



---

---

## **DIRECWAY<sup>®</sup> Application Note**

### **Simple, Standardized, Secure Solutions for**

### **Teleworker and Franchise Networks**

(October 31, 2001)

#### **1. Introduction**

The Teleworker and Franchise Service Packages are enterprise service offerings from DIRECWAY. Both of these network service offerings are designed for the enterprise to support access to corporate private networks over the DIRECWAY system.

The Teleworker service is designed for corporations that want to have their employees access the corporate network from home or remote office locations. The Franchise service is targeted at corporations that wish to have the remote franchise locations access the corporate network.

Both Teleworker and Franchise DIRECWAY service packages consist of the core set of DIRECWAY Internet access and IP Multicast transport services. From a menu of available service options the IT manager can configure a specific package to meet the varying requirements of the organization. These options include but are not limited to:

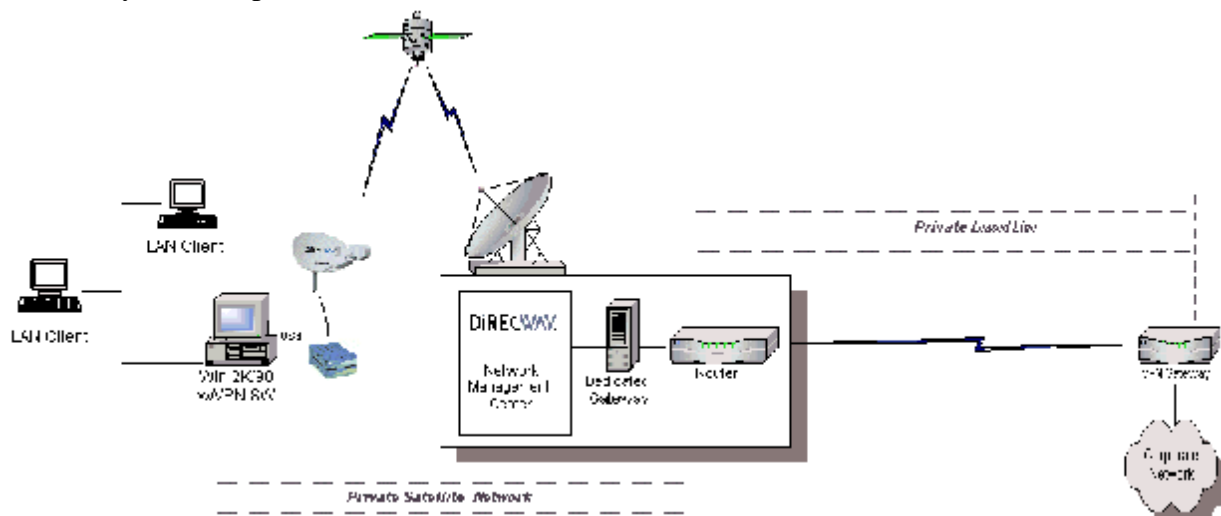
- Onsite repair of DIRECWAY equipment
- Tier 2 or 3 DIRECWAY support
- Customized Service Offerings such as Email accounts or Dial Up Mobility accounts
- General Internet Access via the DIRECWAY NOC
- Web based equipment ordering
- Business Television Services
- Package Delivery Services
- E-Learning Services
- DirecTV equipment bundles
- Static Routable IP addresses
- Business Class Turbo Internet Service Levels

## 2. DIRECWAY Private Network Teleworker and Franchise Networks

The following DIRECWAY Private Network configurations offer solutions for establishing a secure connection to users via DIRECWAY services with the added benefit of DIRECWAY performance enhancing technologies. These technologies include the ability for the DIRECWAY network to accelerate TCP/IP performance with our proprietary software. This software allows a user to experience the fastest communication that DIRECWAY can offer while using the minimal amount of bandwidth. The Teleworker and Franchise network configuration offers fully managed services by DIRECWAY, complete from the users location to the Enterprise LAN connection.

