A Reliability Design Method for Private Networks

Hitoshi WATANABE; Nippon Telegraph and Telephone Corporation (NTT), Tokyo
Minetoshi KUDO; Nippon Telegraph and Telephone West Corporation (NTT West), Osaka
Kazuhiro KAWANISHI; Nippon Telegraph and Telephone West Corporation (NTT West), Osaka
Koji YAMASAKI; Nippon Telegraph and Telephone West Corporation (NTT West), Osaka

Keyword: Network, Design, Telecommunication, Solution-provision business

SUMMARY AND CONCLUSIONS

A method for the reliability design of private networks is proposed. This method is intended to assist in the business of providing private networks that satisfy customers. A new reliability model for networks is proposed based on a consideration of actual network structure. Measures for reliability are defined in terms of network applications and an algorithm for the evaluation of reliability is established. The method is implemented as a software tool for use in network design. Some examples of evaluation in relation to the solution-provision business are presented.

1.0 INTRODUCTION

Reliability is an important factor for telecommunication networks, so reliability design is an important factor in constructing highly reliable telecommunications networks at reasonable cost. Methods of reliability design and management for public networks, including methods of specifying targets for reliability, are fairly well established. For example, the Network Reliability Council in the USA assesses the reliability of the service provided by a telecommunications carrier over a certain period by using the Outage Impact Measure (OIM), which quantifies the effect of telecommunications service outages[(1)]. Each telecommunications carrier manages its network reliability to keep the total OIM over a certain period below a certain level. NTT, the biggest telecommunication carrier in Japan, has reliability-engineering standards that specify reliability targets for telecommunications services, and designs the public network according to these standards[(2)]. Thus, there are fairly clear reliability targets for public network, and efforts are made to meet them.

In a private network, on the other hand, a customer's sites are connected via leased circuits provided by a telecommunications carrier (Fig. 1). Such networks have been becoming more and more popular. Many private networks are used in client-server configurations. In such a situation, whether or not backup servers are in place, are important factors that affect the network's reliability. Furthermore, the number of leased circuits and their redundancy configuration also influences both reliability and cost.

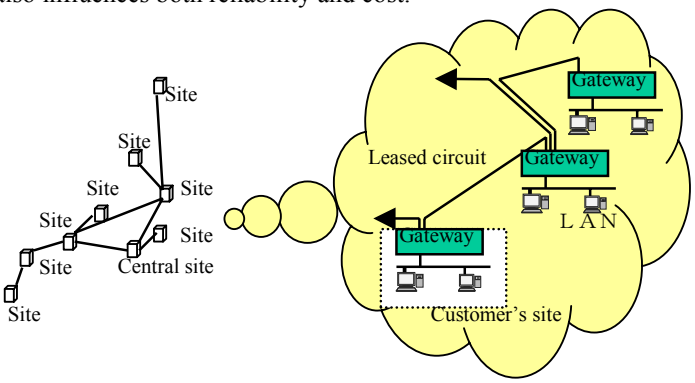


Fig. 1 Example of a private network.

Therefore, we require a reliability design method in which these factors are considered. For certain reasons, however, such reliability design methods have not been established for private networks. Two of these reasons are given below.

(1) Private networks are used in various ways, i.e., as server-client type systems or for site-to-site communication, so common reliability targets will not be suitable for all private networks.
(2) In many cases, the owner of a private network is also the user of the network, and the network designer is the telecommunications carrier that provides the leased circuit. This relationship is different from the case of a public network. Under these circumstances, the owner's satisfaction with the network design, based on a deep understanding of the relationship between reliability and cost is more important than reliability in itself.

The second reason is particular to the solution-provision business. That is to say, from the viewpoint of this business, various network configurations that are proposed must be based on an understanding of the customer's requirements in terms of reliability and cost. A simple software tool for evaluating the reliability of private networks would provide a means for solving these problems. However, while we have

0-7803-7717-6/03/$17.00 © 2003 IEEE

private-network-specific tools for documentation and traffic simulation, we do not have specialized tools for reliability analysis.

