

EMC Smarts MPLS Manager

Innovative Technology for MPLS/VPN Management

Abstract: Increasingly, both service providers and enterprises are turning to Multi-Protocol Label Switching (MPLS) to combine the features, reliability, and predictability of traditional carrier networks with the flexibility, scalability, and cost-effectiveness of IP-based service delivery. This paper discusses the unique management challenges posed by MPLS IP Virtual Private Networks (VPNs), and how the EMC[®] Smarts[®] architecture is uniquely suited to address these challenges.

December, 2005

Copyright © 2005 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, ApplicationXtender, Celerra, ContraStar, CLARAlert, CLARiiON, Connectrix, Dantz, Direct Matrix Architecture, DiskXtender, Documentum, EmailXtender, EmailXtract, HighRoad, Legato, Navisphere, PowerPath, RepliStor, ResourcePak, Retrospect, Smarts, SnapView/IP, SRDF, Symmetrix, TimeFinder, VisualSAN, and where information lives are registered trademarks and EMC ControlCenter, EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, EMC Storage Administrator, Access Logix, ArchiveXtender, Automated Resource Manager, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, Centera, CLARevent, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, DiskXtender 2000, EDM, E-Lab, EmailXaminer, Engenuity, eRoom, FarPoint, FLARE, FullTime, InfoMover, MirrorView, NetWin, NetWorker, OnAlert, OpenScale, Powerlink, RepliCare, SafeLine, SAN Advisor, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, and VisualSRM are trademarks of EMC Corporation.

All other brand names are trademarks or registered trademarks of their respective owners.

S0055

Table of Contents

- Introduction4**
- Fundamentals5**
 - IP VPN over MPLS 5
 - MPLS IP VPN Management Challenges 6
- The EMC Smarts MPLS Solution.....7**
 - A Common Philosophy 7
 - EMC Smarts MPLS VPN Management 7
 - EMC Smarts Service Assurance Manager..... 8*
 - EMC Smarts MPLS Manager..... 9*
 - The EMC Smarts Transport Domain Manager 10*
- Conclusions.....11**

Introduction

Multi-Protocol Label Switching (MPLS) has been called “the wave of the future” for backbone networks. The reason is clear: MPLS brings to IP the features, reliability, and predictability of traditional carrier networks while preserving the dynamic characteristics, flexibility, and cost-effectiveness that have made IP the world’s dominant network protocol. Despite this promising future, traditional network management tools have not been designed to handle the unique characteristics of MPLS networks—creating challenges for forward-thinking network managers seeking to operationalize MPLS in their core network infrastructures.

Network operators are choosing MPLS because, among other benefits, MPLS dramatically simplifies deployment, management, scalability, and flexibility of Virtual Private Networks (VPNs). MPLS VPNs offer the security to conduct private communications over a public infrastructure, the scalability to support hundreds of thousands of users, and the flexibility to accommodate any-to-any traffic patterns. For a number of carriers, MPLS also provides an effective platform for voice-over-IP (VoIP) and a variety of other quality of service (QoS)-based offerings.

MPLS technology achieves its versatility by separating the packet-forwarding component from the routing control component. The packet-forwarding component switches at wire speeds using short, fixed-length packet labels. The control component implements sophisticated traffic engineering policies to deliver predictable and reliable performance over different classes of service and to support the most rigorous transport and bandwidth requirements.

With MPLS, service providers and their customers can leverage existing IP, ATM, and frame relay infrastructures to achieve exceptional business benefits—deploying and maintaining MPLS VPNs faster and more cost-effectively than connection-heavy ATM and frame relay infrastructures, reducing reliance on costly skilled professional resources, and quickly supporting the latest high-bandwidth, revenue-generating services.

As enterprises work to extend mission-critical, intranet-based applications to their customers, suppliers, and partners, service providers are offering competitive, cost-effective MPLS-based network solutions to address these needs. MPLS VPNs enable enterprises to consolidate voice, data, and video into one network, conduct e-commerce, and share content with their customers and partners on a secure, flexible, high-speed, scalable, private network over an IP backbone.

For all these reasons, both service provider and enterprise organizations are eagerly looking for new MPLS solutions and the tools to manage these networks effectively. EMC Smarts has responded to this need with an MPLS management solution that has proven its superior performance in the marketplace.

