

Title	Constructing high availability application servers
Author(s)	Inoguchi, Yasushi; Shikida, Mikifumi; Tan, Yasuo; Matsuzawa, Teruo
Citation	Research report (School of Information Science, Japan Advanced Institute of Science and Technology), IS-RR-2001-026: 1-5
Issue Date	2001-12-06
Type	Technical Report
Text version	publisher
URL	http://hdl.handle.net/10119/8394
Rights	
Description	リサーチレポート (北陸先端科学技術大学院大学情報科学研究科)

Constructing High Availability Application Servers

Yasushi Inoguchi, Mikifumi Shikida, Yasuo Tan and Teruo Matsuzawa
Dec. 6, 2001
IS-RR-2001-026

Center for Information Science
Japan Advanced Institute of Science and Technology
Asahidai 1-1, Tatsunokuchi
Nomi, Ishikawa, 923-1292, JAPAN
inoguchi@jaist.ac.jp

©Yasushi Inoguchi, 2001

ISSN 0918-7553

Abstract

Application servers such as a mail server in the integrated network are required high availability because the server failure stops all systems in the network. Adding redundant network interfaces and service program, our application server keeps their service when a server get into troubled. We implement these approaches on our network and evaluate its efficacy under real network system operation. In consequence, routing schemes for file servers can reduce roundabout routing, and high availability application servers have been continued minimum level services for users in the network.

Introduction

Recently a number of servers and workstations on a network are rapidly increasing, and many sites have a large number of client machines and a lot of large scale high performance servers. However there are no effective implementations to manage these large scale systems.

This paper shows network management operation method for large scale and integrated systems based on experience on JAIST (Japan Advanced Institute of Science and Technology) network. The network in JAIST is one of a great scale network system and it include a number of workstations for each students or faculties, large file servers, some massively parallel computers, and other network servers. Both availability and performance are required for network design because all users in JAIST access all workstations or servers through the network. Each client workstations have to select optimal routing to handle a great number of accesses in the network. Moreover, application servers such as mail server or WWW server are also required performance, availability, and protection capability against cracking.

In this paper we propose approaches and techniques to control these system efficiently, and discuss its effectiveness. We implement these approaches in our site and shows result of operation with these techniques. We show detail of methods that are adopted by JAIST network about network design, routing for file servers, and high availability schemes for application servers.

High Availability Application Servers

High Availability Scheme

Next topic is application servers such as mail[MAIL] or WWW servers. Different from the conventional network, an application server in the integrated network required high performance and high availability, because all users in the network access only one application server. These application servers also required capability of defense against cracking attacking from outside the site[NS], although these servers have to provide useful information to inside users to keep usability. Thus problems for application servers are how to keep availability and how to offer both usability and defensiveness against outside the university. In this subsection we discuss mail server as an example of application servers.

Mail server system in FRONTIER consists of two servers. One-server offers relaying mail service for mail coming from outside of the university, and the other server offers mail spooling, smtp, and pop services for inside users. These servers are a complementary pair for high availability. Figure 1 shows network connection around the mail servers. There are two barrier segments. Inner barrier segment connects mail servers to client workstations in the university, and outer barrier segment connects the mail servers to outside WAN. Each mail

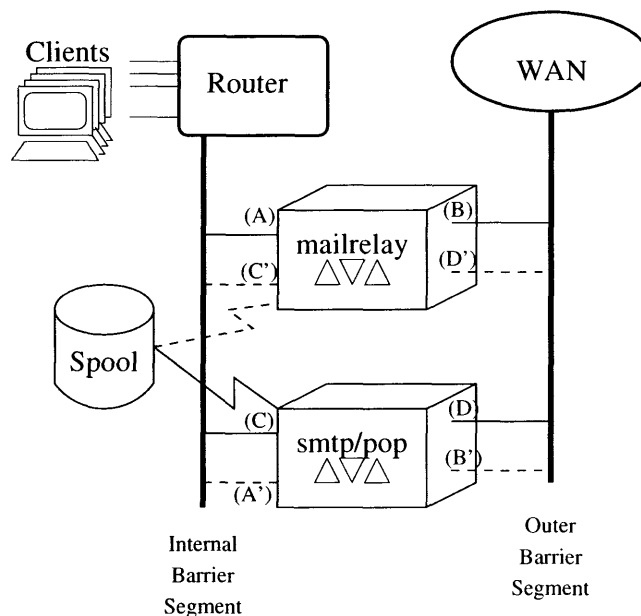


Figure 1: High Availability Mail Server

servers are connected these two barrier segment directory by primary network interfaces like (A), (B), (C), (D) in the figure. These server also have redundant network interfaces like (A'), (B'), (C'), (D') in the figure. Spool disk is connected both servers but only one connection is used at same time.

Normal State Operation

At normal state, primary network interfaces are activated and redundant network interfaces are not used. Figure 2 shows packet flow for mail receiving, mail reading, and mail sending. Coming mails from outside the university are received by mailrelay server, and sent to the smtp/pop server, then stored to the spool disk ((a) in figure 2.) User read the spooled mail by accessing the smtp/pop server like (b) in the figure. Sending mail is simpler as shown in figure 2 (c). Mails from inside users are sent to smtp/pop server through inside barrier network and spooling, then sent to outside WAN through outside barrier network. Thus coming mails and outgoing mails pass through different route.

