

Managing Next-Generation Networks: Service Assurance for new IP Services

Technology Concepts and Business Considerations

Abstract

The ongoing convergence of data and voice networks into next generation networks provides a significant financial benefit through the reduction of capital expenditures. Service providers and enterprises are now offering completely new types of services, making them more competitive and opening up new revenue streams. The key issue is the effective management of these complex service-oriented architectures. This paper discusses the unique management challenges posed by next generation networks (NGN), and how the EMC[®] Smarts[®] architecture is uniquely suited to address these challenges.

Copyright © 2006, 2008 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.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Part Number S0066.1

Table of Contents

Market Trends	4
New Wave of Services.....	4
Network Transformation.....	5
Challenges, Risks and Solutions when Managing the NGN.....	7
The EMC Smarts NGN Solution	9
Unified Data Model.....	9
Mediation.....	10
Automated Root-Cause Analysis	11
Impact Analysis	11
Deployment Architecture	11
Solution Components.....	11
EMC Smarts Business Impact Manager.....	13
EMC Smarts Service Assurance Manager	13
EMC Smarts IP Availability and Performance Manager	14
EMC Smarts MPLS Manager.....	14
EMC Smarts Network Protocol Manager.....	15
EMC Smarts VoIP Availability Manager	15
EMC Smarts Multi-Service Access Manager.....	16
Conclusion	17
Appendix A - Abbreviations	18
Appendix B - References	19

Market Trends

In the past few years, the growth in consumption of broadband services has not kept pace with falling prices for bandwidth from service providers. Consequently, margins are declining and service providers are rapidly transforming their network infrastructure in ways that both reduce operating costs and yet serve as the platform for newer, higher-margin services. Until such a transformation becomes reality, traditional service providers are selling lower-value, lower-margin solutions and face an increasing threat from smaller, innovative competitors with value-added, high revenue-generating services, targeting the fixed and—potentially more lucrative—mobile world of business and private users.

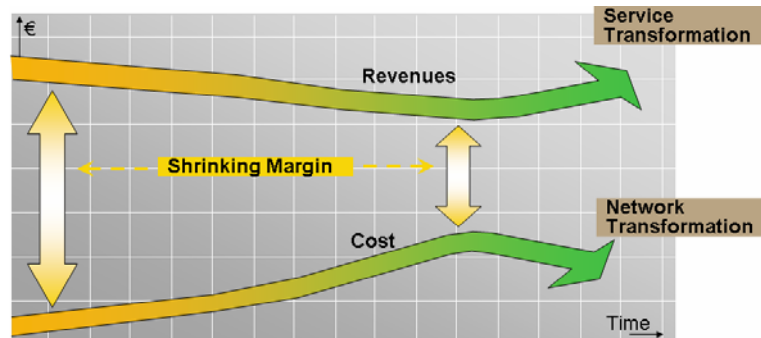


Figure 1 - Financial Trend within Service Provider

The way out of this deadly game requires at least two things: one being the transformation of the existing services into a new, attractive service portfolio in order to increase the average revenue per user (ARPU), and the second is improvements in operational efficiency—significantly lowering operating costs while dramatically increasing the service quality to the customer.

New Wave of Services

Next-generation services are driven by capacity-intensive content that is being delivered to a wider range of terminals than ever before, such as TV, PDA, Smartphone as well as PC-based browsers. Despite the various content sources and target devices, those services have one thing in common—they are currently or rapidly evolving to become IP based.

The new services referred to here, which are already being deployed and adopted by some providers, include IPTV for broadcast TV, Video on Demand (VoD), Voice over IP (VoIP) for telephony, as well as IP VPNs, enabling teleworkers to access their corporate intranet. There are others, not so well known yet, like Over IP Video (OIPV), streamlining demanded videos towards mobile devices, network-hosted Personal Video Recorders (nPVR) allowing the delivery and storage of personalized content, Games on Demand, Content Caching or VODcasting and Podcasting capturing voice or video for subscription purposes or location-aware services providing information in context to the actual location of the user — just to name a few.

It is also very popular to offer services like voice, video, Internet and wireless together as differentiated triple/quadruple-play bundles reducing the customer churn. Past statistical evidence showed that an average bundle of 2.7 services makes it very unlikely a customer turns down the whole package.

David Hawley¹, a senior analyst at The Yankee Group, says “Empirical evidence shows that the more services customers purchase from an operator the less likely they are to churn.”

According to Hawley, bundling two services usually reduces customer churn by 25 percent. Bundling a third product reduces it by an additional 13 percent, and a fourth product reduces churn by an additional 6

¹ Source: www.destinationcrm.com, Article “A 360-Degree View of Customers Is Not Enough” from March 29, 2004

percent. “It is a bigger hassle to cancel two services than one, hence minor annoyances that would lead one to churn do not lead a bundle to churn,” he says.

Just to demonstrate the significance of IP-based services in the telecommunications, media, and entertainment (TME) market, the market forecast for IPTV subscribers alone estimates 37 million subscribers in 2009 with a common average growth rate (CAGR) of 72 percent. The overall IPTV system revenue in 2009 is expected at \$9.9B US with a CAGR of 83 percent (Source: Multimedia Research Group, March 2006).

