White Paper

Service Assurance Solutions for Multi-System Operators

Jim Lochran, VP–Solutions Strategy
Communications, Media and Entertainment

June 2006

Table of Contents

CA Approach to Unified and Simplified Management 3
Operational Transformation 4
CA Service Assurance Solution for MSOs 4
Fault Management 6
Performance Management 8
Service Management 12
Security Management 14
Conclusion 15
About the Author 16

Cable Operators are faced with the daunting task of delivering an ever increasing range of services over an extremely complex mixture of technologies. The result is an increased dependence on systems for customer service and infrastructure management, ranging from customer care, to billing and provisioning, to service assurance. The advent of high revenue services like Video-on-Demand (VOD) and must have services such as VoIP have extended the complexity of these Business Support Systems (BSS) and Operational Support Systems (OSS), and highlighted the need for a set of infrastructure management tools significantly more simplified and unified than ever before. Inside any major Multi-System Operator (MSO) Network Operations Center, one would ordinarily find several different management consoles in use, each managing a different facet of the overall service delivery infrastructure. These consoles evolved as the network was transformed from a video distribution channel into a full service, 2-way, IP-based multi-media service delivery platform. The transformation required the MSO to deploy management systems from each device vendor in order to manage that segment of the service delivery infrastructure. Disparate consoles provide MSOs with only a limited view into the performance of their service offerings and have led to a variety of challenges, including:

- Silos of information between legacy and next generation systems
- Operator information overload
- Inability to understand the impact of outages and/or service degradation on subscribers
- Dependency on manual processes for restoration and maintenance

CA Approach to Unified and Simplified Management

CA (formerly Computer Associates) addresses these challenges with its Enterprise IT Management (EITM™) strategy, providing solutions that unify and simplify the management of enterprise-wide IT. Its SPECTRUM® and eHealth® solutions have a rich history in fault and performance management, with over 100 patents in key technology areas such as Infrastructure Modeling, Technology Relationship Mapping, Root Cause Analysis, Fault Isolation and Integration of Network and Systems Management. CA solutions extend from OSS service assurance to back-office BSS assurance along with a rich portfolio of security and systems management solutions. CA solutions are used by some of the largest MSOs in the world.

The SPECTRUM and eHealth solutions have been serving the MSO needs since 1995 and have continually evolved to support the range of emerging services the MSOs need. The expansion continues today and now includes solutions for:

- DOCSIS 2.0
- Voice over IP
- Video on Demand
- Digital Simulcast
- HFC Plant Management
- Return Path monitors
- End of Line Monitors
- Wireless Extension
- Digital Wireless
- Commercial Service
- Fiber Services
- IPVPN
- Voice

Operational Transformation

A key step in addressing the challenges before MSOs today is the adoption of a transformation model (Figure 1) for service assurance operations. The need for such a transformation is driven in part by the rising complexity of the services being delivered such as voice, and the rising demand for increased service levels associated with premium services. As a result the current operations model needs to be transformed from an Active, manual driven process to a fully integrated service centric Business Driven model in which problems are anticipated and addressed before customer services are interrupted.

Functionally, this transformation requires alignment across the various MSO organizations (Engineering, Operations, Marketing, etc.) with the goal of providing a higher level of service to the customer. Alignment is crucial since the requirements of a service-centric operation cannot be addressed solely at the operational level. For example, service development / engineering must include manageability as part of its service definition, and ultimately vendor selection, in order to ensure that the end product can be properly managed. In addition, operation must have operational support systems and business support systems in place that can quickly adapt to new technologies and services to implement the appropriate instrumentation to deliver a service-centric approach.

The remainder of this paper will focus on the operational support system, specifically the service assurance tools required to facilitate the transformation to a service-centric operation.

CA Service Assurance Solution for MSOs

The MSO infrastructure is a constantly evolving collection of technologies that introduces many unique management challenges. Point tools and proprietary solutions have been implemented over the years to provide basic visibility into the health of the infrastructure. Unfortunately these tools are often not integrated and provide little correlation between their management domains. This forces operations to perform complex correlations manually and make root cause determinations based on their experience and knowledge. The end result is an inefficient and costly monitoring solution that can be quickly overwhelmed during a major outage.

CA's service assurance solutions, SPECTRUM and eHealth, were developed from the ground up to be multi-vendor, multi-protocol and multi-technology platforms. With these solutions, CA offers the industry's broadest catalog for infrastructure modeling with support for over 1000 unique network elements and a wide range of specific cable standards. The following is a partial list of supported cable industry specific standards and infrastructure elements:

Standards

- **High Speed Data**
  - DOCSIS 1.0, 1.1, 2.0
- **Voice over IP**
  - PacketCable
- **Outside Plant**
  - SCTE Hybrid Management Subcommittee

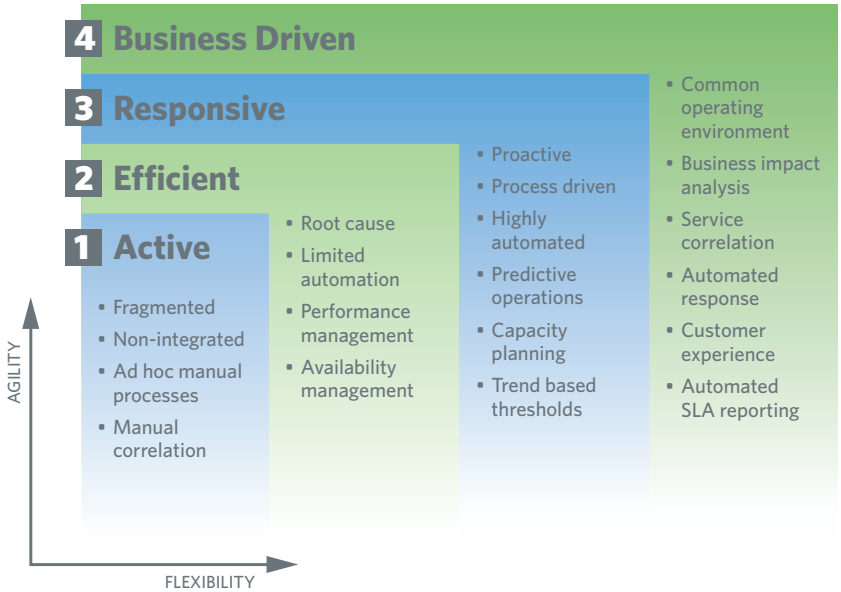


Figure 1. Operational Transformation.