To solve these problems, we have developed a tool for evaluating the reliability of private networks and have used it to investigate the reliability and cost characteristics of certain types of private networks.

The private network of today is mainly used for IP-based communication. Although the final reliability of the communication is affected by the reliability of the applications, in this paper we only consider whether or not route are available. This is the first step in the reliability analysis of IP networks.

2.0 RELIABILITY MODEL

The targets for reliability analysis are networks constructed by using leased circuits to connect the LANs at a customer's sites (Fig. 1). Each leased circuit connects two routers, which act as gateways to the LANs. The network is divided into two parts. One is the WAN part, which is the carrier side of the network including the routers, and the other is the LAN part. Some of the LANs might have one or more servers (including backup servers) and it may be important for them to be accessible form other sites. This paper gives an analysis of the WAN part. Although we have carried out a similar analysis of the LAN part, it is not included in this paper.

In the WAN part, two routers become capable of communicating with each other when they are directly connected by a leased circuit or connected via other routers. In actual IP communications, the bandwidth and number of hops are related to such aspects of communications quality as packet loss or latency, which are thus important factors in network reliability. Here, however, we do not consider these factors.

Customers of leased circuits may think that a leased circuit is a simple line that connects two sites, and that it has a certain probability of failing. Such an understanding, however, only covers the logical level of the network. An actual leased circuit is a sequence of network elements, i.e., transmission systems or subscriber cables. Therefore, this paper deals with a model of a private network in which distributed customer sites are connected by leased circuits, which are accommodated in network elements. Each element has a certain failure probability. This model allows us to analyze the effects of common-cause failures of two or more circuits. Here, the word "failure probability" denotes both unreliability in a time-dependent situation and unavailability in a stationary situation.

In establishing a method for reliability evaluation and developing a software tool to implement the method, we encounter conflicting demands. For example, on the one hand we need to insure model's generality while, on the other hand, we need to restrict variation within the model for the sake of simplicity in software development. Therefore, to take both requirements into account, we define only the following kinds of elements in this paper (Fig. 2). The terms for these network elements and their meanings are given below.

(1) Customer's site and subscriber cable: The leased circuits from a customer's site are accommodated in a subscriber cable and go to the carrier's office. Failure of this element stops all circuits at the customer's site. This might occur through cutting of the subscriber cable or a breakdown of the power-supply system at the customer's site.
(2) Telecommunications node: A main element in the carrier 's network. All circuits accommodated in a node stop when it fails. This might occur when the power-supply system in the carrier's office breaks down.
(3) Telecommunication link: Another main element of the carrier's network. All circuits accommodated in a link stop when it fails. This might occur when the transmission cable is cut during road-works.
(4) Items of equipment in the telecommunications node: A failure here only stops those circuits accommodated in the item. In general, a telecommunications node has multiple elements.
(5) Router: In general, a customer's site has multiple routers. Failure of a router stops all of the circuits that terminated there.

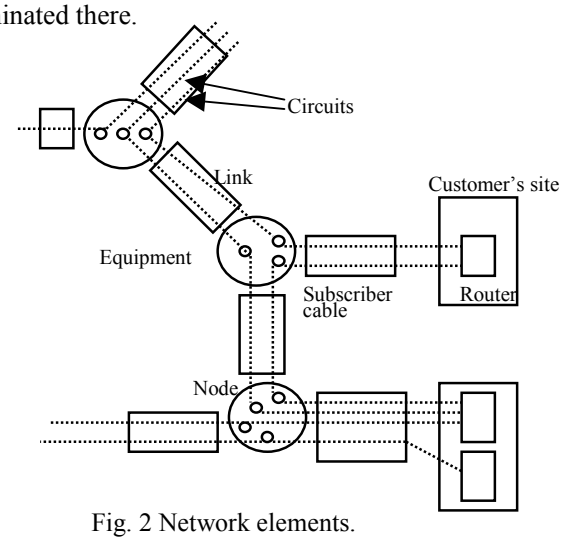


Fig. 2 Network elements.

