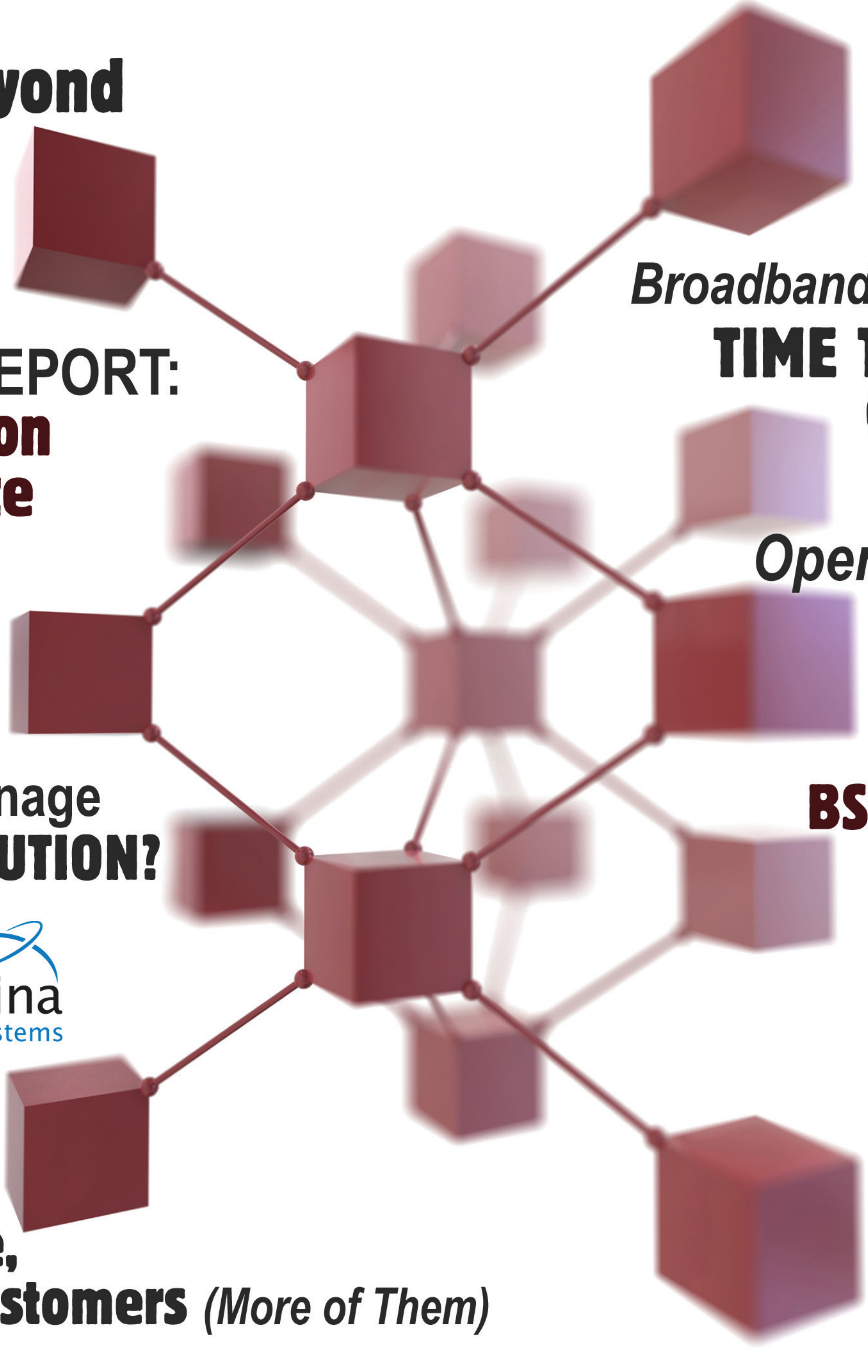
Pipeline | vol. 6 | issue 2

Pipeline

Your OSS/BSS Information Source.



IMS and Beyond

NewsWatch

Broadband Convergence: **TIME TO LISTEN TO CUSTOMERS?**

THE BSS REPORT: **Convergys on Convergence**

Opening Up **SCPs**

How Do I Manage **MY IMS SOLUTION?**

Sponsored by Nakina Systems

BSS Convergence *and Future Infrastructure Needs*

Letter *from the* **Editor**

Convergence, Costs, and **Customers** *(More of Them)*

The Future of Convergence

Pipeline

Your OSS/BSS Information Source.

Under the Covers: How Do I Manage My IMS Solution?

By Sergio Pellizzari

IMS means convergence and the promise of a unified experience: Communications with rich access to voice and internet and related services, with full access to multimedia and applications, and now with the ability for personalization.

Look under the covers and you'll see that the solutions offered by leading manufacturers consist of a complex myriad of individual products in the domains of Maintenance, Applications, Session Control, Charging, and Access. Softswitches, Media Gateways, Application Servers, Agents, Session Control entities, Policy and Billing servers are all common elements.