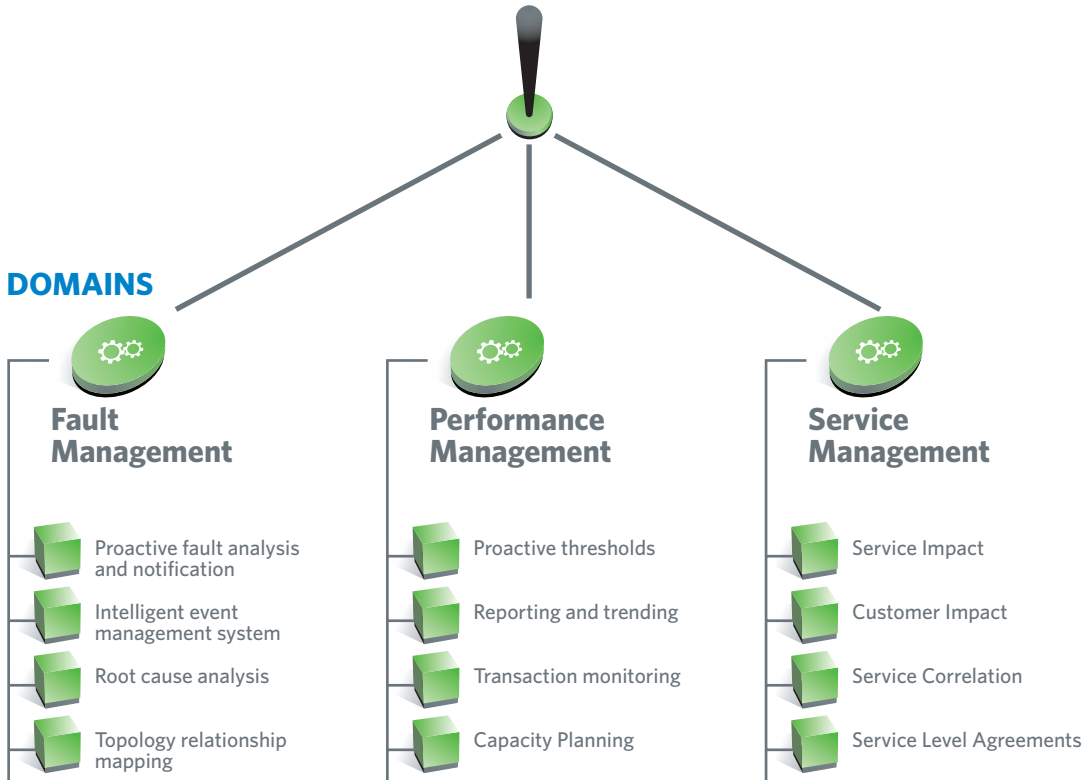


Figure 2. Cross Domain Management.

Infrastructure Elements

- **Backbone Transport**
  - Juniper, Cisco, Nortel, Lucent
- **Return Path Monitoring**
  - Acterna, Trilithic
- **High Speed Data**
  - Arris, Cisco, Motorola, ADC, any DOCSIS compliant CMTS or CM
- **Voice over IP**
  - Cisco, Nuera, Nortel, Siemens, Oasys, CedarPoint, Tollbridge
- **Video on Demand**
  - SeaChange, Concurrent
- **Plant Monitoring**
  - Tollgrade, AM Communications
- **HMS Compliant Power Supply Monitoring**
  - Electroline, AM Communications, Tollgrade

In addition, technologies such as Wi-Fi, 3G, and optical transport technologies are also supported within these products. With SPECTRUM and *e*Health, CA provides a unified view across the infrastructure that allows an MSO to eliminate a number of the point tools and proprietary systems in favor of an integrated solution that leverages embedded management intelligence. With these solutions, MSOs can improve service and reduce costs through rapid problem resolution, proactive service assurance, predictive capacity planning, and effective service level management.

At the core of the service assurance solution is a concept called Business Service Intelligence (BSI) – a methodology for understanding the relationships and impact of the infrastructure on business services. BSI delivers Technology Relationship Mapping, Impact Analysis and Root Cause Analysis that enables MSOs to evolve their network operations from being tactically reactive to strategically proactive, while improving service quality from a customer and business perspective. The solution is based on a broad, mature product offering that can be broken into three functional domains: **Fault Management, Performance Management, and Service Management (Figure 2).**

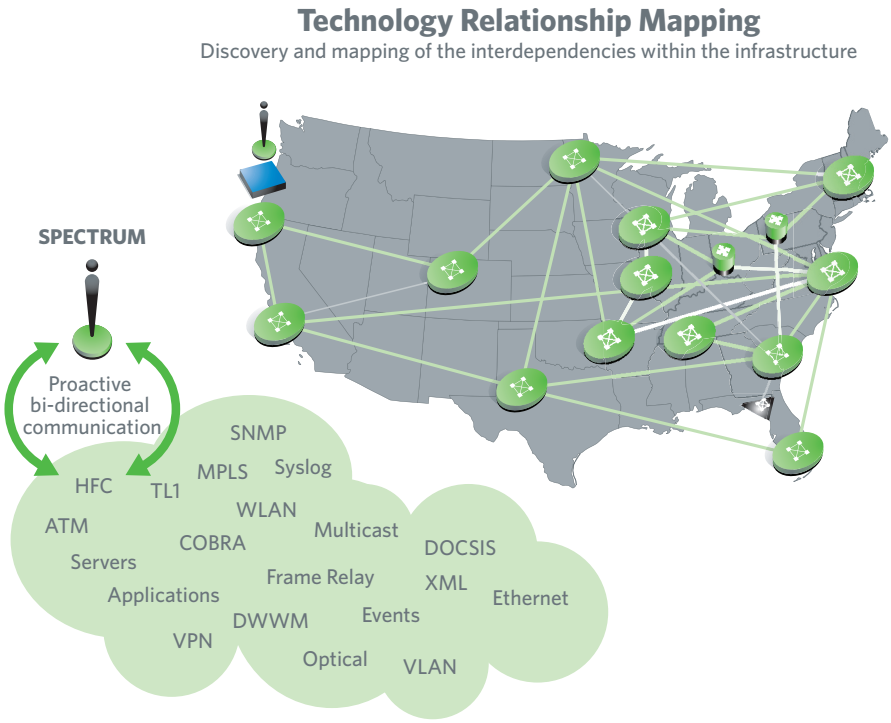


Figure 3. SPECTRUM Technology Relationship Mapping.

