Case Study:
Nucleus Connect

October 2012

Europe:
Infosim GmbH & Co. KG
Friedrich-Bergius-Ring 15
97076 Wuerzburg, Germany
Tel: +49 931 20592 200
E-Mail: info@infosim.net
WWW: http://www.infosim.net

Americas:
Infosim North America
Suite 125
13785 Research Blvd, Hwy 183
Austin, TX 78750, USA
Tel: +1 512 410 6848
E-Mail: info@infosim.net
WWW: http://www.infosim.net

Asia-Pacific:
#04-103C German Centre
25 International Business Park
Singapore 609916
Tel: +65 6562 8286
E-Mail: info@asia.infosim.net
WWW: http://www.infosim.net

Background

Nucleus Connect is the operating company for Singapore's Next Generation Nationwide Broadband Network, an all-fibre optic network reaching every home and business, over **2.5 million end-points**. The network provides user speeds of up to **1Gbps** and delivers key services for businesses such as cloud computing, high-definition video (IPTV) and voice services (VoIP).

In 2009, Nucleus Connect awarded contracts for the new network hardware and OSS/BSS management components to a number of vendors. Due to various issues, the management product chosen failed to meet the requirements and they began evaluating other solutions in February 2011.

Nucleus Connect was contracted to have a working OSS/BSS system in place and functioning to specification by August 2011 to pass a governmental (iDA) audit in order to receive the next seven digit public funding grant.

Customer Requirements

Nucleus Connect required a **fully automated service assurance system** for their next generation fibre-optic transport network. This network comprised an MPLS core, active Ethernet access networks and a passive optical access segment based on GePON (IEEE 802.3 standard).

The network is designed to transport point-to-point connections (PWE3) and point-to-multipoint (VPLS) traffic encoded with dot1q. At the same time it also delivers VRF/VPN connections for IPTV. The backhaul capacity uses DWDM between 11 'Common Offices', or peering points, allowing for future upgrades as necessary.

The solution required needed to be a fully automated flow-through system which would **seamlessly integrate** with existing order-management, single-sign-on, portal, trouble-ticketing and service desk systems.

The customers of Nucleus Connect, the retail service providers, place orders through a fully automated B2B service. Orders must be processed through a zero manual interaction facility using the service assurance solution. Network Operations must not be required to perform any tasks or configurations related to service delivery and are released to do their job: **Manage the network**.

The OSS/BSS solution needed to have the ability to integrate with existing service database and logging systems. At the same time, Nucleus Connect must be able to monitor the key network service delivery components as well as retail service provider service virtual services. Accurate impact and root-cause analysis was a critical requirements to support customer SLAs.

Case Study:
Nucleus Connect

The StableNet® Solution

Infosim installed StableNet® Telco to comprehensively manage the entire active network, the DWDM transport and all server, storage, database and network appliances. A fault-tolerant system was installed in the central location with StableNet® Agents in each of the 11 Common Offices for distributed management.

As standard, StableNet® is a multi-vendor solution which is able to support new devices and features with low implementation and adaption efforts. Even with the complex integration requirements, total solution deployment and integration took **16 weeks** and comprised **240 man-days** of employee time.

Fault and Performance Management

Management is delivered using SNMPv3, Syslog, direct SQL and CSV processing. All processes related to service delivery, fault and performance management are **fully automated and completely integrated**. StableNet® manages and monitors the entire infrastructure including all network devices, servers and key application processes.

This high level of automated monitoring means that the time to repair faults has been shortened dramatically. Proactive monitoring has guaranteed Nucleus Connect, and by extension their retail customers, a high availability of revenue generating business processes through demanding SLAs and KPIs.

Systematic faults across different locations are quickly identified and solutions put in place to mitigate them. Trend analysis allows for proactive planning before problems arise whether that is with a telecommunications circuit, switch, air conditioning unit or a single battery within a UPS.

OSS/BSS Integration

StableNet® receives service change requests from the order processing systems via an encrypted web service interface. When a request is received the associated network resources are automatically provisioned. The new resources are identified before monitoring and measurement policies are applied. All changes are automatically detected and the resources updated. Finally, root-cause and impact rules are configured for the new service, customer and infrastructure before creating the necessary portal performance, fault and SLA reports.

Once the update process is completed, all the physical and virtual resources are covered by pro-active monitoring and reporting. Fault management is facilitated through a two-way integration with the Nucleus Connect trouble ticketing system. The StableNet® root-cause analysis engine ensures that a genuine fault has been detected and is not a false-positive before opening a ticket within the system. When the fault is rectified the ticket is automatically closed. The status of all open tickets are updated in real-time within the StableNet® client application and the customer portals.

Summary

After being selected by Nucleus Connect in March 2011, Infosim worked closely with the client to ensure delivery of a complete solution within the tight timescale. The StableNet® solution went fully live with Nucleus Connect and their retail customers in July 2011 and has been in continual use since then. This has enabled Nucleus Connect to deliver a **fully automated "Dark" NOC** (Network Operations Centre without onsite personnel).