How do you manage a complex solution that has many subcomponents?

These subcomponents ride on Service delivery platforms and specialized hardware platforms but these subcomponents are often independent entities that may come from different organizations within the manufacturer as well as third parties. More importantly, each of these subcomponents has its own lifecycle. Some are mature products near the end of their lifecycle while others are quite new. Often, they run on different operating systems or different releases of an operating system. The result is a group of independent subcomponents expected to work as one, but what happens when they don't? How do you find misconfigurations? How do you deal with the interdependencies? How do you upgrade this complex set of subcomponents? Do you need to sometimes log into each subcomponent with different credentials? How do you integrate these solutions with other existing OSS back-office systems?

Very similar architectures are being used for IPTV, VoIP, and IMS, so how can these types of deployments be easily expanded to a much wider scale? It is difficult enough to manage a deployment in the lab, but how can these be rolled out nationally? Manufacturers are not offering higher level management solutions that unify these solutions, but rather are tying them together through marketing and an underlying expectation that operations staff will be left to struggle with maintaining each subcomponent, treating each individually. Often accompanying each of these subcomponents are large "method of procedure" (MOP) documents that provide comprehensive but complex lists of manual actions required to maintain each subcomponent. These MOPs involve many manual touches of the network components: manual parameter comparison, checks for existence of alarm conditions, and inventory baselining. These manual actions are highly error-prone, resulting in misconfigurations, misinterpretations, and potential outages.

Domain Control and Intelligence (DCI) solutions that act as a blanket across IPTV, VoIP, and IMS deployments are now becoming available and offer solutions to many of the problems that result from complexity and scale. You can consider DCI applications to be much more than single vendor Element Management solutions and even more than stovepipe Network Management solutions.

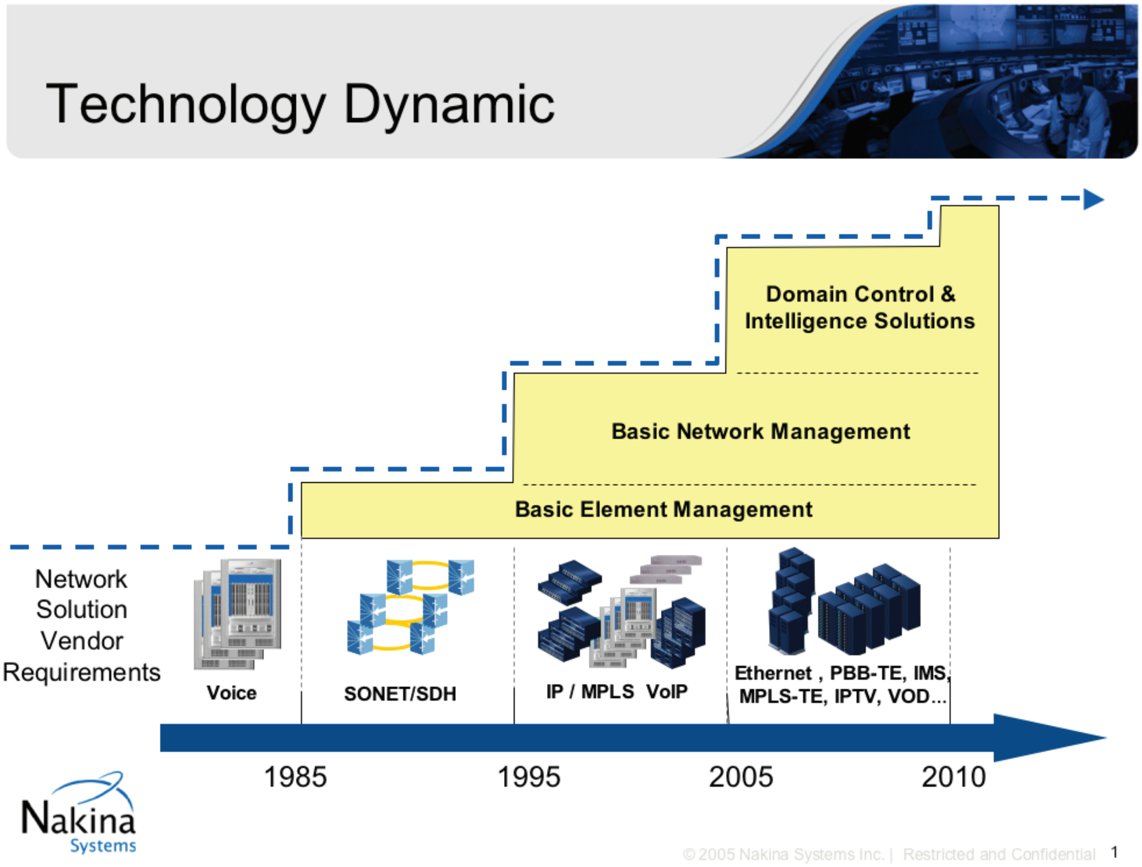
DCI applications treat your network devices as a network, not groups of individual nodes. DCI applications offer the ability to automate the manual steps found in these MOPs through predefined application workflows or by configurable workflows. By automating the MOPs, the average operator can now successfully and accurately perform these steps. Studies have shown that 70% of outages are caused by manual operations, making the automation and control of manual network touches a key element to improving network management efficiency. These elements are a key foundation of DCI applications.