Fault Management

SPECTRUM allows operations staff to isolate outages and degradations and identify root causes behind them. SPECTRUM provides proactive monitoring by directly interacting with the managed elements to gather health and availability metrics. SPECTRUM also provides the ability to passively monitor elements through the receipt of SNMP traps or events from the elements directly or via other monitoring applications. These polled or received events provide critical information that SPECTRUM leverages to determine the root cause and the impact of an outage.

One of the key components of SPECTRUM's fault management capabilities is the ability to map the relationships between infrastructure elements (Figure 3). SPECTRUM provides an industry leading discovery capability that allows the system to automatically discover the infrastructure element and their interdependencies.

SPECTRUM uses the model of the infrastructure to determine the root cause and impact of faults and/or degradations. SPECTRUM's modeling engine detects and responds appropriately to outages in the environment by generating a root cause alarm and suppressing the symptomatic conditions associated with an outage. In the above example an element has failed within the infrastructure, as a result several of its neighbors are impacted. Without SPECTRUM's modeling capability a NOC operator may be flooded with outages. With SPECTRUM, that operator gets a single alarm for the device outage with the symptomatic alarms suppressed. This capability helps the NOC improve service and reduce costs by allowing operations teams to immediately identify and troubleshoot the root cause of an outage.

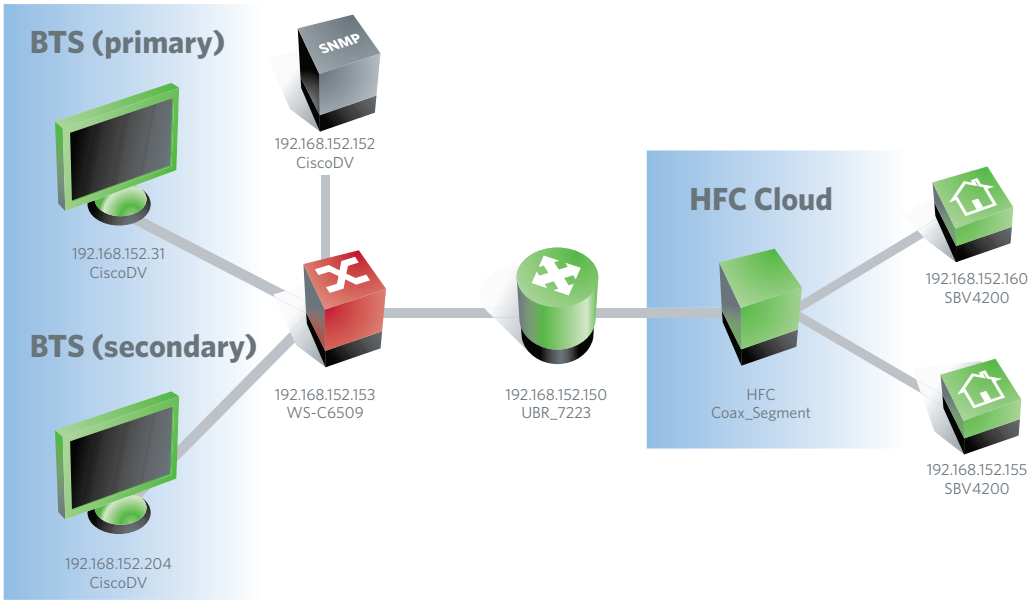


Figure 4. SPECTRUM Topology View.

In addition to SPECTRUM's out of the box modeling intelligence, customers can add their own experience to the system through pre-built flexible event policies (Figure 5). SPECTRUM includes a number of these policies like event rate, pairs, coincidence and condition. In the above example, an event rate policy is used to identify an alarming condition on the router. In this environment it is within normal operating parameters for a router to receive four client connections detected and rejected per minute, so based on the customers policy no alarm will be generated. However if that rate were to increase to twenty events per minute then SPECTRUM will generate an alarm on the router. Operations teams can improve their efficiency by tuning the system to decrease the number events or alarms that the group needs to evaluate.

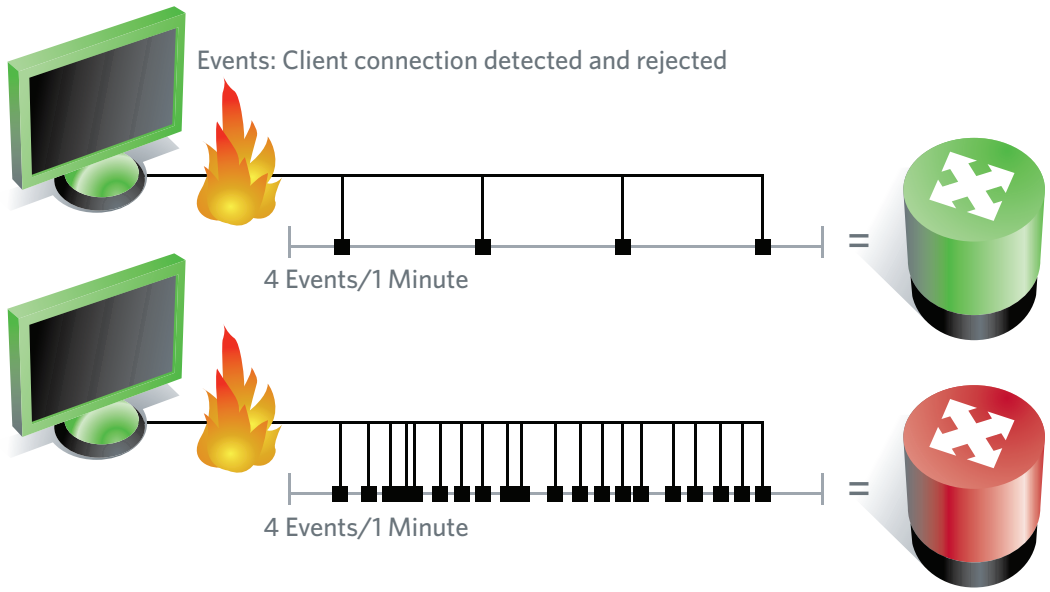


Figure 5. SPECTRUM Event Management.

