(Press Release)

February 26, 2004

Nippon Telegraph And Telephone Corp.
NTT Communications Corp.

NTT Com Begins Operations at OCN of "ENCORE" inter-AS diagnostic system, targeting the construction of an Internet environment with outstanding stability

World's first implementation of an automatic routing information anomaly monitoring and detection system in commercial Internet services

Nippon Telegraph and Telephone Corp. (NTT; Head Office: Chiyoda-ku, Tokyo; President: Norio Wada) and NTT Communications Corp. (NTT Com; Head Office: Chiyoda-ku, Tokyo; President: Masanobu Suzuki) has announced that it will introduce "ENCORE(*1)," a new inter-AS diagnostic system developed by NTT Laboratories, starting from April 2004. The system, which will be incorporated into NTT Com's OCN(*2) Service Network, will automatically monitor and diagnose anomalies in routing information(*3), and is the first in the world to be implemented in a commercial Internet service.

The engine used in the ENCORE system is an innovative technology that enables automatic monitoring and diagnosis of anomalies in routing information between multiple ISPs (Internet Service Providers) on the Internet. Agents(*4) with the ability to observe and diagnose routing information are placed at each ISP, and the information gathered is automatically integrated and analyzed to determine the causes of anomalies.

In this way, it is possible to quickly discover, analyze, and recover from anomalies in routing information between multiple ISPs -- which had been difficult in the past, when individual ISPs conducted monitoring and diagnosis manually -- and to construct high-quality Internet environments that offer outstanding stability (Fig. 1).

The Internet is a conglomeration of countless networks, and the stability of connections between networks is dramatically affected by the service quality of individual providers. NTT Com has constructed a routing monitoring system using ENCORE as its engine, and has incorporated this system into OCN's service network, a world's first for a commercial Internet service (Fig. 2). This implementation is a part of NTT Com's efforts to improve connectivity, which is a fundamental element of network quality.

Background to Implementation

The Internet is a huge aggregate of countless networks, called "Autonomous Systems (AS)," which are operated by ISPs, universities, companies, or other organizations. An IP packet(*5) sent from one AS must pass through several other ASes before finally reaching the targeted AS.

During this process, routing information is exchanged between ASes to set the IP packet route, but a problem has been recognized for some time in that because each AS has its own routing information management policies(*6), inconsistencies in policies between ASes can occur very easily. Furthermore, because policies are set manually, routes have suffered from instability due to setting errors and other problems; at times, there have been incidents of large-scale losses of connectivity. Another problem that has become increasingly serious recently is the appearance of malicious individuals who illegally "hijack"(*7) Internet routes, or use networks to send "SPAM"(*8) mail. There have already been numerous reports of setting errors and routing anomalies due to malicious intent, and the most significant anomalies resulting from the effects of these Internet vulnerabilities are seen in the context of DNS(*9) and BGP(*10). Incidents of loss of connectivity due to routing anomalies could represent a life-or-death issue for customers using the Internet as a core element of their business in recent years, for example in the case of Internet shopping.

In the past, however, routing anomalies between ASes could only be analyzed manually by network operators with specialized skills, and it was extremely difficult for network operators to constantly monitor huge volumes of routing information that changed from moment to moment in order to discover such anomalies at an early stage.

NTT Laboratories thus initiated research targeting automatic route anomaly diagnosis technologies as a part of its efforts to counteract the instability and vulnerabilities of the Internet, and in 2001, NTT's Network Innovation Laboratories developed ENCORE, the world's first system of its kind. Later, NTT verified the effectiveness of the system in evaluation tests on a global scale, connecting four locations inside and outside of Japan. NTT Network Service Systems Laboratories, in collaboration with NTT Com, confirmed the system's feasibility on actual networks, and at the same time added "Missing Route Monitoring" and "Hijack Monitoring" functions based on the results of new research. This process has led up to the start of full-scale operations on the OCN service network.

Effects of System Implementation

The implementation of this system enables continuous monitoring of constantly changing routing information to achieve real-time detection of routing information anomalies, which had been difficult in the past. In this way, network operators can respond quickly to anomalies, and Internet connectivity for customers can be improved.