One DCI solution can offer a Single Sign-On (SSO) proxy across these deployments, ensuring that operations staff use their own login credentials, and are offered access only to those subcomponents that their job function should allow them to access, completely eliminating shared credentials. This type of proxy allows operations staff controlled access to subcomponents through appropriate interfaces through a single portal, while ensuring that the right type of access is permitted based on the privileges for that user. A single point of security administration is offered, allowing administrators to manage user and group credentials and privileges, ensuring that operations personnel access is "right-sized." Furthermore, security administrators have access to full centralized logs of user sessions should outages need to be investigated and forensically traced for root cause analysis.

Studies have shown that 70% of outages are caused by manual operations.

Another DCI solution offers the ability to compare configuration data for specific subcomponents at very fine granularity with either similar subcomponents or templates that break down parameters into National, Regional, or local parameters. This solution offers a very efficient way to compare deployments without individual login to subcomponents. Errors caused by manual actions are quickly identified as deviances and can be quickly reset to "approved" parameter values.

An associated DCI solution is a workflow capability that automates the manual steps involved in the initial configuration or commissioning of IMS, VoIP, or IPTV deployments. Complex manual parameter settings can now be highly automated, streamlining the commissioning process so that, beyond initial IP address configuration, very few manual steps need to be initiated by the installer. No longer is the rapid deployment of new equipment dependent on each installer accurately configuring complex manual parameter settings immediately after power up. Accurate commissioning of newly deployed devices is now centralized, controlled, and tracked.


Technology Dynamic

Domain Control & Intelligence Solutions

Basic Network Management

Basic Element Management

Network Solution Vendor Requirements

Voice

SONET/SDH

IP / MPLS VoIP

Ethernet , PBB-TE, IMS, MPLS-TE, IPTV, VOD...

1985

1995

2005

2010

Nakina Systems

© 2005 Nakina Systems Inc. | Restricted and Confidential 1

Reduce and control manual touches on the network.

SERVICES TRICKLING TO MARKET?
Nakina Systems
OPEN THE FLOOD GATES
ROLL-OUT SERVICES AT UNMATCHED SCALABILITY AND SPEED

Backup and Restore is a key DCI solution that centrally backs up each subcomponent in a uniform manner, ensuring that the latest configuration data for each subcomponent is available should catastrophic failures occur, resulting in the loss of volatile store. There is a lot of comfort in knowing that the configuration data for each and every subcomponent of your IMS, IPTV, or VoIP solution is being properly backed up to ensure that recovery is straightforward.

The Network Audit and Software Delivery DCI application automates the upgrade process by first performing a series of software, alarm, and hardware audits, ensuring that the typical challenges and problems that can occur during an upgrade process be discovered and acted upon prior to commencing the upgrade. Furthermore, with large portions of the manual upgrade MOPs being automated, upgrades become much less prone to error and more repeatable over a nationwide or global deployment.

The Network Inventory DCI application unifies the inventory information for any IMS, VoIP, or IPTV deployment, providing a single point of access for this information through a unified GUI interface. Again, this is another blanket application that unifies your deployment.

Finally, DCI applications offer the ability to provide a single, unified northbound interface offering full inventory, alarm, and performance information through a machine interface, allowing for much easier integration into other OSS systems. Standards organizations are moving to web services-based interfaces, which have proven to provide ease of integration.

DCI applications also offer the ability to perform many standard maintenance and operational actions against your IMS, VoIP, and IPTV deployments without resorting to logging into cumbersome and complex CLI and nodal interfaces for each subcomponent.

Expect to see more DCI applications over the next few years as other complex technologies like LTE begin mass deployments. Domain Control and Intelligence applications are here now and will become more prevalent as customers demand more control over their complex deployments.

About Nakina Systems:

Nakina Systems provides Domain Control and Intelligence solutions to communications equipment and service providers worldwide. Our solutions enable service providers to scale new network service infrastructure more rapidly and cost-effectively.

What makes Nakina different? We combine:

- Proven scalability to 10,000s of nodes;
- Deep function-by-function control for elements of any complexity;
- Built-in configurability and tier one operations processes.

That's why Nakina solutions are deployed in daily use to manage critical telecom network infrastructure in over twenty four countries around the world.

Domain Control and Intelligence bridges the gap between "proven in the lab" and "ready for national and global rollout." Our ultimate objective is to enable service providers to roll out complex new infrastructure - Ethernet, IMS, optical, and wireless - without operational obstacles and expensive manual processes that slow deployment.

For more information please contact:

Sergio Pellizzari
sergiop@nakinasystems.com
1 (613) 254-7351 x222
http://www.nakinasystems.com/pages/contact.php

Nakina
Systems