DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

Redundancy Techniques Using DCB Tunnel Devices and Software
Revised 4/18/2022

Users have come to rely on DCB tunnel products to implement multicast voice over IP networks that might not otherwise be configured to allow it. One example is public safety dispatch, an application in which downtime must be kept to a minimum. Thus it is not unusual for customers to ask questions about techniques that may be applied to make the tunnel network more robust. The purpose of this document is to describe some of those techniques when using UT, XT, or FT encrypted tunnels.

One of the simplest methods users can employ is **unit redundancy**. In planning for the possibility of storms or other phenomena damaging data communications equipment, a few spare tunnel units are purchased to keep on-hand in the event one of the deployed ones becomes unusable. Because each DCB tunnel device can upload its configuration to a file, the most effective way to use unit redundancy is to keep copies of the configuration files for all units on the network. (NOTE: As a security consideration, the files are stored in binary format and are encrypted with a password that can be up to 51 characters in length.) This way, if one of the "shelf-units" needs to be put into service, a previously saved configuration file may be loaded into it and the units may be swapped far more quickly than if the parameters were all re-entered by hand. This also insures that all IP addresses, client names and passwords will be exactly as they had been in the original device, avoiding the risk of having mistyped characters.

Because there is often a main dispatch center hosting the server tunnel device to which one or more remote client tunnel devices connect, this "host site" server is a likely place to begin applying unit redundancy. Otherwise, it could become a single point of failure (SPOF) for the entire network. It is fairly straightforward to set up a backup server by following these steps:

1. Make sure the primary server is currently configured with **all client names and passwords entered exactly as you want them** and with all clients able to connect correctly.
2. Navigate to the **Administration -> Config File** menu on the primary server and save a copy of the configuration file to a PC.
3. Connect the new backup server device to the PC (but not yet to the rest of the network) and load the primary server configuration onto it as well.
4. Modify the untrusted ports (usually labeled LAN1 and LAN2 on most versions) IP addresses of the backup server to be different than the primary, and if distinct names are being used (e.g. "MyPrimaryServer" and "MyBackupServer"), change those in the **Administration -> Set Name** menu.
5. Save a copy of the backup server configuration to a file, then install it on the network.
6. If additional clients are added to the network in the future, ***make sure to add them to the Authorized Client list on both servers***.

Implementing redundancy of servers at the host site is an improvement, but still has certain weaknesses:

- If the power goes out to the entire Host Site, both server units are down
- If (instead of direct Internet connections) both of the server units point to the same router to access the Internet, that router now becomes an SPOF

In order to address the scenario in which both server devices could be lost simultaneously, a technique of **host site redundancy** may be applied in conjunction with the unit redundancy at the server. Such a configuration is diagrammed in Figure 1 below, with the network routers omitted to simplify the drawing.