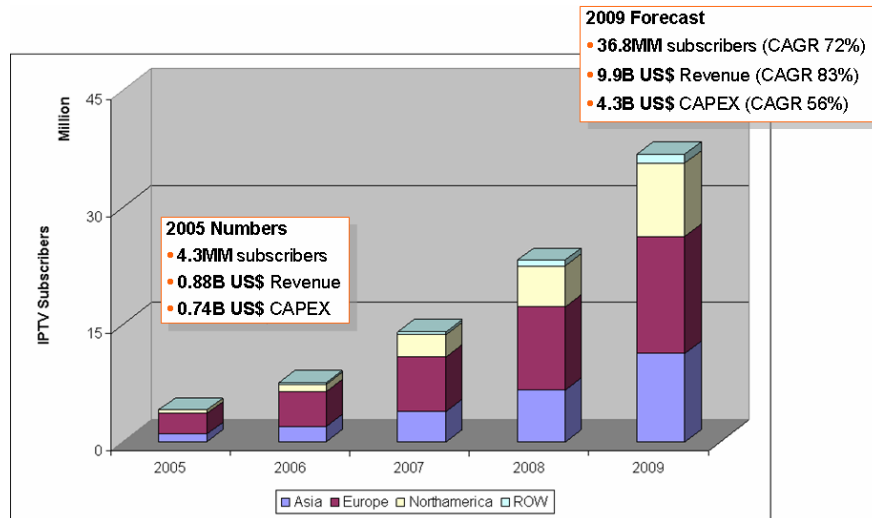


Figure 2 - IPTV Global Forecast – 2006 to 2009

Being first to market can be rewarded with up to 70 percent market share. However, it is not only speed-to-market that determines success and market share, it is also dependent on the general availability and reliability of the newly introduced service. Once the infrastructure is ready for delivery (availability)—from an operational viewpoint—it’s a matter of getting the provisioning (speed), assurance (reliability), and billing (cashing in) right.

The expected gains are promising and service providers are moving up the value chain and starting to host content—the traditional domain of content providers. On the other hand, content providers are deploying their own infrastructures in order to become independent of service providers. The third players in the game are cable operators, who are creating stiff competition with service and content providers.

From a competitive standpoint, it is absolutely crucial for service providers to solve the challenges of a converged next-generation network and its management architecture.

Network Transformation

In order to successfully support the variety of new services and to surf on the new wave of revenue generation, traditional service providers need to shift their mindset and transform their existing infrastructure into an end-to-end service delivery platform—the next-generation network (NGN).

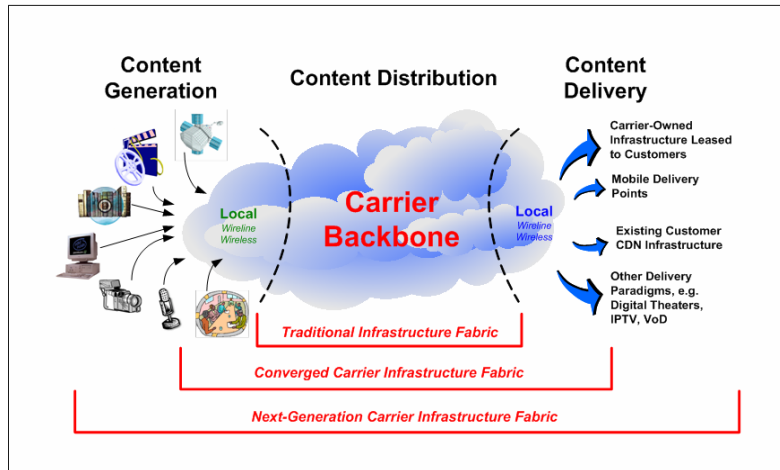


Figure 3 - Network Transformation towards NGN

NGN is a popular phrase used to describe a complete network architecture defined by the ITU and ETSI. The concept behind it is to carry legacy and new services over a QoS-aware IP network from any source to any subscriber device. Multiprotocol Label Switching (MPLS) is the key technology being deployed and combines the benefits of a packet-switched network with quality of service and class of service capability.

The ITU defined the term NGN in Recommendation Y.2001 as follows:

Next-Generation Network (NGN): a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

The diagram on the following page shows the architecture that has been defined for NGN. The transport plane is decoupled from the underlying access networks like DSL, ATM, WiFi, WiMAX, etc. and from the overlaid service/control plane. That flexibility enables service providers to perform a smooth and cost-efficient transition from existing service platforms to a converged architecture where new and legacy services coexist.