MPLS IP VPN Management Challenges

Managing an MPLS IP VPN requires a sophisticated service-assurance platform that can manage each of the following three domains individually, and in correlation with one another:

- The transport domain, including the traditional Layer 1, Layer 2, and Layer 3 elements that comprise the infrastructure of the network.
- The MPLS domain, including the logical connections (LSPs) that are layered over the transport domain, their related policies, and the control entities associated with them.
- The VPN and business domain layered over MPLS, including VPN membership and VPN topology, be it a full mesh, hub-and-spoke, or any other complex topology.

Specifically, an MPLS IP VPN management platform must be able to perform the following functions:

- **Scale to the largest, most complex implementations.** IP VPNs over MPLS can support hundreds of PE and thousands of CE routers underlying complex VPN topologies and layered over globally spanned transport networks. An MPLS management system must be able to scale with the technology.
- **Discover the logical and physical entities and relationships in the related technology domains.** An MPLS VPN management system must discover the entities and relationships in the transport, MPLS, and VPN domains, and then intelligently infer the relationships between elements across domains. For example, it must be able to discover Layer 2 and Layer 3 VPNs, and determine which LSPs provide connectivity between which specific VPN subscribers.
- **Represent the complex topologies across transport, MPLS, VPN, and business domains.** These relationships form complex topologies across domains that cannot be represented by the hierarchical topologies of most management systems. This representation is essential for accurate analysis.
- **Present accurate topology maps.** An effective management system must provide managers with easy-to-navigate views of the entities and relationships supporting the VPN at all layers and across layers. These views should include VPN customers and their relationships to VPN services.
- **Integrate and correlate events across domains.** The management system should be able to integrate event and topology information from multiple sources across transport, MPLS, and VPN domains.
- **Correlate VPN connection health with the health of the underlying infrastructure.** Since the performance of VPNs depends on the health of the underlying infrastructure, a management solution must be able to correlate the end-to-end health of connections between VPN subscribers and the underlying infrastructure.
- **Perform root-cause analysis across technology domains.** Service-affecting problems originating in any domain can cause floods of symptoms throughout the network. An effective management system must be able to pinpoint the problems that must be fixed in order to sustain service. This includes, for example, identifying congestion in a particular device as the root cause of an LSP fault or of tardiness in the VPN service.
- **Perform impact analysis across technology and business domains.** Access and core faults and performance problems can impact LSPs, affecting VPNs and their subscribers. True service impact is determined only by correlating the end-to-end VPN measurements with faults identified in the core and access layers.
- **Correlate fault recovery mechanisms.** An effective management system must be able to correlate MPLS recovery mechanisms, such as backup LSPs kicking in or MPLS fast re-route events, with other symptoms to accurately diagnose the underlying physical faults that triggered them. This is essential, because recovery mechanisms can mask faults that must be addressed to maintain resilience. Furthermore, understanding the workings of these mechanisms is critical to reaching the right diagnostic conclusion.
- **Handle duplicate IP addresses correctly.** Monitoring VPNs from the user perspective is further complicated by the existence of duplicate private IP addresses provisioned over the same global infrastructure.
- **Support policy-driven management.** Because of the large scale of VPN infrastructures, a management system must allow network operators to selectively monitor and manage various elements of the system. For example, a network operator may be interested only in the LSP ingress and egress points, ignoring the individual hops taken by the LSPs.
- **Support multi-vendor architectures.** Today's complex MPLS networks include complex virtual router configurations from multiple vendors. Management systems must be able to support these environments.

The EMC Smarts MPLS Solution

A Common Philosophy

MPLS is a generic switching protocol that can implement any type of network service. This capability is achieved by decoupling the fast, realtime packet-forwarding mechanism from the policies (the routing and network protocols) that construct the forwarding tables. New services and protocols can be introduced without replacing the underlying switching mechanism.

The EMC Smarts Codebook Correlation Technology™ (CCT) approach to correlation is analogous: CCT decouples the realtime correlation engine (the Codebook correlator) from the policies (the object-oriented correlation models and topology) that are used to construct the Codebook. The models and topologies may change to reflect new services, but the underlying correlation engine remains the same.