3.0 MEASURES OF RELIABILITY

A measure of reliability should reflect the kind of work performed and the way the network is set up. A typical usage is as a client-server system. In this case, the main server is set up in a central site and is accessed from other sites. Another usage is to have sites communicating with each other on an equal basis. Furthermore, a network's reliability under disastrous conditions is also important. Reliability under normal conditions is reliability when failure events for individual elements are independent and each element has its own probability of failure. In a disaster, on the other hand, many elements will be damaged at the same time. Therefore, measures that reflect how well the network continues to function when many elements fail are appropriate as the measures of reliability under disastrous conditions. The specific reliability measures are defined as below.
Reliability under normal conditions:
(1) Probability that one or more of the sites is unable to

communicate with any of the other sites
(2) Probability that two particular sites are unable to communicate
(3) Probability that a particular site is unable to access the server or backup server
(4) Probability of a particular number of sites being unable to access the server or backup server
The first and fourth measures are affected by the overall network configuration.
Reliability under disastrous conditions:
(1) The number of customer sites from which the server or backup server is accessible when one or more specific elements is out of service.
(2) The probability that the server or backup server is accessible from a certain number of customer sites when the probability of failure during the disaster is extraordinarily high for a specific group of elements.

4.0 EVALUATION ALGORITHM

4.1 *Basic idea*

Each element has two possible states: up or down. The total number of network states is 2^N, where N is the number of elements. Checking all states is one way of evaluating the reliability, but is too complicated. Therefore, our tool starts by checking states with small numbers of failed elements then proceeds to those that have larger numbers of failed elements. The errors in evaluation are also estimated. In the actual situation, the probability of an individual element's failure is very low, so the above method gives adequately accurate results. Furthermore, in the listing of states, the tool omits those states that are known to have been down on a previous check. For example, if a state in which a certain element fails but no other elements fail causes network failure, then all other states in which the given element fails will also crash the network. We apply these characteristics to reduce the amount of calculation required of this tool. An outline of the algorithm follows.

Let us consider the situation in which the check has started with those states where one element fails and proceeds through those states in which increasing numbers k of elements fail. The following sets and probability are defined.
Set *A1*: The set of states in which the number of failed elements is one and that result in the network being down.
Set *A2*: The set of states in which the number of failed elements is two and that result in the network being down but whether the network is down or up is not known only from the previous check.
……
Set *Ak*: The set of states in which the number of failed elements is k and that result in the network being down but whether the network is down or up is not known only from the previous check.
Set *Bk*: The set of states in which the number of failed elements is k and that does not result in the network being down but whether the network is down or up is not known only from the previous check.
Set *Ck+1* : The set of states in which the number of failed element is $(k+1)$ and whether the state result in the network being down or up is not known only from the previous check, which is performed to the state in which the number of failed elements is k.
Here, this tool uses the following *P1* as the approximate value of network reliability.
P1＝The probability that at least of a state belong to the set $\{A1 \cup A2 \cup \cdots \cup Ak\}$.
The approximation error R does not exceed the sum of the probabilities of states which belong to set *Ck+1*. Therefore, the true value F is obtained as

$$P1<F<P1+R.$$

For software implementation, the listing procedure should be established for *A1*, *A2*, etc. The following is the procedure for listing the states in which the $(k+1)$ elements have failed and the results of previous checks do not tell us whether the network is up or down.
When $k=1$

Let the set $\{u_1, u_2, \cdots, u_N\}$ be the set of all network elements. Let us consider that all states in which one elements has failed are checked in any of n elements $u_1, u_2, \cdots, u_n$ will mean that the network is down. The next check should be of states in which the number of failed elements is two. In this condition, the next check should be of those states obtained by selecting pairs of elements that do not include any of $u_1, u_2, \cdots, u_n$. So, we select pairs of elements from the set $\{ u_{n+1}, u_{n+2}, \cdots, u_N \}$, which is obtained by subtracting $\{ u_1, u_2, \cdots, u_n \}$ from the whole set $\{u_1, u_2, \cdots, u_N\}$. The check is then of states in which two elements from the selected set fail.
For higher values of k

Let us consider the set of states in which k elements have failed and this has not resulted in the network being down.