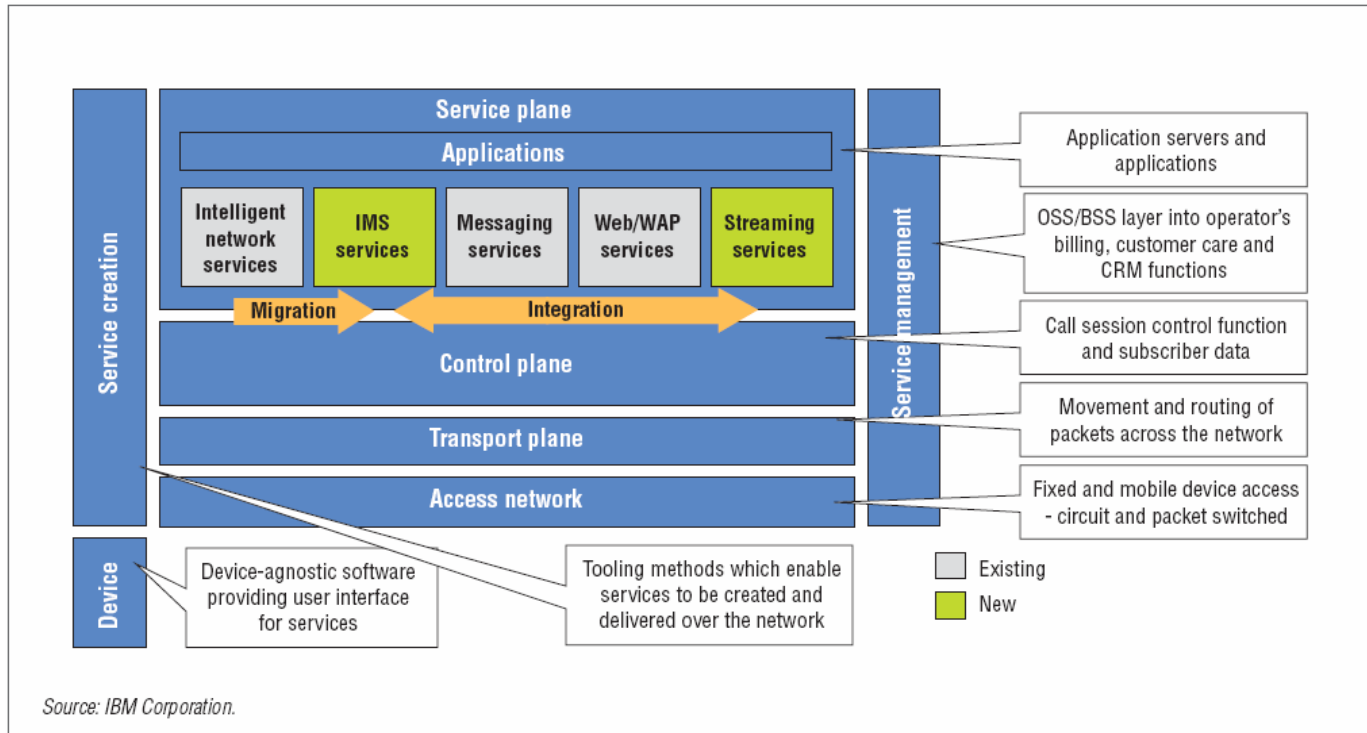


Figure 4 - Next-Generation Network Architecture

Challenges, Risks and Solutions when Managing the NGN

Evolving from a technology-centric, stove-pipe approach—where each service relies on a particular network technology—towards a horizontal, service-centric architecture is only achievable step by step. Legacy voice networks, access/core data networks, and wireless networks will collapse onto a single IP backbone based on MPLS. This goes along with a similar evolution on the management side: The vendor-specific management for each technology needs to be migrated into a more common management of “similar” technologies before it can finally turn into a single management view.

On paper this sounds easy enough, but in reality it’s a long and complex process.

Just consider the situation with OSS management: Each technology silo uses its own OSS architecture for Fulfillment, Assurance and Billing (FAB), which is costly, ineffective, and not scalable. On the service assurance side, the industry took some effort to develop technology-agnostic inventory and fault-management solutions: fault management uses a Manager of Managers (MoM) linked to a single Trouble Ticketing System, linked in turn to a CRM system. For Inventory Management, attempts have been made to build a single inventory of infrastructure and services and the dependencies between them.

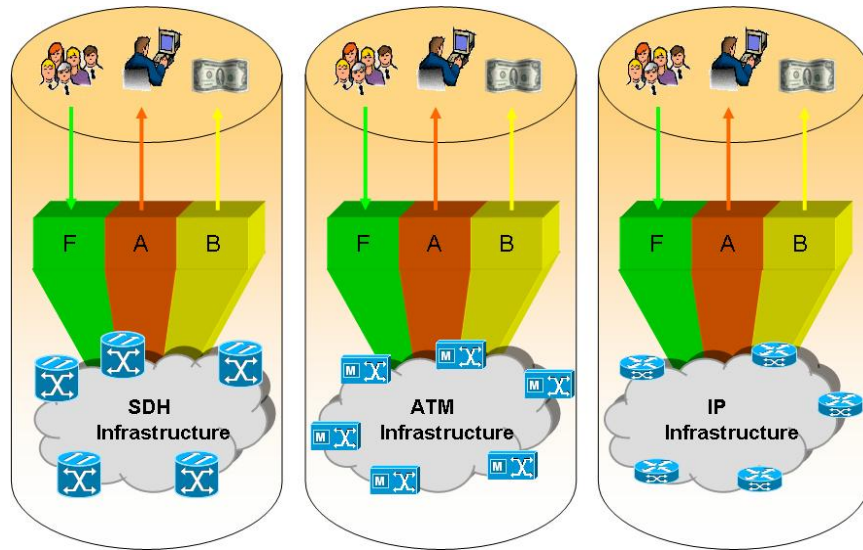


Figure 5 - Management within Technology Silos

However, there are still challenges: Inventory solutions are still technology-specific and use multiple repositories which are limited to service-assurance purpose, vendor-specific implementations, and can be costly to implement and not aware of the realtime status of objects. Also, traditional fault management has limited fault correlation, is lacking built-in logic, abstraction, and topology and is not scalable due to its rules-based approach. This is causing more issues for the service assurance and CRM layers where there is no connectivity information available and the associated ticketing/CRM services can't typically handle the high event rates.

Managing NGN is challenging. True-NGN might be considered as "one" network, but it is by far the most complex of all. Its management has to deal with multiple vendors, multiple physical devices from data and voice networks, multiple applications, multiple databases, and multiple service layers (infrastructure plane, control plane, service plane).

IN A NUTSHELL: SERVICE ASSURANCE FOR NGN IS A MULTI-DIMENSIONAL CHALLENGE.

A next-generation network is a very dynamic environment. Services are continuously being activated and deactivated. Devices are added, removed, and change configuration, thereby changing their connectivity or relationship to others. The increase in available instrumentation has meant an increase in the number of events and alarms presented to operators in a network operation center (NOC). In addition, the converged nature of an NGN means that every alarm could represent a service-affecting fault, but depending on redundancy and resiliency may not be service-affecting on its own.

The challenge to network operators is to identify from this vast stream of data what is important and to do this in real time. In order of importance the conditions which need identification are:

- Failures affecting service delivery to customer "right now"
- Failures, which are not service-impacting now, but cause loss of resiliency
- Deviations from expected network configurations, which may impact ability to achieve an SLA

Traditional approaches to management founded on rules-based correlation won't deliver in NGN environments. The sheer scale and rate of change means that it is impossible for such a solution to keep up to date with changes in the NGN. Network operators are deploying NGNs to allow the rapid rollout of new services. Having a time lag associated with the ability to assure new services is going to delay the deployment of new services, thereby impacting the ROI on NGN deployment.

As a consequence, a different approach is needed for managing service assurance of NGNs.