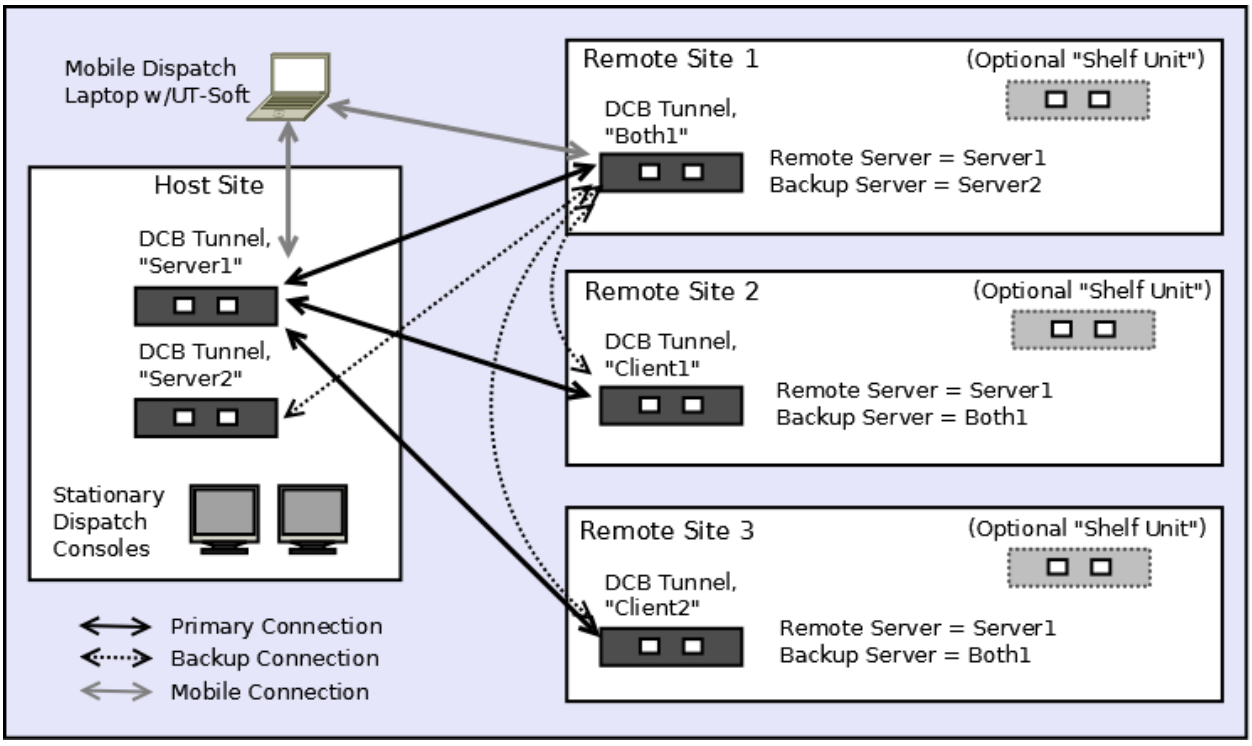

Figure 1 – Configuration for Tunnel Redundancy in a Dispatch Application

This configuration takes advantage of the ability for a DCB tunnel device to be in "**Both Mode**", where it can act as a client to an existing server, but also as a Backup server to other clients. The topology shown in Figure 1 behaves as follows:

In normal operation – Remote sites 1, 2 and 3 all have active tunnels to Server1 at the Host Site. Dispatch duties may be carried out from the stationary consoles at the Host Site, or by a mobile dispatcher using a laptop with the dispatch software and DCB's UT or FT-Soft.

If the Host Site is up, but Server1 fails – Tunnel device Both1 switches over to Server2 as its connection to the Host Site, and devices Client1 and Client2 reconnect to the network as clients of Both1. The mobile dispatcher can redirect the UT/FT-Soft client to point to Server2 and carry on as before.

If the entire Host Site is down – Tunnel device Both1 now acts as the server of a temporary host site, Client1 and Client2 reconnect to the network as its clients and the mobile dispatcher can redirect the UT/FT-Soft client to point to Both1 and carry on as before.

The usage of UT/FT-Soft deserves special mention, in that it allows a mobile dispatcher to connect to the tunnel network ***from anywhere that an Internet connection is available*** and perform their duties from that location. Additionally, the laptop may be configured to quickly connect with any of the three servers of Figure 1 (Server1, Server2, Both1) by creating desktop icons for each of those connections (as detailed in the ***UT/FT-Soft Quick Start Guide***), and by having the UT-Soft client name listed in the Authorized Remote Clients table of each Server or Both unit. Using this technique, the mobile dispatcher may switch from Server1 to Both1 (during a Host Site outage) in just seconds by first closing the Server1 UT/FT-Soft session and then re-launching from the Both1 desktop icon. (**Note: Do not keep two sessions open at once.**)

DCB tunnel devices operate in such a manner that, when the primary connection is once again available (e.g. Server1 is restored or the host site comes back on-line), the clients will re-establish their normal operation without any user intervention. The one exception is the UT-Soft client, but as described in the previous paragraph, with proactive configuration the down-time can be kept to a minimum there as well.

It should be pointed out that the technique of allowing tunnel devices to be in Both mode can only be taken so far. Users have sometimes asked if it is possible to have multiple units in Both mode, each serving the next ones in line in a "mesh" topology. This is possible, but unless great care is taken when configuring each tunnel device, it is also quite easy to create network loops which will cause the whole system to fail. The key point is: ***Between any two nodes, there MUST be only ONE TUNNEL at a time.*** This is the logic which must be carefully thought-out when designing any network incorporating redundancy, and **we would not recommend the mesh configuration be attempted without first consulting DCB Support**.

