



The Network Environment

Korea Telecom operates 31 KORNET Network Service Centers (NSC) nationwide.

Challenge

To monitor, analyze and troubleshoot rapidly increasing traffic to prevent service disruption and facilitate preparations to provide multimedia services.

Solution

Sniffer Distributed enables continuous surveillance of changing traffic conditions and rapid resolution of problems, providing enhanced diagnosis, monitoring, and troubleshooting capabilities as well as scalability for future expansion.

Benefits

Sniffer Distributed deployed across the NSC network allows Korea Telecom Ethernet easier analysis of Gigabit traffic and speeds troubleshooting, thereby obtaining stable service operation. In addition, the modular architecture provides flexibility of configuration to cope with changing needs.

Korea Telecom Corporation is Ready for a Multimedia Explosion, Thanks to The Sniffer Distributed System

Introduction

Korea Telecom Corporation (Korea Telecom) is the largest telecommunications and Internet service provider in Korea. Korea Telecom seized the number one position in Korea, in June 2000, a mere year after the company entered the high-speed Internet market. In September 2000, Korea Telecom subscribers surpassed the one million mark for the first time among local telecom players.

Korea Telecom has established itself firmly as a world leader in broadband service. Korea Telecom's subscribers exceeded four million in March 2002 and grew to five million in January 2003. By 2004, Korea Telecom's volume skyrocketed by more than 880% and is currently still growing at a rate of 30-40% annually.

Korea Telecom introduced Sniffer Distributed to the network to manage the ever-increasing traffic driven by rapidly increasing subscribers and to facilitate preparations to provide multimedia services.

Deploying 24x7 Traffic Surveillance System for the Backbone Network

Service providers require continuous surveillance of traffic conditions and preparation for potential problems and post-event forensics. This is essential because even minutes of service disruption or any delay to customers can be a catastrophe. Korea Telecom felt that its traffic analysis solutions were insufficient to analyze and troubleshoot the ever-increasing traffic and decided to replace them with solutions designed to monitor gigabit links.

Korea Telecom aimed to establish a system to monitor backbone traffic 24x7 through the upgrade. When traffic congestion occurred, the network utilization rate and frame transmission rate of each segment must be identified and the node that caused the congestion must be found instantly. Checking traffic conditions on a regular basis is also important because server traffic conditions are directly related to the service quality for users.

Additionally, collecting and analyzing harmful packets is necessary. It is essential that a service provider has the capabilities to determine causes of service failure and to analyze incoming data packets to identify worms and viruses or the possibility of hacking attacks. Security capabilities against threats from unknown network worms and viruses should also be secured. By monitoring traffic flows and patterns 24x7 for possible harmful attacks, the IT staff can isolate the source and cause and provide stable services.

Finally, assigning in-line 24x7 traffic analysis of major nodes to provide in-depth traffic analysis capabilities was required.

With these goals, Korea Telecom began the process of selecting a vendor for this upgrade project.

Powerful Traffic Assessment and Analysis Tool Required For Stable KORNET NSC Network Operation

Korea Telecom operates 31 KORNET Network Service Centers (NSC) nationwide. To analyze the protocol of the NSC network, Korea Telecom decided to adopt a traffic analysis tool to examine abnormal traffic and secure stable system operations.

To adopt the optimal solution, Korea Telecom took the following items into consideration.

- Any indication of abnormality in the 10/100/1000Mbps Ethernet and wireless 802.11 a/b/g networks should be detected from one console and accurate data on the abnormality should be extracted in the fastest-possible time frame.
- In order to analyze abnormal packets in an emergency, an intuitive graphic user interface should be available in real-time through a matrix traffic map.
- When harmful packets of defined form and type or abnormal traffic occur, response measure options should be provided.
- More than 400 protocols based on RFC should be analyzed and captured.
- When new Internet threats such as unknown viruses or worms occur, causes should be identified and analyzed and appropriate countermeasures should be taken immediately.