EMC believes that a model-based approach to management of complex multi-service environments such as NGNs is the most effective approach. This belief is echoed by organizations or guidelines such as the Telemangement Forum, IEFT, SNIA, and ITIL. A generic model is required that describes the services, their dependency on infrastructure and application components, as well as the behaviors and constraints associated with those managed objects. The associated objects should be automatically discovered, mapped against the generic information model, stored and re-discovered when necessary, so that the model reflects the managed environment at all times. This model then provides the basis for automated Root Cause Analysis and Service Impact Analysis without requiring constant maintenance.

Coupled to the data model described above, flexible, open and automated mediation is required, which allows the data model to describe the NGN environment regardless of vendor, model, or access method. While existing and emerging mediation standards such as SNMP, TMF814, MTOSI, and MTNM will, in time, reduce the mediation challenge, much of the existing equipment requires the use of other mechanisms. In conjunction with the data model, the mediation must be able to automatically adapt to changes in the environment. This automation includes discovering changes to the infrastructure and services, but also automatically applying the correct management policy. An example of such a policy might be to monitor the availability and performance of “gold” VPN services while monitoring the availability only for “silver” VPN services.

Any management solution for NGN must be architected such that it can scale to manage the current and projected NGNs. This scalability challenge has three dimensions which must be addressed as follows:

- Number of network elements/network size
- Range of technologies in the NGN
- Number of services/subscribers in use

Linked to this scalability challenge is a requirement for flexibility such that the solution can be rapidly adapted to support new services and technologies in future without the need for “forklift” upgrades. Another facet of this flexibility is the ability to integrate with other OSS applications to provide automated flow through from Order→Provisioning→Activation→Assurance→SLM.

For further information see [1]

The EMC Smarts NGN Solution

EMC® Smarts® address the requirements outlined above through the use of a set of patented technologies packaged in an application architecture which meets the requirements for scalable and flexible deployment architecture.

Unified Data Model

Embodied within every EMC Smarts application is a unified data model known as ICIM. Based on standards such as the IETF CIM, TMF SID, and others, ICIM provides an abstract description of infrastructure components, application services, control-plane services and business services. It also describes the dependencies and relationships between each of these.

This aspect of the ICIM model allows EMC Smarts to describe an NGN and the services provided by the NGN, regardless of vendor or technology, in one single place. This capability is particularly powerful when applied to managing today’s NGN architectures which are inherently multi-vendor and multi-technology.

As an example a typical NGN deployment will include legacy transmission network technologies such as WDM and SDH, with a variety of access technologies providing consumer connectivity. For high-density metro areas, providers are deploying Metro-Ethernet and FTTH access networks, medium-density access is provided by DSL, and low-density or mobility provided by WiFi, WiMAX , 3G, and HSPDA networks.

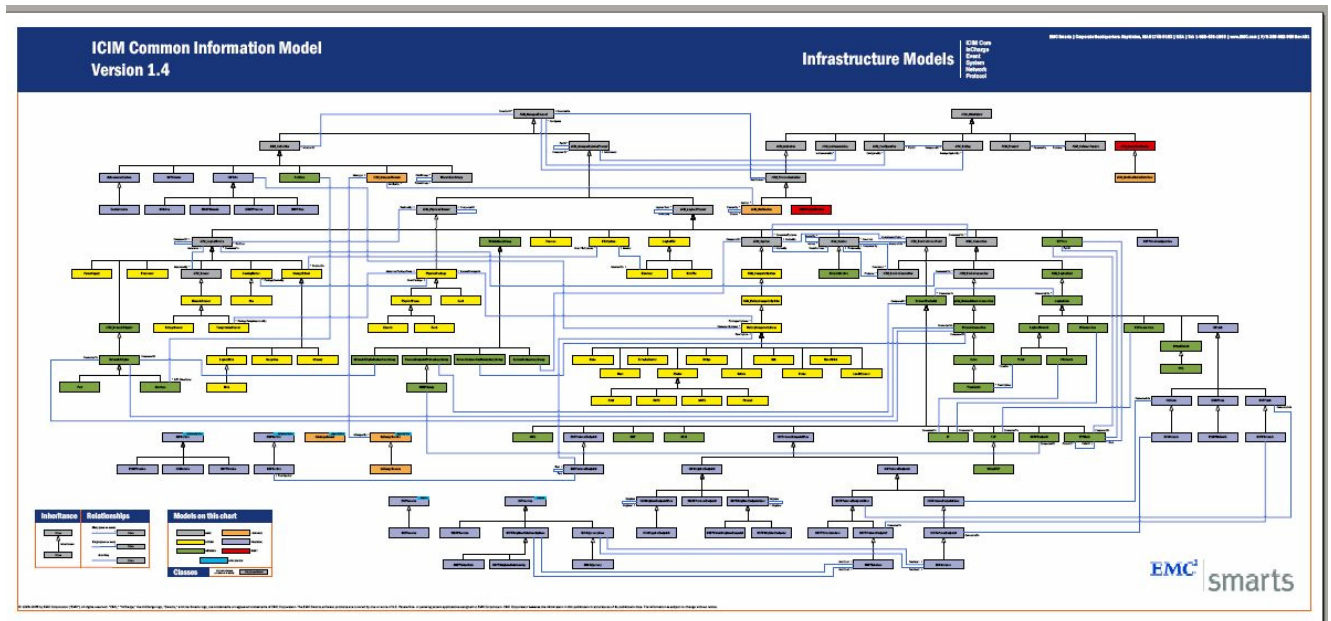


Figure 6 - The EMC Smarts Common Information Model (ICIM)

While the ability to describe the entire infrastructure and services in a single place is extremely powerful, EMC Smarts has taken ICIM a step beyond this by also modeling generic behaviors within infrastructures. These behaviors broadly cover known constraints and known propagation behaviors. As an example of constraint modeling in the network control plane, the model is inherently aware of the configuration parameters associated with protocols such as BGP and IS-IS and will automatically highlight when the control-plane configuration is incorrect. As an example of modeled propagation behavior, the model is aware of the fact that when a device fails, the impact of that failure will radiate outwards from the device along known L1/2/3 relationships. These behaviors are independent of vendor or technology.

