS in routed path tracing, management of configuration files for routers, and clearly provides more features for monitoring switched WAN services such as Frame Relay and ISDN. Enterprise NMS, on the other hand, excel at Autotopology, Event and Alarm Management, MIB Browsing, and flexible reporting. In conjunction with integrated Element Management applications and value-added Frame Relay packages, the Enterprise NMS solution is superior for configuration management and Frame Relay management as well.

Copyright