The solution for the project should have practical analysis functions such as the capability to capture packets of necessary size and simultaneously save captured files. These are the requirements Korea Telecom used in selecting an appropriate solution. Because even minutes of service disruption or any delay to customers can be a catastrophe.

Most Advanced Technology and Excellent Support Capability

During Korea Telecom's evaluation of companies that participated in the open competition, NetScout met the technology standards with the highest technology score as well and also received excellent marks in technical support. Sniffer Distributed is based on Sniffer Portable, equipped with decoding and expert systems familiar to Korea Telecom network engineers.

A project manager at Korea Telecom said, "[NetScout's] products are well known as the industry's best data filtering and analysis tools. Their modular structure provides scalability and their excellent technical support system enables fast troubleshooting."

After multifaceted assessments including technology, performance and support, Korea Telecom decided to introduce Sniffer Distributed. Sniffer Distributed is a modular, high-performance hardware solution designed for high speeds and complex enterprise network architecture. In particular, with a modular chassis design, Sniffer accommodates up to four full-duplex Gigabit Ethernet links and eight Gigabit Ethernet media modules which provides configuration flexibility and manageability, reducing space requirements.

The system's excellent network monitoring capability, high-speed capture ability at a maximum of 8 Gbps, asymmetrical routing, monitoring and troubleshooting capability of multilink trunking provides Korea Telecom with quick and accurate analysis and management of anomalies and performance across a complex network. Korea Telecom explained that Sniffer, in particular, provides network-specific analysis technology that supports more effective and accurate network performance management.

The project manager at Korea Telecom said, "Sniffer Distributed is optimized for networks, so it makes the analysis of Gigabit [Ethernet] traffic easier and is suitable for swift network troubleshooting." He continued, "Sniffer Distributed provides a sufficient level of detailed and specialized data when conducting traffic diagnosis consulting for clients such as Yonsei University and Kookmin Bank, and provides enhanced troubleshooting." Furthermore, Korea Telecom is satisfied with the quick and smooth response for requests for technical support.

"With the development of the Internet, the IP-based media including Internet TV, video chatting and multimedia continues to increase. It is very important for service providers to regularly assess and analyze the growing traffic and provide stable services. The analysis tool meeting this requirement is Sniffer Distributed."

**Project Manager
at Korea Telecom**

In an extensive test accommodating the maximum modules at the NSC in South Gyeongsang area, the Sniffer Distributed successfully conducted traffic analysis and performance management work during full operation. Korea Telecom expects that Sniffer Distributed will have no problem supporting the system when the network is expanded.

Korea Telecom plans to utilize Sniffer Distributed in the analysis of malicious codes once its use for traffic analysis and troubleshooting is stabilized. Korea Telecom also plans to expand its use for BcN, its next-generation multimedia communication environment. Korea Telecom is confident that Sniffer's performance management and troubleshooting capability will help the company maintain stable and high-performing Internet services.



About NetScout Systems

NetScout Systems provides advanced network and application service assurance solutions that deliver complete visibility into real-time, packet/flow-based operational intelligence. IT operators at the world's largest enterprises, government agencies, and service providers use the Sniffer and *nGenius* solutions to troubleshoot service degradations faster and more efficiently in order to reduce MTTR.

Our world-renowned Sniffer and *nGenius* solutions include:

- Intelligent Data Sources for high capacity, deep-packet recording and monitoring
- Analysis Software for real-time and historical network and application performance management, troubleshooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application services

Corporate Headquarters

310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 888-999-5946
www.netscout.com

European Headquarters

NetScout Systems (UK) Ltd.
100 Pall Mall
London SW1Y 5HP
United Kingdom
Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters

Room 105, 17F/B, No. 167
TunHwa N. Road
Taipei, Taiwan
Phone: +886 2 2717 1999
www.netscout.cn

©2008 NetScout Systems, Inc. All rights reserved. NetScout, the NetScout logo, Network General, the Network General logo, *nGenius*, Sniffer, InfiniStream, Business Container, Business Forensics, NetVigil and Quantiva are trademarks or registered trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.