The unmatched scalability of the Smarts architecture makes it the perfect contender for MPLS IP VPN management. As new services are introduced in the MPLS core, CCT adapts automatically to manage any type of service and any type of topology.

EMC Smarts MPLS VPN Management

Given the different domains participating in an MPLS VPN, an effective way to manage such networks is to partition the management along the same domains, and manage each domain both individually and in correlation with the other domains. The Smarts solution for MPLS IP VPNs is organized as an integration of three domain-specific solutions for:

- The transport domain, including Layers 1, 2, and 3.
- The MPLS domain, including LSPs and their related policies.
- The VPN and business domain, including VPN membership and topology.

Smarts integrates and correlates information across these domains by leveraging the EMC Smarts ICIM Common Information Model™. Each domain is responsible for a portion of the model, and domains overlap at specific points. The points of overlap are conduits for causal propagation of information across domains. Figure 2 depicts these domains and their intersection points. The use of a common information model across these solutions allows the management information to be seamlessly integrated and cross-correlated by EMC Smarts Service Assurance Manager.

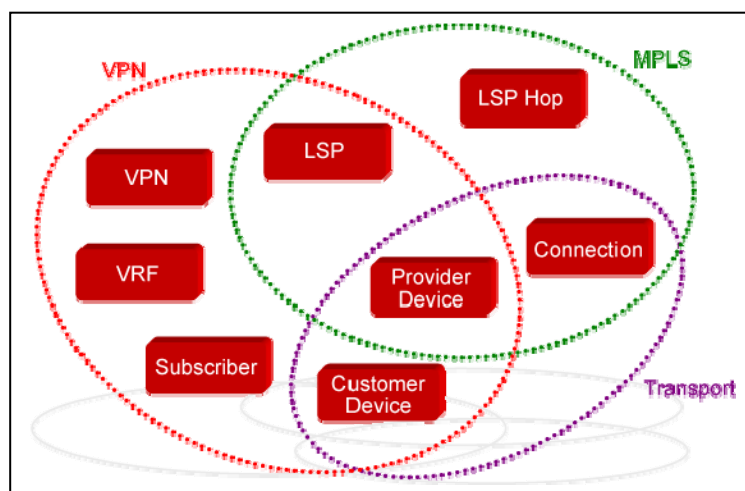


Figure 2: Model Intersection Points

To follow MPLS VPN scalability, the Smarts solution uses a separate domain manager to manage each of the underlying domains (EMC Smarts IP Availability Manager and Performance Manager manage the transport domain), and an EMC Smarts Service Assurance Manager to integrate and correlate across all underlying domains (Figure 3). Further scalability is achieved by partitioning any or all of the underlying domains into separate domain managers. For example, one may use a single domain manager for the VPN domain and a single domain manager for the MPLS domain, while partitioning the transport network into a provider core domain and multiple customer edge domains.

Smarts' recursive distributed architecture naturally supports this type of partitioning, while preserving the ability of individual domain managers to communicate with one another. Furthermore, the Smarts architecture supports seamless rollup of multiple independent domain managers into an integrated and correlated higher-level view of the overall managed environment. This rollup is supported through any number of tiers, making scalability truly unlimited. A high-level domain has automatic access to all the details of its subtending domains. In addition, operators can view the more detailed information via point-and-click drill-down.

