Pipeline | Volume 7 | Issue 4

Pipeline

Your OSS/BSS Information Source.

Stepping Towards the Edge

Consolidation and Data Privacy Making Headlines

AT&T ON VoIP

The Secure and Profitable Edge

MANAGING MANY EDGE DEVICES

SPONSORED BY Nakina Systems Network Integrity

SOLVING THE BANDWIDTH CRUNCH

RIM's War

Letter from the Editor

LIVIN' ON THE EDGE

Pipeline
Your OSS/BSS Information Source.

Managing the Growing Myriad of Edge Devices

By Sergio Pellizzari of Nakina Systems and Walt Bowers of Hitachi Communication Technologies America, Inc.

The edge of the access network at one time simply involved reaching an end customer with a copper pair or a coax cable. Access equipment then became a little more complicated being through a DSLAM, CMTS, or other inside plant technologies, but the intelligence and complexity effectively remained in the service provider premises. Reaching a customer and managing the end-user experience was still achieved through management of simple termination points, and service guarantees were achieved through the inherent connectivity of the network.

Today and as we move into the future, access equipment lives on the edge, in the hands of the consumer. It is a piece of telco-owned or consumer-owned gear residing on the customer premises that is managed (at least partially) by the service provider. These devices include more intelligence to allow the operators and cable companies to provide a richer set of services to the consumer. Set-top boxes, DSL/Cable modems, broadband home routers, femtocells, and LTE assets: all are examples of service provider owned and managed devices that reside at the edge—on the consumers premises rather than being exclusively under direct physical control of the service provider.

Today's management systems need to manage the hardware edge device domain AND the applications platform middleware domain.

The certainty is that more and more types of edge devices are being developed and their complexity is skyrocketing. These devices will be managed, monitored and configured by the service provider and that management needs to be remote, scalable, and secure. Management systems need to evolve to be capable of managing the scale and complexity of these devices. TR-069 has been used as a starting point for edge device configuration but we need to move beyond it's capabilities and there are so many more devices that do not support TR-069 yet require similar management capabilities.

As the intelligence on these edge devices continues to increase, their importance to the service provider continues to increase as well.

- These devices become the key gateway and control element of the home network.
- Service providers introduce new home network based services and applications to generate additional revenue.
- Therefore, these edge devices also become the "application platforms" for the service provider to introduce new revenue generating applications.
- Finally, the broadband battle between telcos and MSOs moves from a "most bandwidth wins" battle to a "win the home network, win the subscriber" battle.

Therefore, the remote management of these edge devices, and the applications and services operating through them, becomes essential to the service provider's success.

A critical question that is very challenging to answer would be: "Which devices in my network do not follow a defined 'Gold Standard'?"

Pipeline Publishing L.L.C

Traditionally, vendors that do not follow new paradigms in network management expect operations staff to log onto every device, navigate the GUI or command line interface, manually inspect the parameter settings and determine compliance of many parameters to the gold standard. At which point, each parameter for each device is manually checked off a master list of devices to record the fact that inspection has been completed on that device. This process clearly falls well short when it comes to dealing with large numbers of parameters or devices, and a system that automates these process steps becomes mandatory for operational efficiency and customer satisfaction.

What if a new version of software needs to be deployed to those edge devices? The equipment vendor has likely provided a suitable manual procedure, and a large document is available to allow operations staff to step their way through the upgrade process for a single device at a time. One device completed, 99,999 devices to go. Edge devices that are deployed in large numbers need special consideration for functions like service activation, upgrades, backups, security, etc. These functions must be managed by OAM systems in such a way to allow large numbers or groups of devices to be acted upon together, en masse.

New edge devices such as home gateways, plug computers, and set-top boxes are becoming even more interesting, because many are integrating software-based application platforms such as OSGi (Open Services Gateway Initiative) to provide enhanced device intelligence and additional feature rich services. The capabilities of these devices are expanding to not only provide traditional home internet service, IP telephony and associated computing functions, but also to introduce home services in the "app store model". A consumer can purchase software from a service provider that could include value-added functionality such as home automation, home security, home nursing, remote meter monitoring, entertainment, gaming, or any number of other useful functions. Software application installation and configuration obviously needs to be managed on these devices in addition to the management of the devices themselves. Adding the applications and services on top of the device increases the number of objects that need to be managed. This again begs for a new paradigm in how these edge devices are managed.

OSGi and other application-enabled platform devices rely on common services and functions shared by many different applications. Making sure that these services are installed and configured correctly on hundreds of thousands or even millions of devices requires the ability to insure that large numbers of parameters are correctly configured. Monitoring the configuration against common profiles such as the "Gold Standard" becomes absolutely critical.

Today's management systems need to not only manage the hardware edge device domain but also the applications platform middleware domain running on that device as well, and perform the following functions:

- Maintain a database of inventory information, configuration information, version/release information, etc. and that database needs to be redundant, fault-tolerant, highly reliable, highly available etc. to meet the service provider's demand for high quality services to its subscribers.
- Receive, prioritize and manage alarms and alerts as well as provide historical trends and analysis for both domains (also with the same high reliability and availability described above).
- Gather performance metrics and monitor statistics for both domains, also with historical trends and analysis.
- Provision, configure and upgrade both domains in the edge device. Provide customer and operations security for both domains.

The edge is changing and the need for centralized management solutions is critical, especially those that promise new paradigms in management of both device and application domains, and that focus on dealing with these domains en masse, automatically configuring, continuously auditing them, managing not only the devices but their parameters and software in bulk.

Nakina solutions are used by three of North America's top five service providers.

About Nakina Systems:

Nakina Systems, the network integrity company, enables service providers to avoid outages and efficiently manage rapid growth of new distributed network infrastructure such as LTE, IMS, FTTh, and cloud applications. The company's solution portfolio is based on the ultra-scalable Nakina Network OS operations platform, and includes Intelligence applications such as the Network Integrity Controller, an automated network software audit and gold standard discrepancy manager, and the Network Discovery and Reconciliation Manager, an online network inventory discovery solution and Network Security and Single Sign on, a comprehensive credential system with secure access and video logging capabilities.

Nakina solutions are used by three of North America's top five service providers, and delivered as OEM products by three of the world's top ten communications equipment providers.

For more information please contact:

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