$$(a_{11}, a_{12}, \cdots, a_{1k})$$
$$(a_{21}, a_{22}, \cdots, a_{2k})$$
$$(a_{31}, a_{32}, \cdots, a_{3k})$$
$$\cdots\cdots\cdots$$
$$(a_{M1}, a_{M2}, \cdots, a_{Mk})$$

Here, $(a_{i1}, a_{i2}, \cdots, a_{ik})$ $(i=1, \cdots, M)$ denote the state and M is the number of states that satisfy the above condition. Those states are ordered by the following rule. A state $(a_{i1}, a_{i2}, \cdots, a_{ik})$ has an earlier in order than $(a_{j1}, a_{j2}, \cdots, a_{jk})$ if the first different sorting criterion is the kth one a_{ik} is smaller than a_{jk}.
Here, the set of states to be checked $(b_1, b_2, \cdots, b_k, b_{k+1})$, must satisfy the following condition.
Any k elements selected from $(b_1, b_2, \cdots, b_k, b_{k+1})$ must coincide with one of the above set $(a_{11}, a_{12}, \cdots, a_{1k})$, $(a_{21}, a_{22}, \cdots, a_{2k})$, $\cdots$, $(a_{M1}, a_{M2}, \cdots, a_{Mk})$.
Therefore, exhausting such combinations of elements without overlapping and omission leads us to a solution.

4.2 *Method for checking of the network state*

To implement the above method of analysis as a software tool, a clear procedure for checking whether the network is up or down for a given state has to be established. The tool treats the network configuration as a connectivity

matrix.

A leased circuit connects two routers. The connectivity matrix is the matrix whose element (i,j) is 1 when routers i and j are connected and 0 when they are not connected. A leased circuit stops when an element that accommodates it fails. For the failure of a given element or elements, we start by carrying out a search to identify circuits that stop in that case. Next, the corresponding elements of the connectivity matrix are changed from 1 to 0. Thus, the connectivity matrix for the failure condition is obtained. As the element (i,j) of the matrix which is obtained by N times the product of connectivity matrix under failure condition denotes whether or not routers i and j are connected under failure conditions. Where N is the dimension of the matrix. We can check whether the network is up or down for an arbitrary state.

5.0 SOFTWARE TOOL

By using the above model and algorithm, we have developed a software tool for evaluating the reliability of private networks. This tool has a man-machine interface and an analysis module. The man-machine interface allows editing of the reliability model through the use of symbols that represents network elements (telecommunications nodes, telecommunications links, etc.), and sends the condition thus set up for evaluation to the analysis module. The analysis module performs the reliability evaluation.

Measures that may be applied to improve network reliability are summarized in Fig. 3. The relationship between the measures and analysis by this tool is described below.

Using high-reliability equipment is a simple measure to improve network reliability. Its effectiveness is included by changing the probability of failure for the relevant network elements. A further measure is to set up a backup server. The effectiveness of this measure is also included in the evaluation. These measures are taken by the customer. On the other hand, avoiding the concentration of circuits in the carrier network or setting up of a back-up route for transmission are performed by the carrier. Their effectiveness is also included in evaluation.

6.0 EXAMPLE OF EVALUATION

The following is an example of evaluation. We consider this to be a typical case in the business of providing private-network solutions.

6.1 *The role of reliability value in evaluation*

Precise values for equipment reliability are not important, because the customer's attention will be focused on differences between the reliability of different network designs. However, effective measures are not selectable without a rough knowledge of equipment reliability.

A leased circuit has very high reliability, because the telecommunications carrier will usually use special high-reliability equipment and the transmission hierarchy includes a redundant route for the links. On the other hand, the equipment at a customer's site will not have such high-reliability. In particular, IP communication is becoming increasing popular, and the reliability of IP communications and IP equipment is much lower than that of communications provided by a telecommunications carrier. A few research results for Japan have been reported by JIPDIC[3] and REAJ [4]. They show that the MTBF of the telecommunication network in a typical office is thousands of hours and the average downtime is one or two hours. Therefore, the unavailability is of the order of 10^{-3} to 10^{-4}. These levels of reliability are very low compared with those for a carrier.