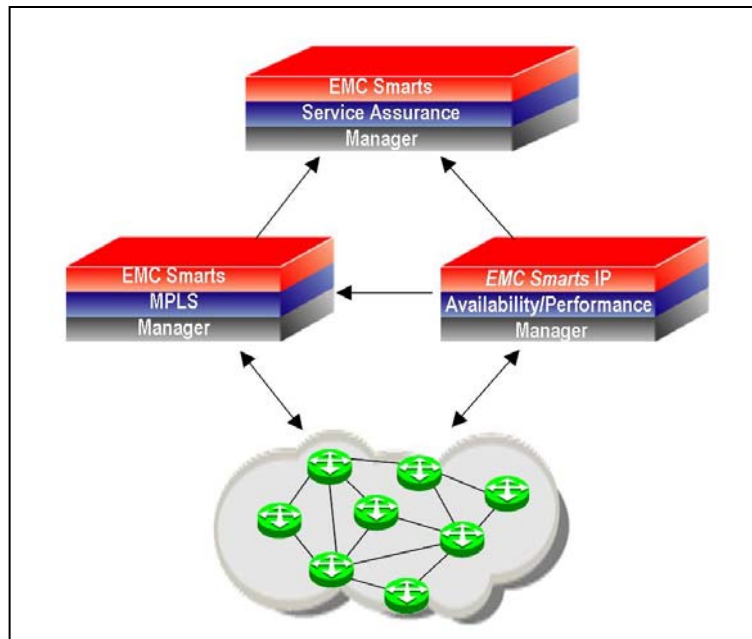


Figure 3: EMC Smarts MPLS Manager Architecture

EMC Smarts Service Assurance Manager

Service Assurance Manager gives the system operator a seamless, integrated and correlated, high-level view of the overall entities and relationships in underlying domains (Figure 4). It also represents VPN service offerings and subscribers and their relationships to infrastructure entities. While Service Assurance Manager maintains a high-level global view, detailed information about the entities and relationships is maintained in the subtending domain managers. In addition to the infrastructure entities of the subtending domain managers, Service Assurance Manager represents relationships between VPN service offerings and subscribers and between VPN service offerings and infrastructure entities. This information is used to accurately identify the detailed business impact analysis of problem notifications received from managers of the underlying domains. Note that competitor topologies that are limited to hierarchical representations with containers are insufficient to represent relationships accurately. As a result, their impact notifications contain an unacceptable amount of false positives.

As an adjunct to Service Assurance Manager, the Cisco ISC Adapter automatically associates VPNs with customer names (as opposed to just IP addresses), and reconciles topology with provisioning data provided by Cisco IP Solution Center (ISC) element-management applications.

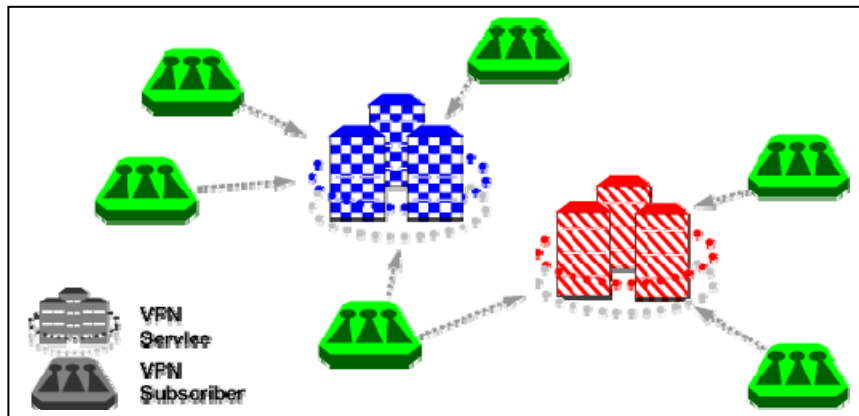


Figure 4: EMC Smarts Service Assurance Manager View

EMC Smarts MPLS Manager

EMC Smarts MPLS Manager manages elements of the PE (provider edge) and CE (customer edge) routers that are related to the VPN offering. It holds a detailed view of the VPN membership and VPN topology, including peering relationships between PE routers, VPN membership subscription of CE routers, control protocols between PEs and their attached CEs, and complex virtual router configurations.

Figure 5 depicts an example of two VPNs and their underlying entities, including CE routers, PE routers, VPN Routing and Forwarding (VRF) tables, and BGP peering between PE routers, which determine the VPN topology. To simplify the picture, the lines showing the association between the VPN instances and their underlying entities have been omitted. Instead, these relationships have been color-coded: all blue (checkered) entities are members of the blue (checkered) VPN, and all red (striped) entities are members of the red (striped) VPN.