For further information see [1].

Mediation

To apply ICIM to a service provider network requires a mechanism to populate the data model with the specific infrastructure components and configuration. This is achieved through the use of an automated and open discovery capability. While traditional IP networks have provided SNMP and allowed the use of direct device interrogation for discovery, many NGN components rely on Element and Network Management systems. To this end, EMC Smarts provides discovery capability across a wide range of mediation protocols including SNMP, TL1, TMF814, as well as proprietary EMS/NMS interfaces.

For example, in recent deployments, EMC Smarts MPLS Manager is used to discover and manage a single MPLS network through a mixture of SNMP and EMS. From the EMC Smarts console, an operator can view an LSP end to end even though it is layered over two vendors' equipment.

Today, EMC Smarts supports over 1,500 device types from many vendors over multiple mediation mechanisms. Due to the abstracted nature of the data model and the openness of the mediation framework, this number is increasing rapidly as in many cases, EMC Smarts customers can add additional device support.

The second aspect of the mediation framework is the ability to consume realtime state information from multiple sources and correlate the information within the model. As with discovery, EMC Smarts supports multiple mediation mechanisms to collect the data required. These include SNMP, TL1, TMF814, SysLog,

EMS/NMS, and programmatic APIs. In many cases these mechanisms have already been applied to network equipment to enable device support “out of the box” without requiring customization or integration.

Automated Root-Cause Analysis

Every EMC Smarts application embodies patented correlation and root-cause analysis technology, which leverages the ICIM model to automatically generate root-cause analysis logic. The data model described how fault conditions propagate along established relationships between infrastructure components, which allow the EMC Smarts applications to automatically precompute the likely set of alarms produced for specific failure conditions. Therefore, in realtime the EMC Smarts applications provide operations staff with the source of the failure, rather than the hundreds of raw alarms. This reduces the diagnosis time associated with network failures, thereby improving service quality to the customer.

For further information see [3] .

Impact Analysis

Coupled with the root-cause analysis, EMC Smarts provides the ability to describe the layering of business services over infrastructure end-points. The impact analysis engine then links the root cause to the impacted business services.

As an illustration, let’s take the example of a VPN service to a customer linking several sites. The VPN and the underlying MPLS network are automatically discovered. The VPN service is composed of a set of CE devices. Following a failure of a card in a PE device, the EMC Smarts application automatically provides a diagnosis of the card failure as being the root cause, explaining the fact that multiple CE devices are unresponsive. The business impact analysis then shows that the VPN service is impacted but links the cause of the impact to the PE card.

The key advantage of this approach is that the service model is highly simplified as the relationship between network core and access points has been automatically discovered. Without the unified data model and the root-cause analysis provided by EMC Smarts the operator would need to manually work out that the PE card and the VPN service are linked.

Deployment Architecture

The powerful architecture that drives all EMC Smarts solutions is highly distributed and scalable. EMC Smarts scalability advantages have been proven repeatedly in the marketplace, managing the world’s largest and most complex enterprise and service provider infrastructures. Today, EMC Smarts is in a leadership position in resource management, working with key vendors and operators to manage some of the largest IT infrastructure deployments in the world.

The keys to the scalability provided with EMC Smarts are distribution and abstraction. Distribution allows multiple cooperating software instances to be deployed in the optimal manner for the environment. Abstraction allows the results from the distributed components to be presented within a single topology model in a scalable manner, with the ability to drill down to the detailed composition of a single network element where required.

Solution Components

The EMC Smarts solution for NGN is a combination of multiple EMC Smarts products. Each product provides domain specific discovery, monitoring and root-cause analysis for dedicated technology layers.

Depending on the service provider’s exact requirements, the EMC Smarts solution for NGN is organized as an integration of domain-specific managers and may include:

- **EMC Smarts Business Impact Manager**, providing realtime impact of business services
- **EMC Smarts Service Assurance Manager**, correlating and presenting the relationships of all subtending domain managers
- **EMC Smarts IP Availability and Performance Manager**
- **EMC Smarts MPLS Manager**, including LSPs and their related policies.
- **EMC Smarts Network Protocol Manager** for BGP, OSPF, EIGRP, or IS-IS routing protocols and related interfaces
- **EMC Smarts VoIP Availability Manager** for media gateways, IP/PBX gateways, and other voice components
- **EMC Smarts Multi-Service Access Manager**

EMC Smarts integrates and correlates information across these domains by leveraging the EMC Smarts Common Information Model™ (ICIM). 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 7 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 the EMC Smarts Service Assurance Manager.

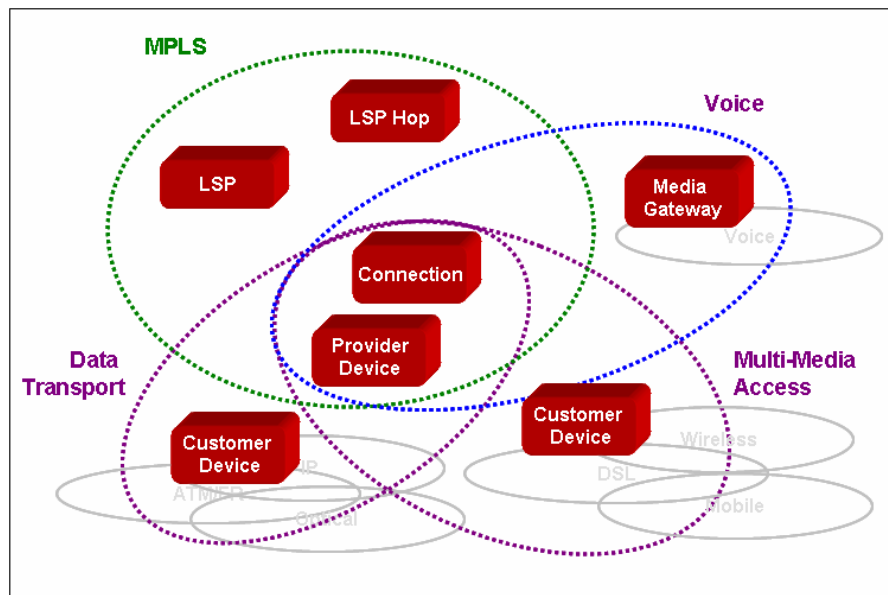


Figure 7 - Model Intersection Points

Another reason to use separate domain managers is scalability. If necessary, even a particular technology domain can be partitioned into several sub-domains each managed by one domain manager. Again, the EMC Smarts Service Assurance Manager is responsible for the integration and cross-correlation.