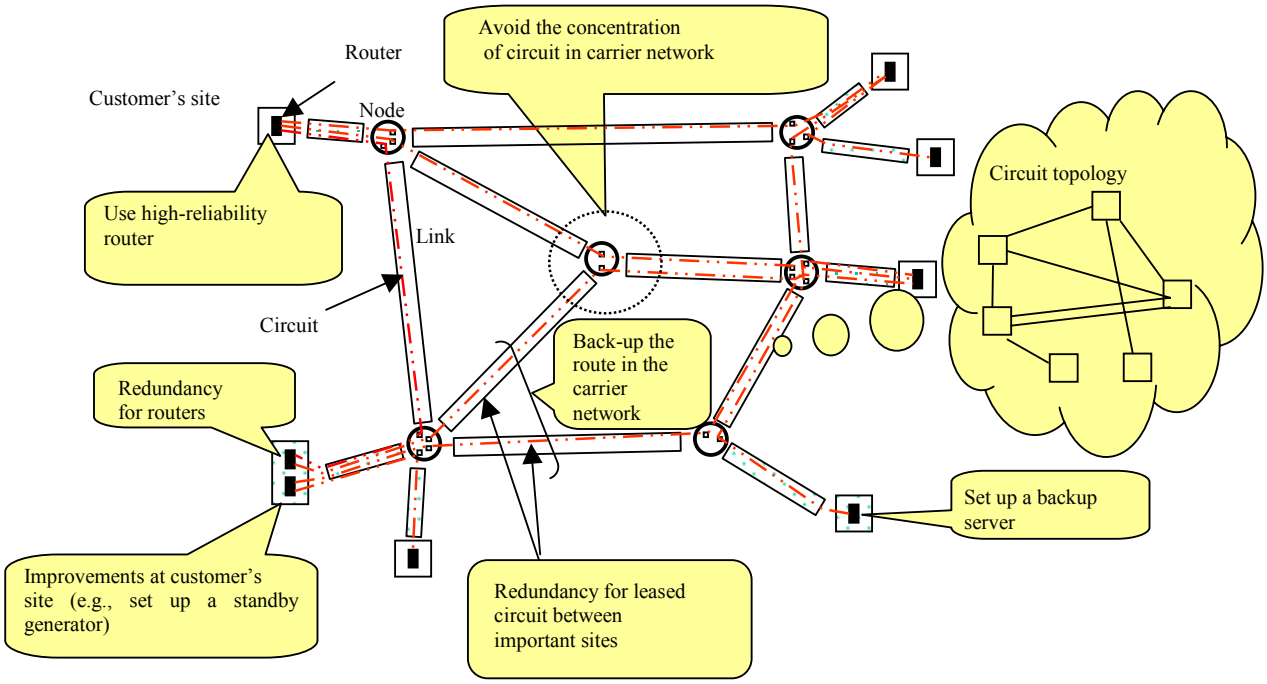


Fig. 3 Measures to improve network reliability.

Therefore, in actual analysis, we can suppose that the reliability of the customer's equipment is low while the reliability of the carrier's equipment is high. That is to say, the customer's sites and routers have low reliability and telecommunication nodes, equipment in telecommunication nodes, and telecommunication links have rather high reliability.

6.2 *Example network*

As an example, consider a network in which each branch site is connected, via a leased circuit, directly to a central site that has a server (Fig. 4). This configuration forms a shape like a star, and so is hereafter called a star network. This is a typical configuration for the private networks used by many companies and government organizations. How can we improve the reliability of this network?

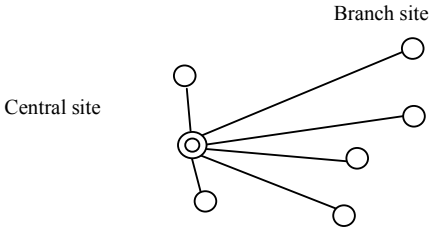


Fig. 4 A star network

Firstly, we need to investigate how the customer uses the network. We suppose that there are two types of use, as defined in section 3. Specifically:
(1) Type 1: A server is placed at the central site and branch sites access it. Traffic only flows along links between the center and each branch sites.
(2) Type 2: Each site communicates on an equal basis. Here, traffic flows between distributed combinations of points on the network.