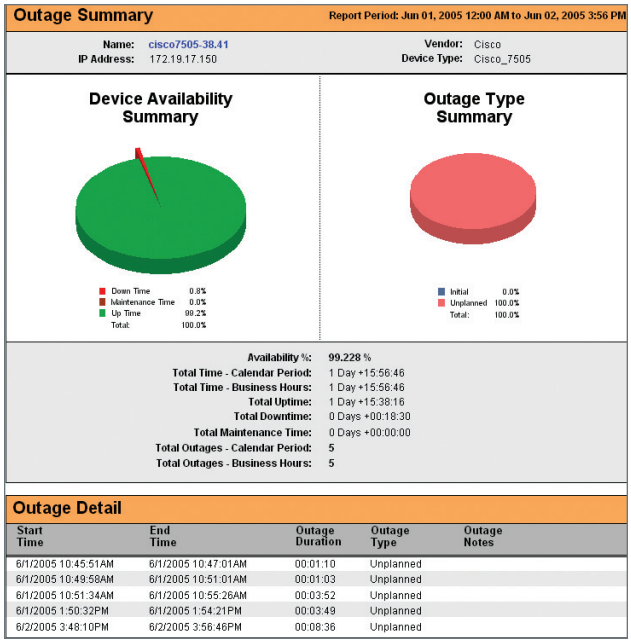


Figure 6. Availability Report.

In addition to outage reports, SPECTRUM can also provide comprehensive availability reports (Figure 6) for all monitored assets. These availability reports provide all of the details regarding any down or degraded time. The report below demonstrates an overview of the devices availability including uptime, downtime and maintenance time on the right and on the left is a break down of the outage time. In addition the user can "drill into" the outage details and see each outage event including the root cause and duration.

Performance Management

Performance management is comprised of two main components, response time monitoring and element performance. Each component plays a critical role in understanding the performance of the infrastructure and its impact on the services being delivered. Response time monitoring involves measuring and reporting on the performance from the end users perspective, and across the network infrastructure. Element performance involves measuring the performance of the network and server infrastructure components to determine current health and to predict future health. Each of these components plays a crucial role in determining the health and availability of services. For performance management, CA augments SPECTRUM's asset management capabilities with eHealth's historical and predictive performance reporting and capacity planning.

Performance Management starts with understanding the infrastructure from an asset inventory standpoint (Figure 7). SPECTRUM's Technology Relationship Mapping capability feeds the asset reports to ensure timeliness and accuracy of the asset inventory. This inventory information is used by eHealth for periodic polling (every 5 or 15 minutes) of critical performance management data from the monitored infrastructure. Advanced performance management algorithms and reporting mechanisms are applied to polled data in the eHealth database to produce a wide range of reports, for audiences ranging from technical operations and engineering staff to line of business owners.

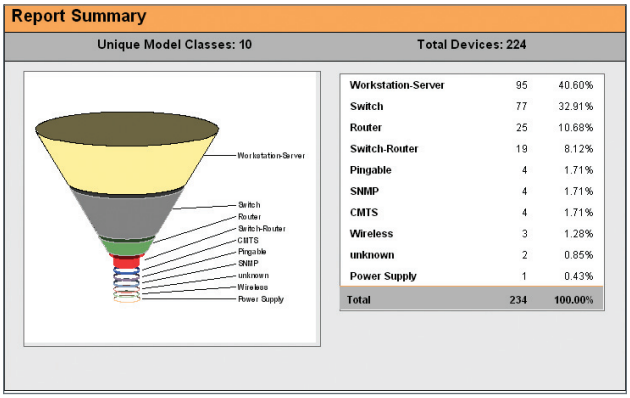


Figure 7. Network Asset Report.

eHealth provides comprehensive performance analysis capabilities to base line performance and provide proactive notification through SPECTRUM when key performance indicators are outside of expected values. This flexible solution can also report on other performance indicators like errors, discards, retries, etc. The screenshot below is an example of a report dashboard that provides the Modem details (Total, Active, Registered) per upstream interface as well as the CPU utilization for a given CMTS (Figure 8).