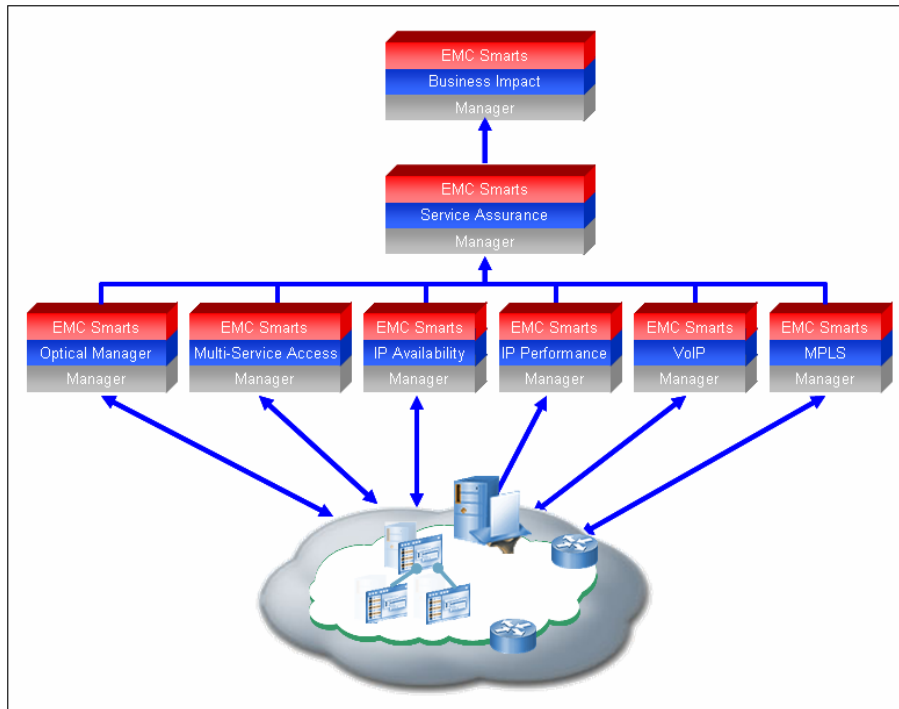


Figure 8 - EMC Smarts NGN Solution Components

EMC 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 EMC Smarts architecture supports seamless roll-up 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.

EMC Smarts Business Impact Manager

The EMC Smarts Business Impact Manager automatically calculates and determines the impact of infrastructure and application issues on business services and customers, and is the only solution that can model business processes and tie them to underlying infrastructure. With this precise impact analysis, service providers can take swift action to protect the services and processes most critical to their business.

For further information see[4] .

EMC Smarts Service Assurance Manager

EMC Smarts Service Assurance Manager is the cornerstone of the EMC Smarts management suite. It integrates and correlates topology, events, and analysis from its subtending domain managers and other sources and gives the system operator a seamless, high-level view of the overall entities and relationships in the underlying domains (Figure 9). It works with the EMC Smarts Global Console or EMC Smarts Business Dashboard to provide a real-time, end-to-end perspective on the business-critical IT environment, its health, and its impact on business processes.

Detailed information about the entities and relationships is still maintained in the technology-specific domain managers for IP, MPLS, DSL, Wireless, ATM/FR, etc. In addition to the infrastructure entities of those domain managers, Service Assurance Manager represents relationships between NGN service

offerings and subscribers and between NGN 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

During the auto-discovery of the customer-specific environment, EMC Smarts Service Assurance Manager builds a dedicated representation of it, called the EMC Smarts Common Information Model Repository. This is the basis for any end-to-end and top-down analysis of infrastructure and application problem , as well as their impacts across technology domains and to the business level.

As single integration point, the EMC Smarts Service Assurance Manager brings together business and operations support systems. It provides the basis to incorporate the complete EMC Smarts solution into an existing OSS architecture consisting of inventory and asset management systems, third-party fault and performance managers, CRM systems, etc. As a result, the user maximizes the value of existing tools, while leveraging the unique integration, correlation, and root-cause and impact analysis delivered by EMC Smarts solutions.

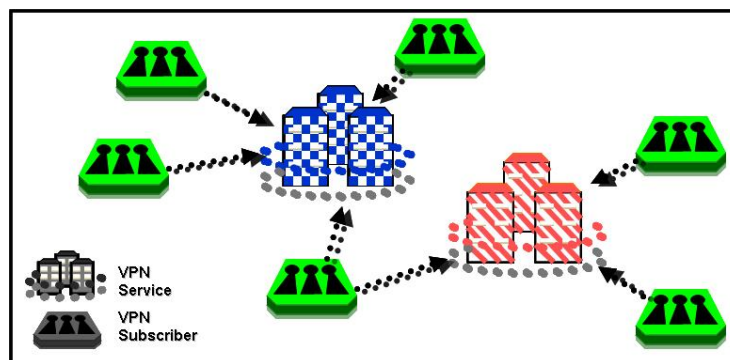


Figure 9 - EMC Smarts Service Assurance Manager View

EMC Smarts IP Availability and Performance Manager

The EMC Smarts IP Availability Manager is a core component of the EMC Smarts suite and provides a comprehensive solution for isolating faults and speeding problem resolution in complex IP networks. It automates realtime root-cause analysis of Layer 2 and Layer 3 network faults and determines the impact of these problems on the rest of the infrastructure. Instant, accurate, and totally automated diagnosis of service-affecting authentic problems helps to protect business-critical services.