From viewpoint of security, the mailrelay server offers limited information to protect against cracking, because it accepts connection from the outside WAN. On the other hand, smtp/pop server should offers many useful information such

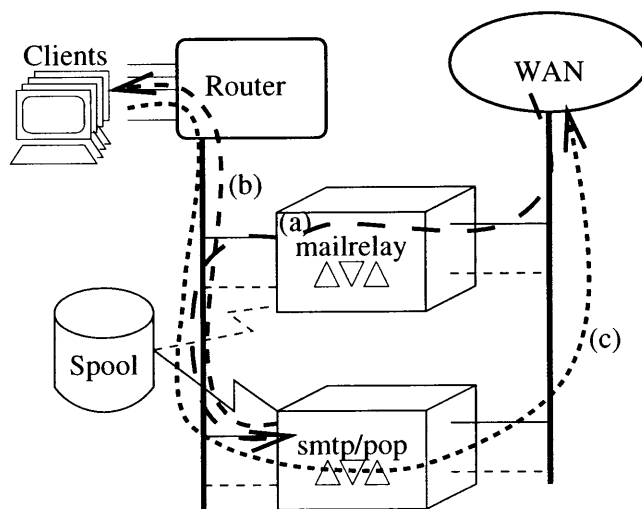


Figure 2: Routing for Mail at Normal State.

as members of mailing lists to enhance usability. This server accepts connections coming from only inside of the site. Thus, inside user benefit of usability keeping defensiveness against cracking.

Operation at a Server Failure

Now we consider about availability against a server failure. Figure 3 shows operation at the smtp/pop server failure. If smtp/pop server broken, mailrelay server activates its redundant network interfaces. IP addresses used by original smtp/pop server is set to the redundant interfaces, and the smtp/pop server can be acceptable both traffics to the smtp/pop server and traffics to the mailrelay server. The spool disk is disconnected from smtp/pop server and connected mailrelay server. Then the mailrelay server can also act as a smtp/pop server.

In this case, coming mails are received by the mailrelay server as normal state but these mails are stored to the spool disk directly by the mailrelay server (shown as figure 3 (a).) Since mailrelay server also offers pop service, stored mails are read from the spool disk through redundant interface ((C') in the figure) of the server like figure 3(b).

Outgoing mails are sent from inside workstation to the mailrelay server through redundant network interface ((D') in the figure), and these mails are throw toward outside WAN. The route (c) in the figure shows this traffic. No user notices the server trouble since service for users are continued.

On the other hand, in case of smtp/pop server failure, smtp/pop server also

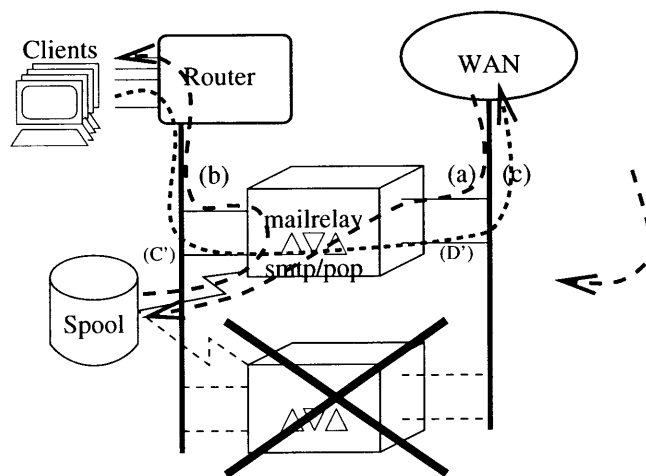


Figure 3: Routing to keep Availability.

activate their redundant network interfaces, and offer both mail relaying and smtp/pop services with these activated redundant network interfaces.

Evaluation

Our FRONTIER has been used this high availability application server for half year. Against our expectation, this system has some disadvantage. We have to maintain application program twice. Under simple smtp/pop server configuration, we maintain only one program on one server. However under this high availability system, we have to maintain programs both on smtp/pop server and on mailrelay server. Moreover, configuration for these application programs must be different between primary service and redundant service because server's condition is not same. Therefore administrator has to install an application program to two servers with different configuration. As the result of this complicated installation, it is difficult to work the program correctly at any time.

Although these disadvantage, we have been provided minimum level services continuously at anytime. There are no client workstation trouble caused by this mail servers system for this half year.

Conclusion

This paper addressed schemes to construct integrated network. Comparing integrated network design and conventional network design, it was shown that the integrated network design has many advantages. However there are many hurdles to realize a large scale integrated network.

Constructing network policy, a routing method for file servers in a large scale network, and a high availability scheme for application servers are discussed. These schemes are installed and evaluated in FRONTIER which is a sample of large scale integrated networks. The routing method for file servers effectively reduced traffic between In-House backbone routers, and the high availability scheme could keep minimum level services for inside client workstations. As the result, proposed schemes are helpful to construct the integrated network. Evaluation under controlled conditions is future work.

References

- [DNS] Paul Albits and Cricket Liu, *DNS and BIND*, O'Reilly & Associates, Inc., 1992.
- [MAIL] Bryan Costales and Eric Allman, *sendmail, Second Edition*, O'Reilly & Associates, Inc., 1997.
- [NETB] Brendon W. Mills, *Where To Turn For Network Bandwidth*, Unix Review, July 1995.
- [NS] Charles Kaufman, Radia Perlman, and Michael Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall, 1995.
- [RFC1058] Hedrick, C., *Routing Information Protocol*, STD 34, RFC 1058, 1988
- [RFC2328] John Moy, *OSPF Version 2*, RFC2328, 1998.
- [RFC2453] Gary S. Malkin, *RIP Version 2*, RFC2453, 1998.