(1) Improved stability of IP packet transmission

Automatically detects routes that are missing from OCN's routing table, enabling improvements in the stability of IP packet transmission between OCN and other ISPs.

(2) Improved quality and security

Automatically detects when OCN routing information has been hijacked, enabling identification of the problem AS to allow improved quality and security.

Keys to ENCORE's technologies

(1) Placement of Agents (Fig. 3)

Encore places agents with monitoring and diagnostic capabilities at each ISP, integrates the information gathered by these Agents to infer routing information behavior, and analyzes the causes of anomalies. When an abnormality is detected through regular monitoring, the system diagnoses the anomaly and identifies the factors inhibiting communications. This process functions even when a single ISP (AS) is comprised of several elements (sub-ASes).

(2) Missing route monitoring function (Fig. 4)

When a route is omitted due to an erroneous filter setting by the network operator or a

difference in policies among ISPs, the agents at the two ISPs in question exchange and analyze observation information to automatically detect routes that are missing from a given ISP's routing table, enabling improved stability of IP packet transmission.
(3) Hijack monitoring function (Fig. 5)
ENCORE detects cases in which a given router's routing table have been rewritten due to an erroneous routing information advertisement from another ISP, and identifies whether the source of the error is being operated as a proper "punching hole"(*11). In this way, when a given ISP's route has been taken over as a result of an illegal setting by a malicious third party or an erroneous setting resulting from an oversight by a network operator, the situation can be quickly and automatically detected, and the ISP at the root of the problem can be identified.

Future Developments

NTT Laboratories will continue to promote research and development in autonomous network management environment based on intelligent agents as an extension of the ENCORE system. At the same time, NTT Com will continue its efforts to provide the world's highest level of quality and service as a "Global IP Solution Company," aiming for even safer and more secure network applications.

Glossary

***1 ENCORE**
Stands for "Inter-AS diagnostic ensemble system using cooperative reflector agents." NTT Network Service Systems Laboratories created an illegal route detection system based on an intelligent diagnostic system developed by NTT's Network Innovation Laboratories, adding on new functions in the process.
***2 OCN**
Stands for Open Computer Network. A large-scale domestic Internet connection service provided by NTT Com. Service began in December 1996, and the number of subscribers surpassed four million in November 2003.
***3 Routing information**
A type of destination information required for IP communication between ASes. Exchanges of information between ASes enables interactive IP communications.
***4 Agent.**
As the name suggests, in the context of computer networks, this term refers to a function (or software) that autonomously gathers information and assesses network conditions to execute appropriate operations without the need for operations by the user.
***5 IP packet**
A unit used when transmitting information via the Internet. Information is divided into small segments (packets), each of which contains destination information.
***6 Management policy**
Operation rules that determine how actual IP packet transmissions will be controlled.
***7 Hijack**
In the context of the Internet, "hijacking" refers to taking over routes on which IP packets are transmitted.
***8 SPAM mail**
Commercial e-mail sent in huge volumes, without the receiver's consent.
***9 DNS**
Stands for Domain Name System. An system for providing IP address allocation

services based on a given host name.

***10 BGP**

Stands for Border Gateway Protocol. One of the communication protocols used in environments like the Internet, where multiple networks are interconnected, to exchange routing information between various networks. Currently, BGP is the main communication protocol used to control route information between ASes on the Internet.

***11 Punching hole**

A multihomed site connected to multiple ISPs may obtain a small prefix from a ISP and announce it from multiple ISPs to achieve better reachability. This technique is called "punching hole".

For further information,plese contact:
NTT Information Sharing Laboratory Group
Planning Division
Public Relations:Chizuka,Sano,Ida
Tel. +81 422 59 3662 / koho@mail.rdc.ntt.co.jp

NTT Communications Corporation
Media:
Akiko Suzaki or Tei A. Gordon
Media Relations, NTT Communications Corporation
Tel. +81 3 6700 4010 / info@ntt.com

NTT Communications Corporation
All others:
Satoshi Imai
Broadband IP Services Business Division, NTT Communications Corporation
Tel. +81 3 6700 8619 / sa.imai@ntt.com

NTT NEWS RELEASE