For further information see [5] .

The EMC Smarts IP Performance Manager monitors the health of Layer 2 and IP elements in switched and routed networks and warns proactively of potential problems in the managed environment. It analyzes the root cause of network performance issues in real time and determines the impact of these problems on the rest of the infrastructure. This allows proactive fixing of those problems and keeping the infrastructure operating at peak performance.

EMC Smarts MPLS Manager

As Multi-Protocol Label Switching (MPLS) remains a key technology for next-generation networks, having the right management tools in place becomes vital. EMC Smarts MPLS Manager delivers the industry's leading MPLS management solution with the mission-critical fault management of virtual private networks (VPNs) and Label Switched Path (LSP) networks.

The domain manager leverages topology information from VPN provisioning systems, SNMP management information base (MIB) instrumentation, and other sources to automatically discover logical and physical

objects and relationships in MPLS and related domains. That includes PE (provider edge) and CE (customer edge) routers, LSPs and its corresponding LSP segments (hops), VPN Routing Forwarding (VRF) tables, Layer 2 and 3 VPNs, VPLS and VPN/MPLS connectivity.

EMC Smarts MPLS Manager also discovers the relationships between LSPs, their 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 protocols, 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 10).

For further information see [6] .

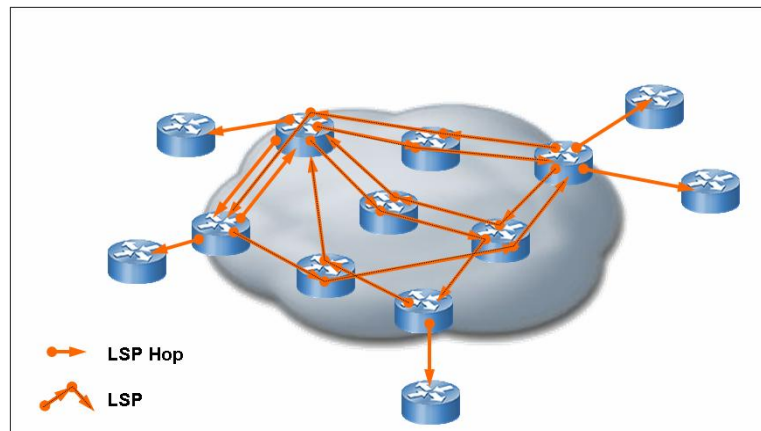


Figure 10- EMC Smarts MPLS Manager View

EMC Smarts Network Protocol Manager

EMC Smarts Network Protocol Manager extends management of the MPLS control plane by managing the routing protocols that support MPLS-based services and provides insight into routing process and adjacency failures, pinpointing root-cause problems in routing protocol domains and correlating these events with problems in the underlying IP network. The IP network availability is enhanced through deep discovery of the logical routing topology, monitoring of routing adjacencies, and explanation of their failures.

EMC Smarts VoIP Availability Manager

EMC VoIP Availability Manager delivers the same capabilities and levels of reliability associated with traditional network management tools. It addresses a broad range of VoIP devices—including voice switches, media gateways, hosts and VoIP application redundancy groups, IP PBXs, routers, and phones. It automatically discovers the elements, builds the topology of relationships and dependencies among VoIP devices in applications and the network infrastructure, maps VoIP entities to VoIP classes and monitors the VoIP network systems, as well as applications for availability, thereby immediately identifying the root cause of any problems.

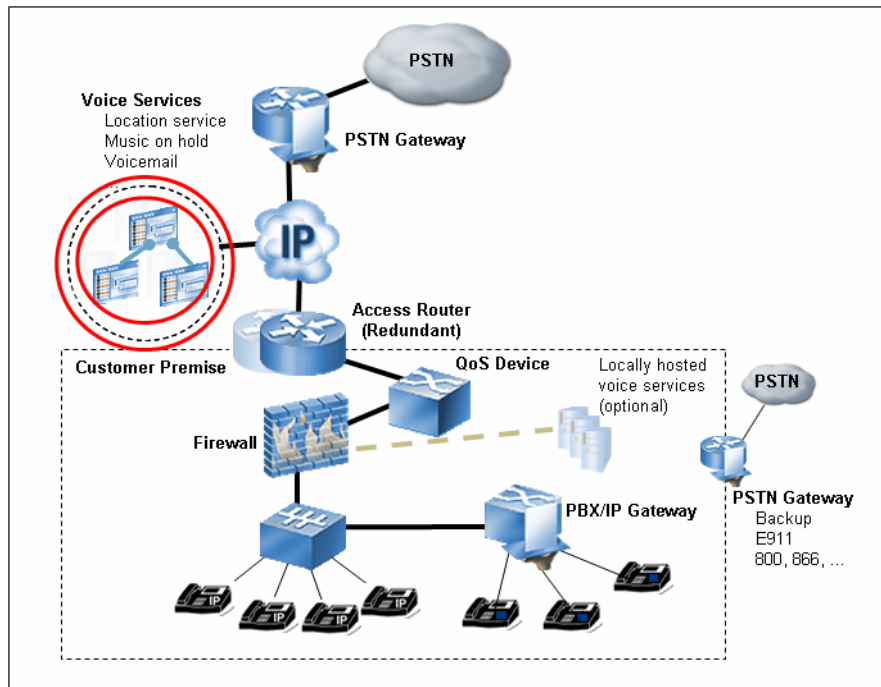


Figure 10 - Voice Components Managed by EMC Smarts VoIP

EMC Smarts Multi-Service Access Manager

EMC Smarts Multi-Service Access Manager monitors the availability of Access Network Elements such as DSLAMs and MSANs. Working with IP Availability Manager and MPLS Manager, it identifies the root cause of user access connectivity problems whether caused by failures in the access device or failures in the core network.