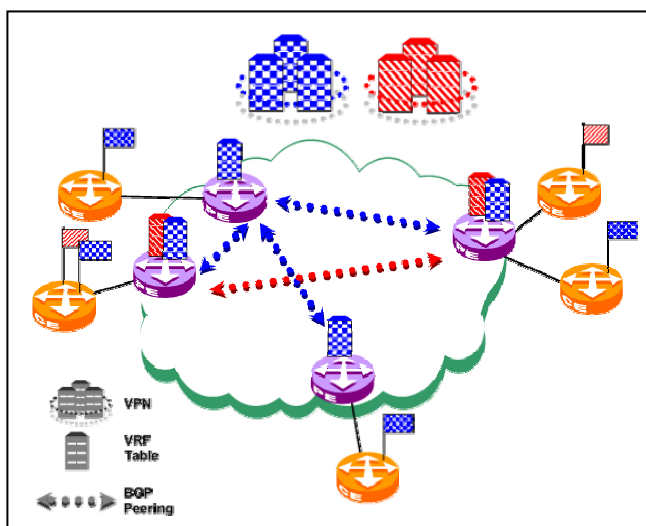


Figure 5: EMC Smarts MPLS Manager View

A specialized VPN Remote Ping—also known as VRF Ping—enables managers to determine if a CE is impacted by an MPLS network failure. VRF Pings can be driven in both a manual or on-demand mode, using a right mouse-click from a device on the map, or they can be scheduled to occur periodically. VRF Pings can be driven from CE to CE router, PE to PE, or PE to CE router. It is configured as a ping of a VRF interface to Router IP Address.

EMC Smarts MPLS Manager also discovers LSPs in the underlying network and their relationships to physical devices and connections in the network. It monitors and correlates realtime fault and performance data from the P and PE routers with routing protocol entities, signaling protocol LSP alarms, and measurements across the MPLS network. End-to-end LSP measurements are correlated with physical and logical alarms in the core by associating each PE-to-PE connection with an underlying LSP, and the LSP with the specific hops along its path (Figure 6).

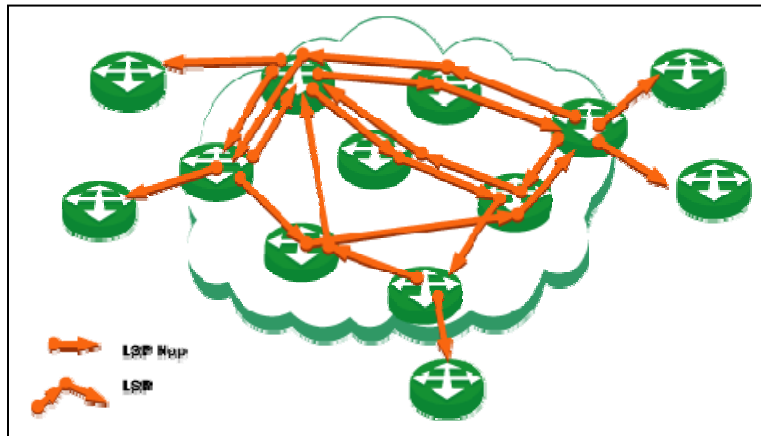


Figure 6: EMC Smarts MPLS View

The EMC Smarts Transport Domain Manager

The EMC Smarts transport domain managers (such as Availability and Performance Managers for IP, ATM/Frame Relay, SONET/SDH/DWDM, etc.) auto-discover Layer 1, Layer 2, and Layer 3 topology, both logical and physical, out-of-the-box. This includes identifying Layer 2 connections between components in the transport infrastructure, including the provider's network and the customer edge. It analyzes root causes of both connectivity and performance faults in the underlying transport domain and their impacts on other entities within the transport domain, as well as on entities in the MPLS and VPN domains (Figure 7).

For Layer 2 VPNs, MPLS Manager discovers Layer 2 devices and circuits, including MPLS pseudowires. It discovers access circuit information for Ethernet, Frame Relay, and ATM, and verifies end-to-end connectivity. It supports cross-domain correlation between MPLS pseudowires and Ethernet VLANs, and provides support for Martini-draft VPNs in Cisco and Juniper environments, and Kompela-draft VPNs on Juniper equipment.