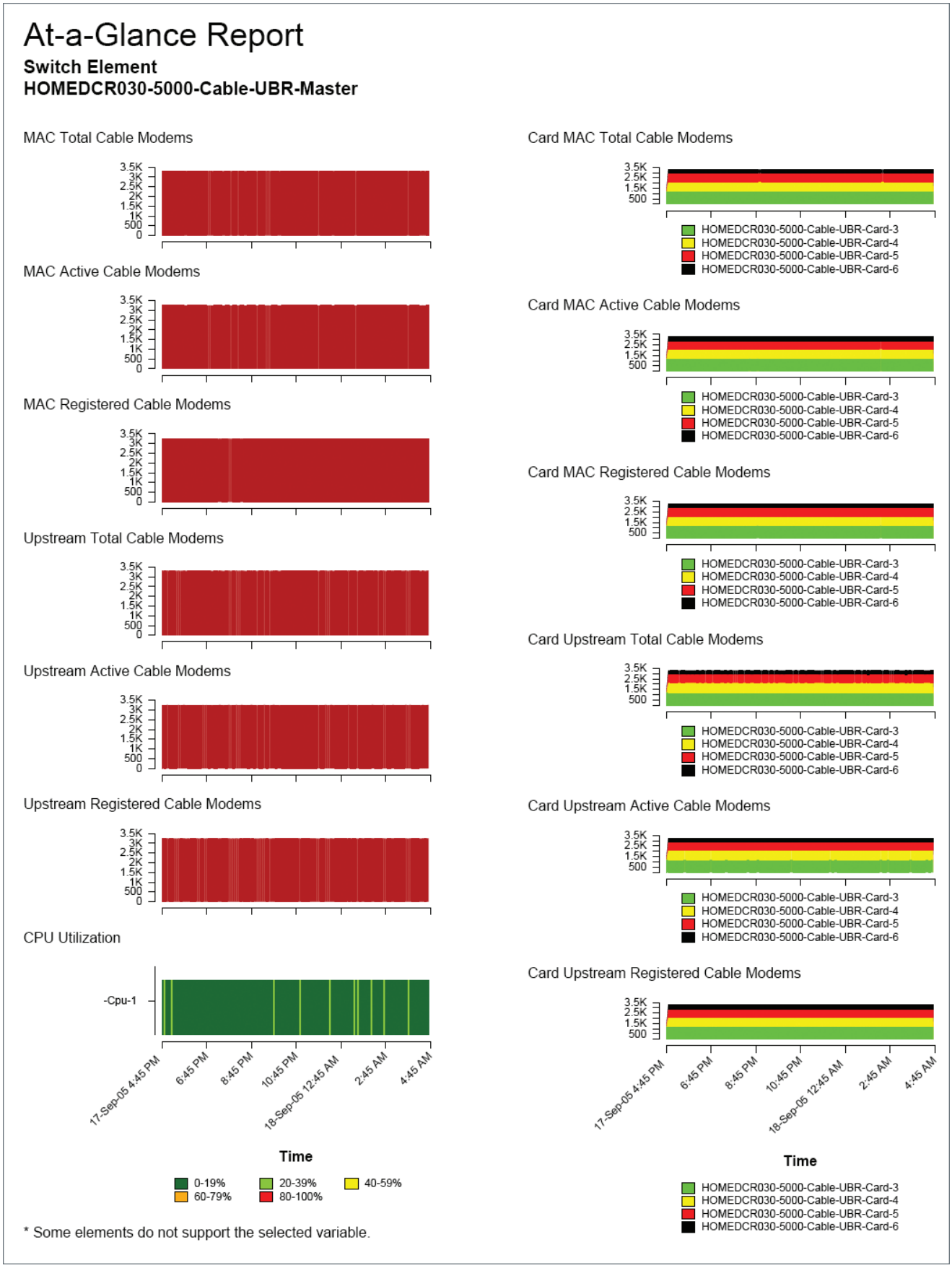
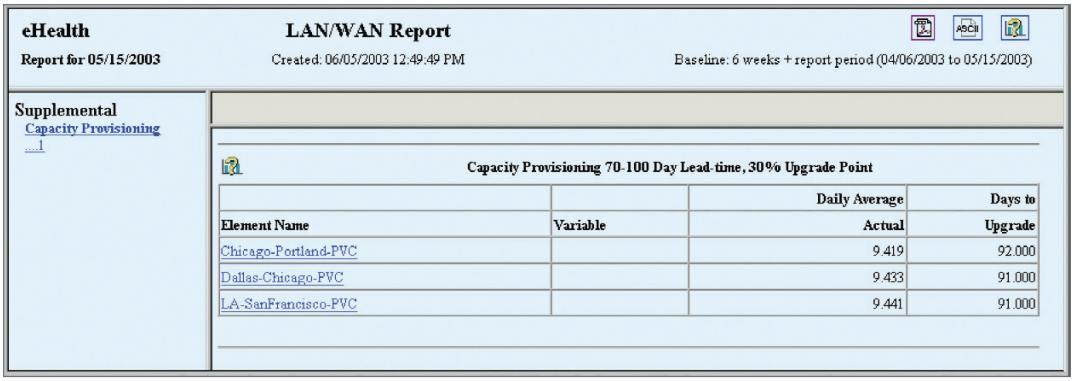


Figure 8. eHealth Performance Report.



eHealth

LAN/WAN Report

Report for 05/15/2003

Created: 06/05/2003 12:49:49 PM

Baseline: 6 weeks + report period (04/06/2003 to 05/15/2003)

Supplemental

Capacity Provisioning

....1

Capacity Provisioning 70-100 Day Lead-time, 30% Upgrade Point

Element Name	Variable	Daily Average Actual	Days to Upgrade
Chicago-Portland-PVC		9.419	92.000
Dallas-Chicago-PVC		9.433	91.000
LA-SanFrancisco-PVC		9.441	91.000

Figure 9. eHealth Capacity Planning Report.

The rapid introduction of new services into the market provides MSOs with a significant capacity management challenge. They need to ensure adequate capacity exists to capture the revenue from market demand for new service, but they also need to control capital expenditures by timing purchases to when they are really needed. eHealth's application of advanced algorithms to historical utilization and performance data allows MSOs to closely match bandwidth to subscriber demand. In the "Provisioning Lead-Time" report below (Figure 9), capacity planners select two parameters to make this type of informed decision. First, they choose provisioning lead-time — the time delay between when they order additional bandwidth from their provider and when it is available for use. Then, they select the upgrade point, or the pre-defined threshold for when they need additional capacity to be available. The report then provides a listing of all of the locations in the network for which additional capacity needs to be ordered today in order to avoid violating the upgrade point during the ensuing provisioning lead time.

CA's unified approach to service assurance provides a single vendor solution for monitoring both the network infrastructure and the services that are delivered over that network. For example, a leading VOD vendor sends an SNMP trap every 30 minutes that includes critical statistical information regarding the health of the VOD service for a particular Market. The solution receives the trap, extracts the statistical information and updates a web based report that shows the current number of active streams, streams in error, OK streams and the total number of streams. This provides an easy use, self maintaining VOD market report that key stakeholders within the MSO can leverage (Figure 10).

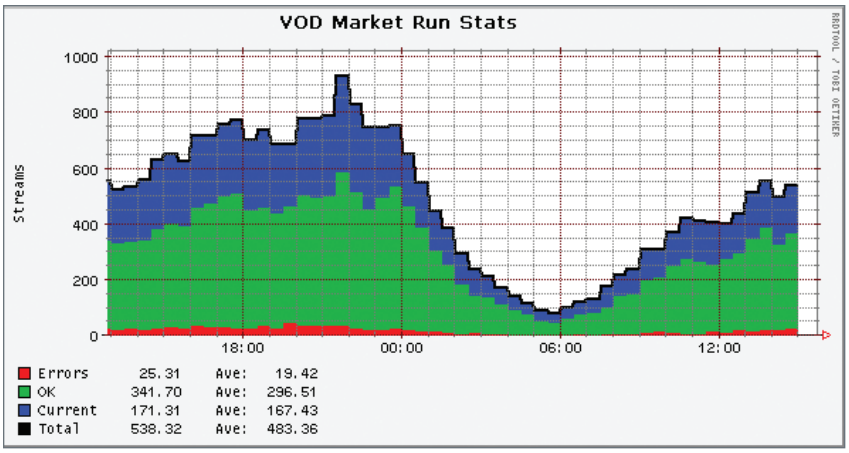


Figure 10. VOD Report.