Secondly, we consider major failures in the network. These are of two major types.

(1) Breakdown at a customer's site: A failure that causes a complete equipment outage at a site. One of the causes of such a failure is a system failure in the power supply at the customer's site.
(2) Breakdown of equipment at a customer's site: A failure due to an individual equipment outage. Such a failure only affects one router.

Then assumptions based on the difference in reliability between the customer and carrier sides. Therefore, the network malfunctions can be classified into two cases.
Case 1: A failure at the customer's site or of the customer's equipment causes loss of communications originating at the site.
Case 2: A failure at the customer's site or of the customer's equipment causes loss of communications passing through the site.
After the above preliminary investigation, we evaluated the effects of some measures for improved network reliability for each type of network usage.

6.3 *Countermeasures for type 1 usage*

For this type of usage, applicable countermeasures vary according to whether or not there is a backup server.
Case 1: There is no backup server
If the central site breaks down, all communications are lost. Therefore, the only approach is to improve the reliability of the central site. One countermeasure is to set a standby generator up at the central site. If a branch site breaks down, communication related to this site is lost. There is no countermeasure against it. If a branch site that is handling a communication-in-transit fails, that communication is lost. One countermeasure against failures of this type is to set up a circuit connecting the branch site directly with the center. Therefore, in case that there are no backup servers, countermeasures are restricted.
Case 2: There are back-up servers
The probability of both the server and backup server breaking down is low, so the reliability of the central site's functions is improved. This has another effect. Fig. 5 shows the probabilities that certain numbers of branch sites will be unable to access the server or backup server under several network configurations.

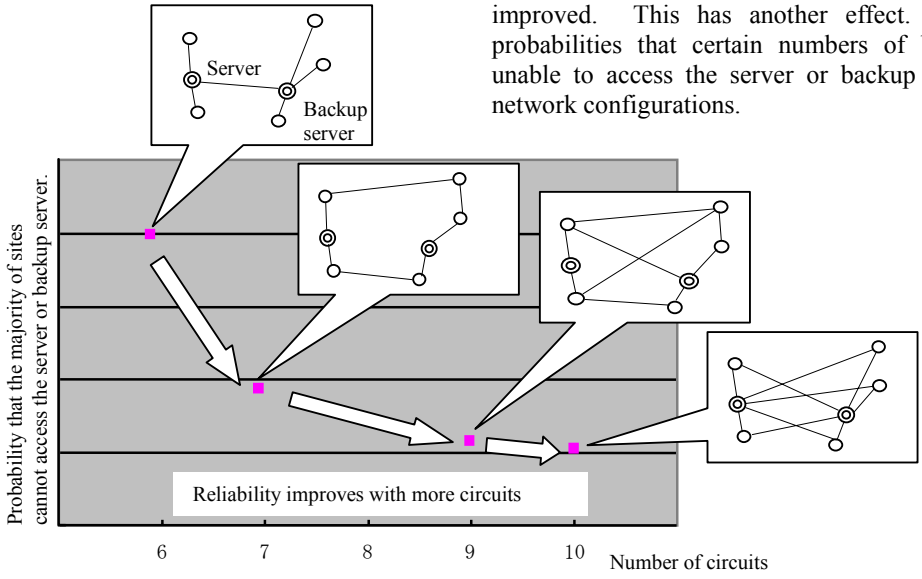


Fig. 5 Evaluation example.

The effect of improving reliability by increasing the number of circuits depends on the skill of the designer in determining the network configuration. Our tool is an effective aid for the designer. The backup server does not have the full functionality of an active server. If we give the backup server only the important server functions, there will be very little increase in cost. In many previous studies of network reliability, the link reliability was assumed to be much lower than the node reliability. In that case, providing redundant links is an effective approach. On the other hand, we might think that link redundancy would serve no purpose under the above conditions, but this is not correct. Site-to-site communication is performed via other sites; link redundancy is thus useful because it provides a roundabout route via another circuit, so it does improve reliability. Increasing the number of links leads to greater reliability.