The EMC Smarts Multi-Service Access Manager can also be configured to monitor user connections and provide notifications when user connectivity is impacted by network failures.

Conclusion

The service provider community already recognized the value of the new services and started to roll out their NGN to support them. Depending on their service offerings and their individual burden of legacy services, the migration will vary from provider to provider. The common goal from a management perspective is to move from the vertical, technology-specific management towards a horizontal, technology-agnostic and service-centric management.

The most pressing NGN management requirement is the provisioning of a unified device and service view. Due to the growing complexity of NGN platforms, there is also the strong requirement to have a solution in place to automatically identify the root cause of a problem out of thousands of related alarms and to calculate the business impact on all affected services.

Excellent service assurance for legacy and emerging services is the key to satisfying existing and new customers. Due to the ever-increasing complexity of the managed infrastructure, the amount of problems are also increasing. Traditional service assurance solutions with a rule-based approach are now facing their limitations.

EMC Smarts can help to overcome the technology issues with its leading and patented model-based root-cause analysis and business impact calculation. Once the infrastructure, consisting of varying networking technologies, servers, applications, storage devices and even virtual resources is discovered, all subsequent changes and modifications in that dynamic environment are automatically detected and analyzed.

Benefits of the flexible and modular EMC Smarts solution can be grouped into three areas:

- **Business** — Actionable information is available at any time, enabling the service provider to react quickly according to business requirements, which increases service quality and customer satisfaction.
- **Operational** — Minimal maintenance is required due to automatic adaption to changes in the IT infrastructure. Immediate and actionable information significantly reduces the time and resources spent on fault isolation, which results in faster mean-time-to-repair and lower total cost of ownership.
- **Financial** — Existing assets and resources are utilized, decreasing the revenue and productivity loss. This leads to higher transparency and fewer SLA penalties.

Service providers need to consider their NGN management requirements carefully and consider the benefits of the approach described here in order to profit from their deployment of NGN services.

Appendix A - Abbreviations

3G	Third-Generation Mobile: general description of new mobile technologies
API	Application Programmers Interface
ARPU	Average Revenue Per User
ATM	Asynchronous Transfer Mechanism
BSS	Business Support System
CAGR	Common Average Growth Rate
CAPEX	Capital Expenditure
CE	Customer Edge Router in a MPLS network
CIM	Common Information Model
CRM	Customer Relationship Management
DSL	Digital Subscriber Line: Access Technology
DSLAM	Digital Subscriber Line Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing: fiber-optic transmission technique
ICIM	EMC Common Information Model
EIGRP	Enhanced Interior Gateway Routing Protocol: Cisco proprietary Internet protocol
EMN	Element Management System
ETSI	European Telecommunication Standard Institute: standard organization
FAB	Fulfillment, Accounting and Billing: Model of the Telemanagement Forum
HSPDA	Highspeed Downlink Packet Access: wireless, mobile access technology; part of 3G
IETF	Internet Engineering Task Force: standard organization
IPTV	Television over IP
ISIS	Intermediate System to Intermediate System Protocol: IP protocol
ITIL	IT Information Library: Guideline for Best Practice in IT environment
ITU	International Telecommunication Union: Standardization organization
LSP	Labeled Switch Path: End-to-End connection in a MPLS network
MIB	Managed Information Base
MoM	Manager of Manager
MPLS	Multiprotocol Label Switching: network technology
MSAN	Multi-Service Access Networks
MTNM	Multi-Technology Network Management: object model of the TMF
MTOSI	Multi-Technology Operations System Interface: standard interface the TMF works on
NGN	Next-Generation Network
NGOSS	New Generation Operational Support Systems: Initiative of Telemanagement Forum
NMS	Network Management System
NOC	Network Operation Center
nPVR	Network-based Private Video Recorder: service offering
OiPV	Over IP Video: service offering
OSPF	Open Shortest Path First: IP protocol
OSS	Operational Support Systems
P-Router	Provider Router in a MPLS network
PBX	Private Branch eXchange
PE Router	Provider-Edge Router in a MPLS network
QoS	Quality of Service
ROI	Return on Investment
SDH	Synchronous Digital Hierarchy: transmission technology
SID	Shared Information Data: standard framework from Telemanagement Forum
SLA	Service-Level Agreements: part of Service-Level Management
SLM	Service-Level Management
SNIA	Storage Networking Industry Association: standard organization
SNMP	Simple Network Management Protocol: standard protocol to manage IP devices
TL1	Standard Interface between network equipment and management systems
TMF	Telemanagement Forum; standard organization
TMF814	Solution Set for the Multi-Technology Network Management Interface,

VoD	Video on Demand: service offering
VoIP	Voice over IP: service offering
VPLS	Virtual Private LAN Service: VPN service on layer 2
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding
WiFi	Wireless Fidelity: wireless access technology
WiMAX	Worldwide Interoperability for Microwave Access: wireless access technology

Appendix B - References

All listed documents are part of EMC's Technical Library and are accessible via www.emc.com/techlib/. Look for "EMC Smarts" under the section "Softwa".

- [1] **Scalability Requirements for Managing the World's Most Complex IT Systems: EMC Smarts Distributed Architecture** , EMC Engineering White Paper, December 2005
- [2] **The ICIM Common Information Model** , EMC Engineering White Paper, October 2005
- [3] **Automating Root-Cause Analysis: Codebook Correlation Technology vs. Rules-Based Analysis** , EMC Engineering White Paper, October 2005
- [4] **EMC Smarts Business Insight** , EMC Engineering White Paper, October 2005
- [5] **EMC Smarts IP Availability Manager** , EMC White Paper, December 2005
- [6] **EMC Smarts MPLS Manager: Innovative Technology for MPLS/VPN Management** , EMC Engineering White Paper, December 2005