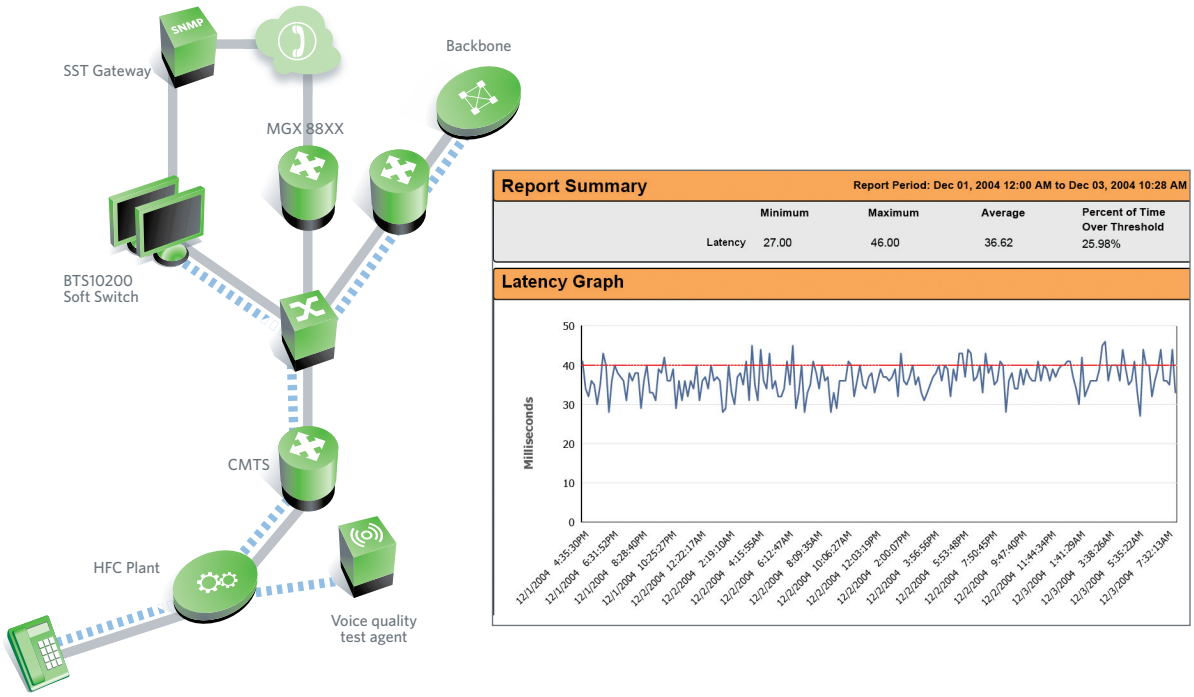


Figure 11. Service Performance Management.

SPECTRUM is also able to take this information and generate an alarm if the percentage of VOD streams in error violates a defined threshold allowing the Operations group to proactively address the issue.

Another important aspect of performance management is response time monitoring. This involves leveraging response time testing capabilities built into leading hardware vendor's firmware that allows a management system to configure, threshold and report on synthetic transactions across the infrastructure. CA solutions import response time data directly from these devices for both fault and performance management, and can also accept events from 3rd party test agents from vendors such as Brix Networks®, Tollgrade®, Acterna® and others for voice quality testing. Data from these systems are then applied to the appropriate infrastructure elements within SPECTRUM and eHealth for analysis and correlation (Figure 11).