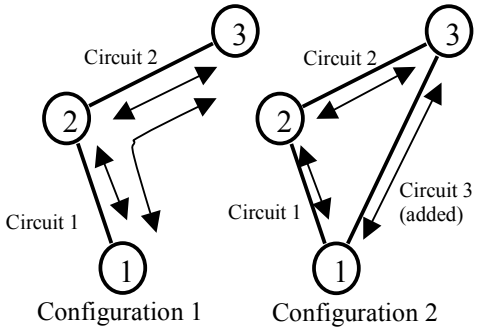
6.4 *Countermeasures for type 2 usage and a new design concept*

For this type of usage, the countermeasure is to add circuits that directly connected pairs of branch sites between which the traffic is heavy (Fig. 6).

This reduces failures in which traffic is lost when site-transit traffic is blocked. This countermeasure increases the number of circuits. Therefore, customers might dislike this network configuration. However, the amount of switching traffic is lowered (Fig. 6), which makes a reduction in the cost of switching possible. This is a new design concept.

Furthermore, if we combine the countermeasures for both types of usage in an effective way, we might be able to improve reliability without increasing the total cost of network6.5 *The evaluation of carrier-side reliability*

Although reliability on the customer side is poor, some customers will want to know about the carrier-side reliability. In evaluating the carrier-side reliability, we assume that the probabilities of failure in the customer's site and routers are 0. This evaluation makes the real worth of carrier-side reliability clear. Fig. 7 shows the probability that the server or backup server is inaccessible to particular numbers of branch sites. These conditions of evaluation should be changed according to the type of solution to be provided. This tool copes with such usage.



Traffic handled in each element

	Config. 1	Config.2
Circuit 1	2	1
Circuit 2	2	1
Circuit 3	___	1
Transit node	2	0

Fig. 6 A countermeasure for type 2 usage.

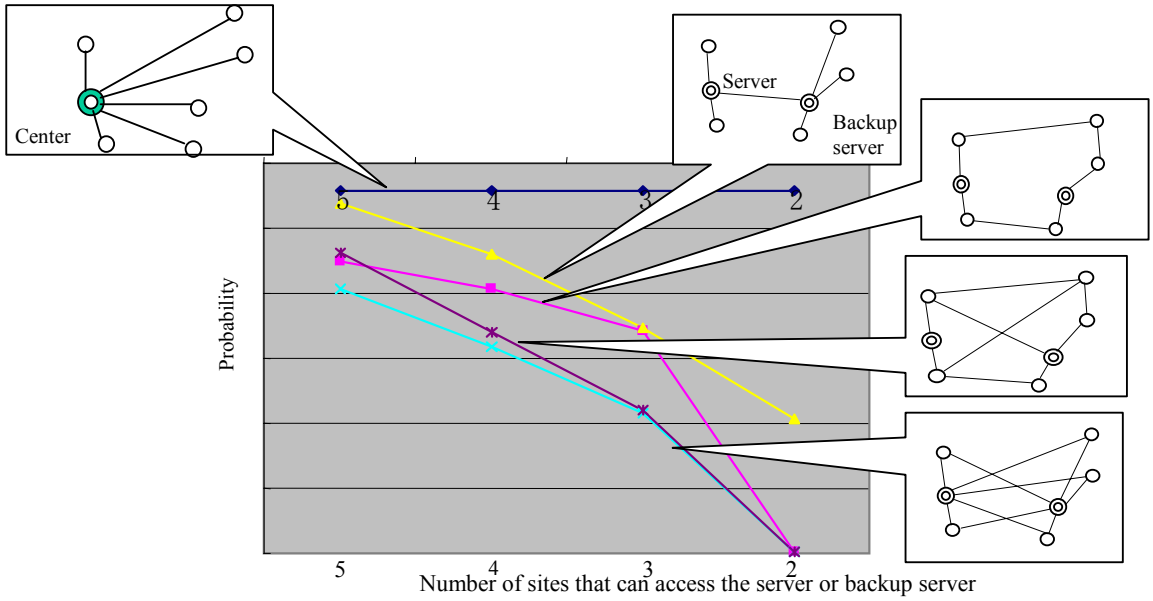


Fig.7 Evaluation of carrier side reliability

7.0 CONCLUSION

We have developed a tool for evaluating the reliability of private networks. It is designed to ensure that the network owner is satisfied with the reliability design. We investigated the reliability characteristics of many types of private networks, taking into account the work performed with the aid of the network. We also pointed out the possibility of a new design method that is applicable to achieving both high levels of reliability and low cost.