Everything up to this point has been focused on scenarios in which a single tunnel device or an entire site might fail, but another possible point of failure is the network segment that connects any pair of sites. To mitigate a network link failure, one must have a backup network path to use if the primary network is lost. A representative implementation of **path redundancy** between a host site and a remote site is shown in Figure 2 below:

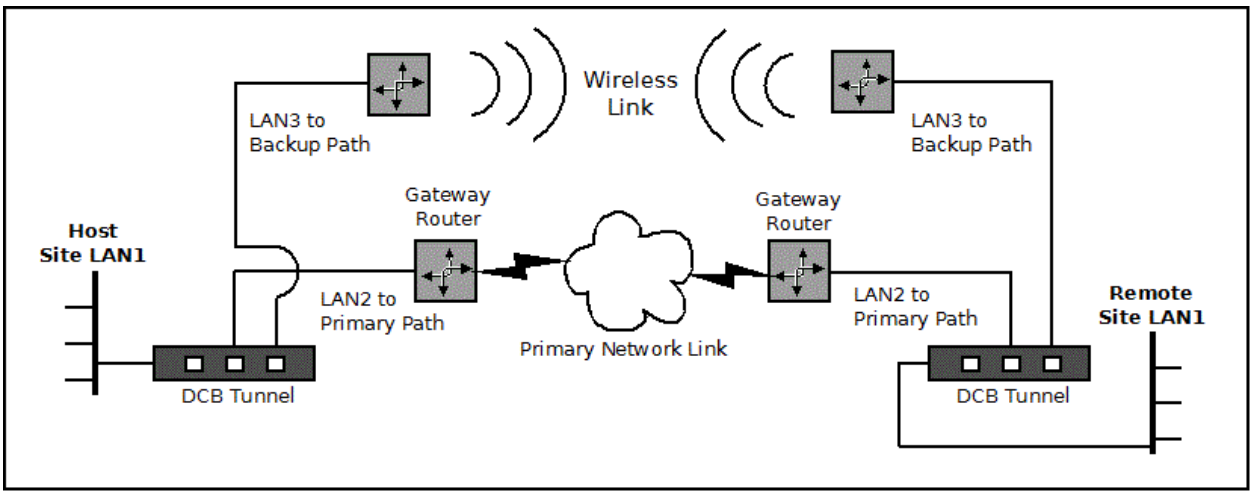

Figure 2 – An Example of Path Redundancy Between Tunnel Devices

Some features to note in this topology:

- One must use the specific models of DCB tunnels that have both LAN2 and LAN3 ports for this purpose.
- If the redundant links were both connected to a common router on either or both ends, the router itself will become a single point of failure: Full path redundancy requires dedicated routers on each path, and at each end.
- It would be best if two distinct network providers were used for the two links, as an outage on a single provider's terrestrial network may have impacts on their wireless links as well.
- Similar to the previous discussion, fail-over will take place automatically, and the link will also automatically return to using the primary path again once it is available.
- The same Client Mode Settings are configured as before, but with the additional option of LAN3 as a Backup Interface, as shown in Figure 3 below:

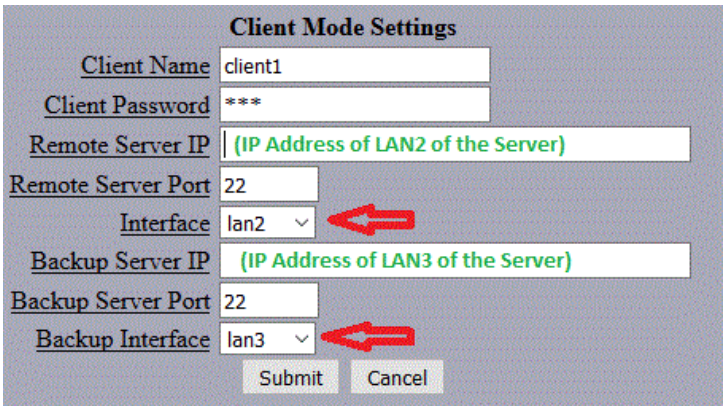

Figure 3 – Client Mode Settings For Path Redundancy

If the wireless link shown in Figure 2 is point-to-point, this method would only work between a single host and remote site. However, if the wireless link is a Wide-Area Network (WAN) such as LTE, it could be applied at multiple sites, allowing elements of the host site redundancy of Figure 1 to also be implemented in conjunction with path redundancy.