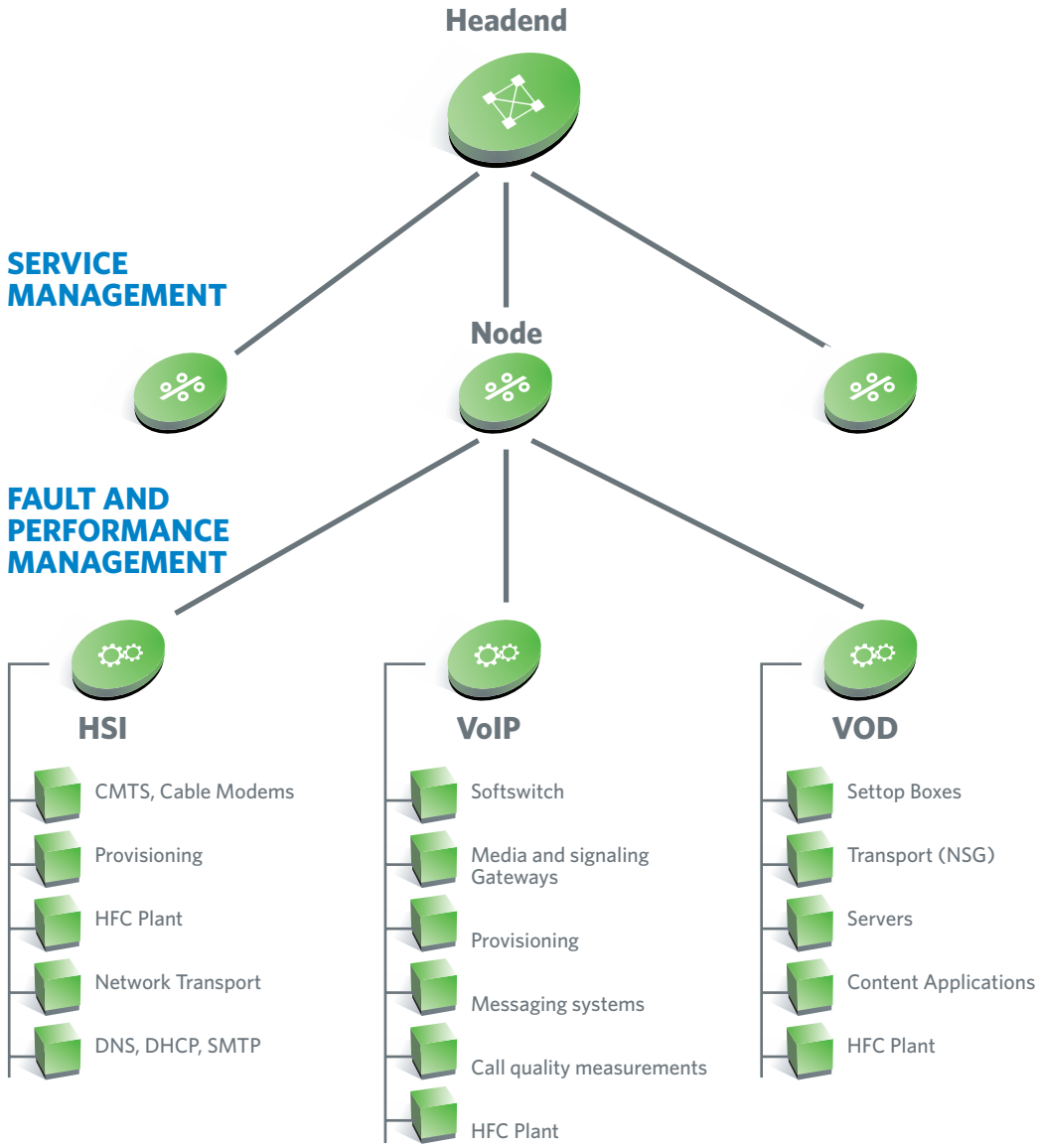


Figure 12. SPECTRUM Service Modeling.

Service Management

SPECTRUM and eHealth extend from infrastructure fault and performance management by providing a comprehensive view into the health and availability of critical services delivered over that infrastructure. Today's MSOs take a customer centric approach to operations management, so the assurance tools on which they rely need to provide a service view in addition to an infrastructure view. SPECTRUM's correlation engine has been extended to allow an MSO to define services on a per node or service area. These nodes or service areas can then be collected into regional or market views that culminate into a national service view if desired (Figure 12). Service views are accessed via the SPECTRUM OneClick Service Dashboard which provides an at a glance view into the health and availability of services at each level of the service hierarchy. The solution also leverages an innovative condition based correlation engine that evaluates events from disparate sources across management domains to identify the root cause of an outage and identify the services impacted.

The health and availability of services are driven by SPECTRUM's fault and eHealth's performance monitoring data. SPECTRUM is able to interpret the events occurring within a Node or Service Area across the different service domains and determine the underlying root cause of the outage or degradation.

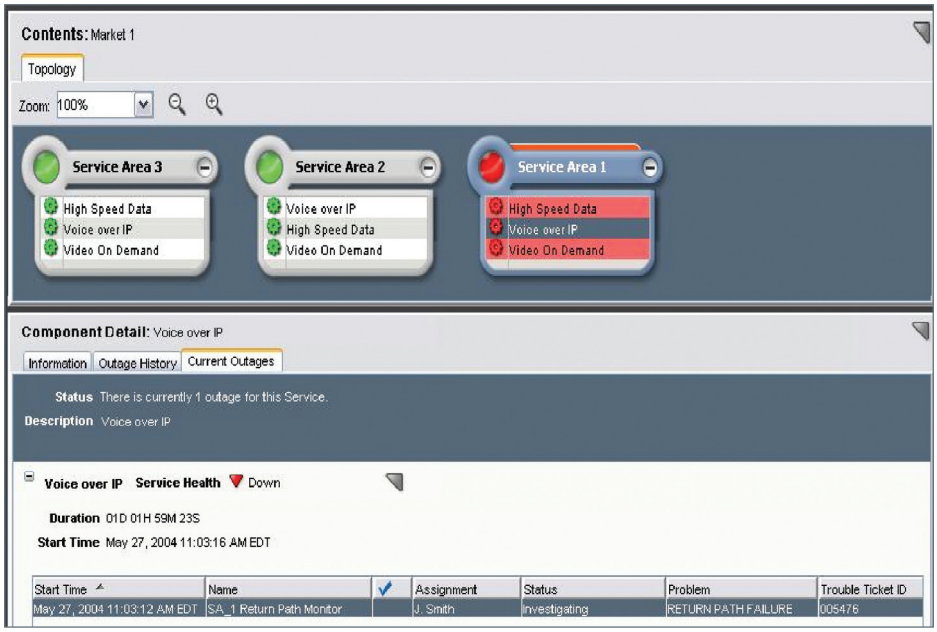


Figure 13. Service Dashboard.

As an example, SPECTRUM may process the following events:

- VOD server (high tune errors service are S1567)
- Harmonic NSG (Weak signal... RF output errors QAM...)
- Return Path Failure (Node ID 135...)
- CMTS event - High % of cable modems go offline (interface 2.1 feeds node sa135, sa136, sa137)

These events evaluated individually appear to indicate a failure within the infrastructure; however by being aware of these events as a whole, SPECTRUM is able to determine the root cause of the outages as well as the services impacted by the outage. In the above example, SPECTRUM identifies a Return Path failure as the root cause of this outage and tags the other events as symptomatic of the root cause event (Figure 13).

From the Network Operations (Figure 14) perspective, one would see a single alarm within the OneClick alarm view and in the details view see the services impacted by the outage as well as the symptoms identified by SPECTRUM. From the Service Desk analyst user or managers perspective, the Service Dashboard would indicate that a service is down and its impact to the business. They can alert customer support of the outage so they are prepared to handle customer calls. The analyst assigned to the problem can drill into the current outage to see the root cause and take the immediate corrective steps to restore the service.

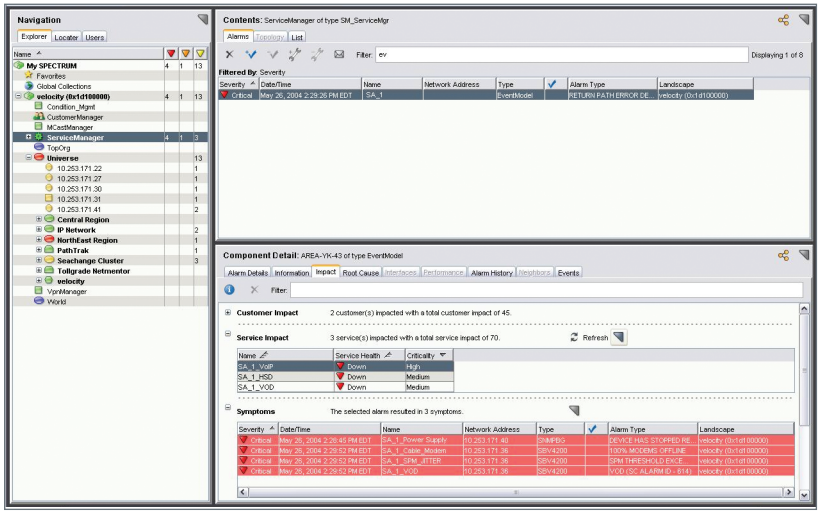


Figure 14. SPECTRUM OneClick Console.