REFERENCES

(1) Eric S. Tollar and Jay M. Bennett: "Network Outage Measure for Telecommunications", IEEE Symposium on Computers and Telecommunications, Alexandria, 1995
(2) S.Nojo and H.Watanabe: "Incorporating Reliability Specification in the design of Telecommunication Networks", IEEE Com.Mag., June 1993. pp.40-43, 1993
(3) http://www.jipdec.or.jp/ (in Japanese)
(4) http://reaj.i-juse.co.jp/(in Japanese)

BIOGRAPHY

Hitoshi Watanabe
Nippon Telegraph and Telephone Corporation (NTT)
9-11, Midori-Cho 3-Come
Musashino-shi, Tokyo 180-8585 Japan

watanabe.hitoshi@lab.ntt.co.jp

Hitoshi Watanabe graduated from the Nagoya Institute of Technology with a Bachelor of Engineering degree in Electronics in 1979. In 1981, he graduated from the Nagoya Institute of Technology with a Master of Engineering degree in Electronics. He has received his Ph. D (Engineering) from Nagoya Institute of Technology in 2002. He joined NTT laboratory in 1981 and had engaged in research of reliability design of telecommunication networks and systems. He is now a Senior Research Engineer of NTT Service Integration Laboratories.

Minetoshi Kudo
Nippon Telegraph and Telephone West Corporation (NTT West)
NCB Bldg. 6-2-27 Nakanoshima kita-ku, Osaka 530-6601, Japan

m.kudo@bch.west.ntt.co.jp

Minetoshi Kudo graduated from the Dousisha University with a Bachelor of Engineering degree in Information Technology in 1973. He joined NTT in 1973 and has engaged in the development of data communication systems and communication software. From 1995, he has been engaging in the solution provision business, especially of the high reliable private network. From 1995 to 1997, he was the Project Manager of Designed and developed system for Hyougo Prefecture Emergency disaster information system. Now he is the Project Group Manager of Application system Design and Development Department of Solution Business Headquarters in NTT West.

Kazuhiro Kawanishi
Nippon Telegraph and Telephone West Corporation (NTT West)
NCB Bldg. 6-2-27 Nakanoshima kita-ku, Osaka 530-6601, Japan

k.kawanishi@bch.west.ntt.co.jp

Kazuhiro Kawanishi graduated from the Tsukuba University with a Bachelor of Science and Engineering degree in Information Science in 1993. In 1995, he graduated from the Tsukuba University with a Master of Science and Engineering degree in Information Science. He joined NTT in 1995 and belonged to the Multimedia Business Department. From 1998 to 2000 he has engaged in the design of computer software and network (LAN/WAN) at some systems. Now he is the Chief Engineer of Sales Department of Solution Business Headquarters in NTT West. Currently he is engaging in the planning of visual communication systems and WEB application systems and development of the evaluation program for network reliability.

Koji Yamasaki
Nippon Telegraph and Telephone West Corporation (NTT West)
NCB Bldg. 6-2-27 Nakanoshima kita-ku, Osaka 530-6601, Japan

k.yamasaki@bch.west.ntt.co.jp

Koji Yamasaki graduated from the University of Ryukyu with a Bachelor of Engineering degree in Mechanical Systems Engineering in 1993. In 1995, he graduated from the University of Ryukyu with a Master of Engineering degree in Mechanical Systems Engineering. He joined NTT in 1995 and had engaged in network solution business especially for networks for disaster information. He is now a member of Sales Department of Business Communications Headquarters of NTT WEST.