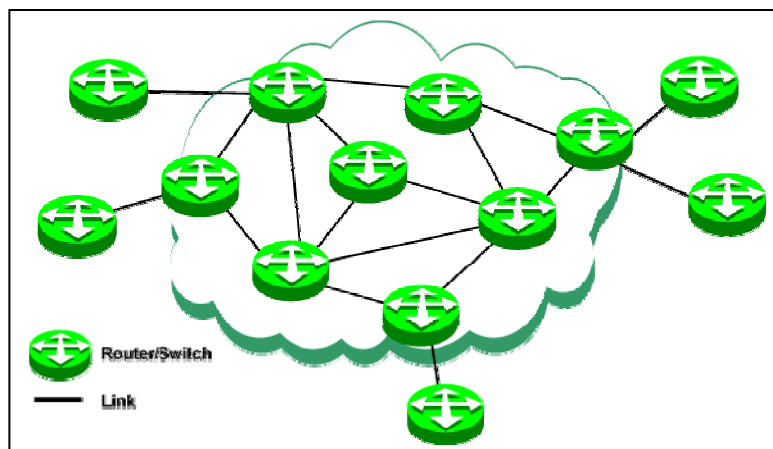


Figure 7: EMC Smarts Transport View

Conclusions

Increasingly, both service providers and enterprises are turning to MPLS to combine the features, reliability, and predictability of traditional carrier networks with the flexibility, scalability, and cost-effectiveness of IP-based service delivery.

Managing MPLS IP VPNs poses unique management challenges. The Smarts architecture is uniquely suitable to addressing these challenges, as demonstrated by the EMC Smarts MPLS Manager solution.

- **Scalability.** Smarts scales to the largest, most complex networks. Smarts' recursive distributed architecture is uniquely capable of scaling to VPNs of unlimited size and complexity by dividing management into cooperating distributed Smarts domain managers.
- **Discovery.** Smarts' discovery engine discovers the rich set of logical and physical entities and relationships in the related technology domains, including LSPs, VRFs, VPNs, BGP sessions, and others. Furthermore, it intelligently infers the associations between entities across domains, yielding a common information model across layers and technologies.
- **Complex topology modeling.** The EMC Smarts Common Information Model and its repository are unique in their ability to model the rich set of entities in technology and business domains, as well as their complex webbed relationships within and across domains, for accurate representation and analysis.
- **Rich topology maps.** The EMC Smarts Global Console and Business Dashboard are unique in mapping the rich set of technology and business entities and relationships within and across technology domains. These powerful display devices support easy navigation across layers and domains, using both object-centric and alarm-centric paradigms.
- **Cross-domain integration and correlation.** The ICIM model and topology enable integration of event and topology information from a variety of sources across the transport, MPLS, and VPN domains.
- **Correlation of VPN connection and infrastructure health.** Smarts leverages end-to-end VPN performance measures, correlating them with the health of the underlying MPLS, IP, and transport infrastructures. ICIM enables this correlation by maintaining relationships between VPN connections and underlying infrastructure entities.
- **Root cause analysis.** Codebook Correlation Technology is the only technology on the market capable of analyzing root cause authentic problems in any domain, including problems originating in the transport, MPLS, and VPN domains, which spread symptoms both within and across domains.
- **Impact analysis.** EMC Smarts Business Impact Manager aligns IT management with business by determining the impact of access and core physical and logical faults on LSPs, and extending this impact to the affected VPNs and subscribers.
- **Correlation of recovery mechanisms.** Codebook Correlation Technology correlates recovery events with fault and performance events to isolate authentic problems that reduce resilience or are masked by recovery mechanisms.
- **Management of duplicate IP addresses.** EMC Smarts' patent-pending approach to managing duplicate IP addresses provisioned over the same global infrastructure enables distinguishing between duplicate IPs in MPLS IP VPNs.
- **Policy-driven management.** EMC Smarts' intuitive graphical administration console supports defining object groups and associated monitoring policies, making it easy to selectively monitor and manage various elements of the system in accordance with the organization's policies and resources.

EMC Smarts leverages patented technologies to deliver a powerful VPN MPLS management solution. Both the ICIM Common Information Model and the Codebook Correlation Engine, architectural features unique to Smarts, are the keys to the unprecedented level of automation provided by this solution. The solution also leverages Smarts' distributed scalable architecture, treating each of the intersecting managed domains separately and cross-correlating them within EMC Smarts Service Assurance Manager. EMC Smarts Business Impact Manager completes the solution by providing an integrated business view extending to VPN users, customers, and service agreements.