Figure 15. CA Security Management Solutions.

Security Management

As today's MSOs allow their customers automated access to web-based content for self-service billing, customer-care, and service ordering, security management is added to the list of critical infrastructure management requirements. Through its *e*Trust® line of products, CA provides a broad range of solutions for Identity and Access Management, Integrated Threat Management, and Security Information Management (Figure 15). These solutions are built on the same principles as its service assurance solutions — multi-vendor, integrated, and highly scalable — once again providing the benefit of a single vendor solution to multiple management needs.

Managing users and their access is no longer a simple task in today's complex business environment. Users' roles have expanded beyond the traditional enterprise users customers, suppliers and partners are now an integral part of an organization. Business partners require a trusted relationship to execute business transactions. Public-facing websites and business processes exposed via Web services must be protected from unauthorized access. The complexity of identity management is further increased because it must have the capability and capacity to manage identities and security in different types of legacy and distributed systems and applications, including HR, ERP and supply chain management systems.

*e*Trust Identity and Access Management Suite provides a secure, open identity management platform. All of its components are seamlessly integrated to maximize efficiency and provide a foundation for additional integrations, greatly reducing deployment and enabling a quick return on investment. *e*Trust Identity and Access Management Suite leverages a high-performing X.500 directory as its embedded repository. This LDAP V3-compliant solution enables you to take advantage of directories, such as Microsoft's Active Directory or Sun Java System Directory Server.

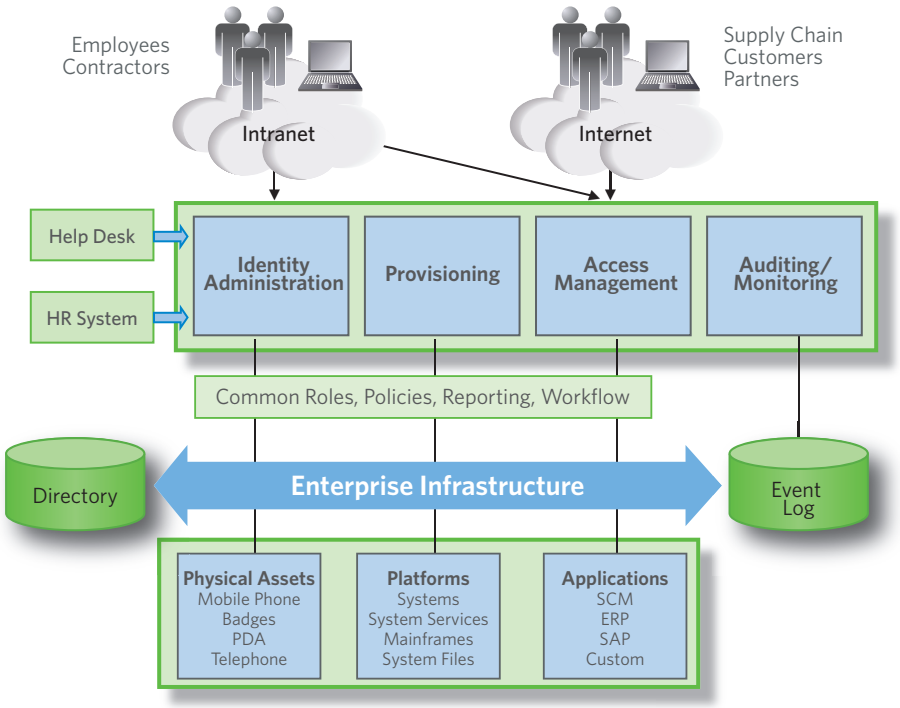


Figure 16. CA Identity and Access Management Suite.

*e*Trust Identity and Access Management Suite provides comprehensive visualization and management of virtually all aspects of identity across the enterprise and federated worlds (Figure 16).

*e*Trust provides identity and access management services to organizations that need to improve overall information security, enhance regulatory compliance, reduce costs and increase user satisfaction with their web-delivered applications. In addition to the security enforcement capabilities, *e*Trust delivers administrative services that automate the management of a user's identity lifecycle within the organization, from creation to modification, to eventual deletion.

Conclusion

The CA MSO solutions are helping many of the top tier MSOs deliver a higher level of service at lower costs to their customers through proactive service assurance, rapid problem resolution, predictive capacity planning, and effective service and security management. As MSOs race to deliver new bundled services ahead of their competition, the CA solutions have become an enabling technology by offering greater insight into the capabilities of the infrastructure to support new service offerings. The result is successful launch of new services that are managed and supported from day one.

The CA solution continues to expand in meeting the needs of customers around the world. Recent enhancements like Multicast Management and Quality of Service Management, critical technology participants in defining and delivering a service, extend the solutions view of the infrastructure to support Digital Simulcast deployments. Enhancements like these come as a direct result of the relationships and interactions with our customers that help drive the roadmap for new features and / or enhancements. As a result, the solution continues to evolve and deliver increased value to customers by supporting new technologies that yield revenue generating services.

CA's integrated service assurance solutions provide the tools necessary to identify service degradations and outages, yielding root cause information that provide operations the actionable information required to quickly restore services. Its security solutions provide the means by which operators can control user and customer access to services, centrally manage threats, and take a holistic approach to security information management.

To learn more about how CA MSO Solution can help you manage what matters, please call toll-free in the U.S. at (877) 437-0291 or worldwide at +1 603-334-2100.

About the Author

Jim Lochran has 10 years experience defining and developing service assurance solutions for the telecommunications industry inclusive of Wireline, Wireless and Cable providers. Jim's background is in development and solution architecture within Aprisma Management Technologies flagship product SPECTRUM. In this role, Jim lead several development projects focused on extending SPECTRUM's scalability, technology support and root cause analysis capability to address the needs of the service provider community. Currently, Jim is leading a team of solution architects within the CA Communications, Media & Entertainment business unit, focused on helping CA's Communication, Media and Entertainment customers achieve their goals by providing solutions that unify, simplify and secure the service delivery infrastructure.

MP303530606