WORLD METEOROLOGICAL ORGANIZATION

ISS/ET-DCST 99/Doc. 18
(22.IX.1999)

COMMISSION FOR BASIC SYSTEM
OPAG ON
INFORMATION SYSTEMS & SERVICES
EXPERT TEAM MEETING ON DATA-COMMUNICATION SYSTEMS AND TECHNIQUES

ITEM 5.1

GENEVA, 27-30 SEPTEMBER 1999

ENGLISH only

Dedicated telecommunications circuits

Submitted by Germany

This document should provide some basic ideas for setting up ISDN backup links

i. Use of ISDN as backup to dedicated links

If there is the requirement to have an almost 100% availability for a network link, a backup mechanism is needed.

If there is more than one path to a given destination, one could achieve backup by routing the packets along a second (backup) path in case of a failure on the primary link. However, this always has the risk of overloading the backup link and therefor delay the transfer of all other data being transferred there. So careful traffic engineering and management would be required before implementing it. Also, the involved centers have to agree on a routing policy that would permit a center to use another than the primary (and mostly direct) path and perhaps even some cost issues would have to be clarified.

Another very common method to establish a backup is to set up an ISDN line. This causes always additional costs since there is at least the basic monthly fee. An ISDN line can be used as a backup to more than one center (in case those centers have ISDN backup installed as well), and the resulting higher reliability of the communication infrastructure is in most cases worth the extra costs. However, each center has to decide how reliable it wants to set up it's network links and whether or not it's necessary to have a backup link.

For Cisco routers, there are several options as to how configure the backup.

1. backup interface

   The easiest way to achieve backup is to define the ISDN line as the "backup interface" to the interface that connects to the primary line. As long as the primary line is up, the ISDN line will be in a "down" state, and it will be brought up automatically when there are problems on the primary line. When the primary line comes up again, the router will automatically take down the ISDN backup line (after a configurable time delay).

   The disadvantage with this approach is that each 2 centers have to agree on which side configures the backup interface (it can only be done on one side). Also, the ISDN line can't be used for anything else (e.g. testing purposes).

2. configuring so called “floating static routes”

   If a center has more than one dedicated link that should be backed up, configuring static routes with a higher “metric” than the routing protocol uses (floating static routes) is the more preferable solution.
   In that case, the dynamically created routing information in the routing table would disappear when the primary link fails and the static route would be installed. Every IP traffic would then be sent along this backup path. Each center can issue the ISDN connection setup.
   For the ISDN connections between 2 centers IP networks similar to the primary lines would be required. Since this in turn has influence on the routing protocol and size of routing tables, careful planning of IP addressing is required. It might be a good idea to allocate 2 continuous networks for this purpose (1 for the Leased Line, 1 for the ISDN backup line) to allow for route summarization.

   The ISDN backup like can be used also for other communication then, e.g. for testing.

   Floating static routes have been used in DWD’s national network for 3 years now, and the experience is that it is a very reliable backup solution. The applications using the network infrastructure normally don’t even notice the switch to backup link or vice versa.

   Our experiences also show that it is very important to set up a mechanism that informs about the failure of a primary link (e.g. a network management system or some script that permanently checks a routers SYSLOG entries). Since a fast converging routing protocol ensures that the backup line goes into operation before any tcp timer finally expires, the applications will continue to work. So if no action is taken about the failed primary line, the ISDN line will stay up infinitely and cause extra costs.
   It is also necessary to decide carefully which traffic should bring up the backup line; e.g. ping from network management systems and UDP traffic could keep up the line. One can also check the calling party and accept only calls from authorized centers.

   Once the primary link comes up again, the newly learned dynamic route will be installed in the routing table, the IP traffic will be sent along the primary path, and the ISDN call will disconnect.

   Depending on the router hardware, one can bundle 1 or more ISDN basic lines together, and can either have backup to more centers that way or also use more than 1 ISDN B-channel to one destination (always assuming the remote center has the required hardware too).

   Sample Cisco router configuration files for each case can be provided.

   If the costs for an ISDN line are too high, but the center has an Internet connection, backup could also be established via the Internet. It is then necessary to implement a different security policy than the one that is now recommended in the guide. The security measures are necessary on both the hosts and the router/firewall system(s) that connect to the Internet.