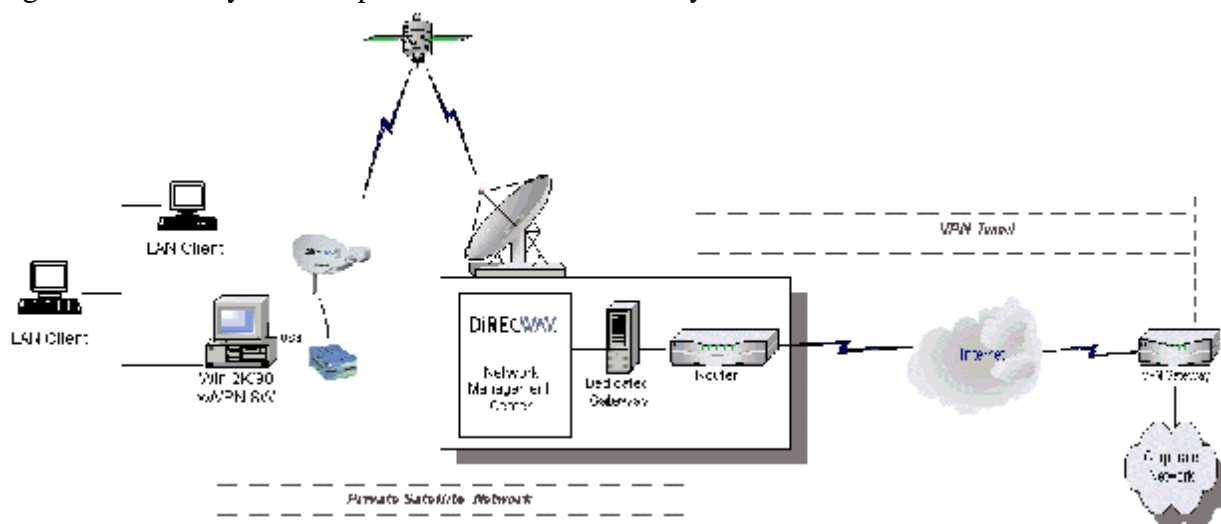
### A. Dedicated Backhaul Option

A dedicated connection to the DIRECWAY Network is a solution that would be effective in most situations where a connection to a corporate Intranet is required. In reality, this is one large private network comprised of two pieces: 1) the DIRECWAY satellite network, and 2) the organization's own private network. A secure point-to-point circuit connects the two secure networks instead of creating a client/server VPN connection over the Internet. For example, an organization's network is connected to the DIRECWAY network using a dedicated leased line (e.g. frame relay T1 circuit). No *virtual* private networking is involved, since two private networks are simply connected together. This approach features dedicated enterprise Network Operations Center (NOC) equipment, including a Turbo Internet gateway, and leased line terminating routers. All equipment and backhaul components are fully managed by Hughes Network Systems as part of the DIRECWAY service.



### B. Secure Shared Backhaul Option

Should the Dedicated Backhaul Option not be a viable option due to availability or cost, the Internet can alternatively be used as the backhaul connection. As the DIRECWAY network is a private network, only the virtual private network connection has to be made across the Internet (the public portion of the data path). This Secure Shared Backhaul requires the enterprise to have their own dedicated Network Operations Center (NOC) equipment, which includes a Turbo Internet Gateway, and two VPN routers/servers. Two Internet-connected VPN routers are used to establish the Secure Shared Backhaul connection; one VPN router is placed in the DIRECWAY NOC and the other on the customer's network. A VPN tunnel is established across the Internet between the DIRECWAY NOC and the customer network, and all data traffic is sent through the established tunnel. As in the previous example, all components are fully managed by Hughes Network Systems as part of the DIRECWAY system.



Both of these network architectures support Teleworker and Franchise Services.

### 3. Why Do Enterprises use VPNs?

Historically a **Virtual Private Network (VPN)** is an extension of a private network that encompasses links across shared or public networks such as the Internet. VPN connections allow users to work at home or at other remote office locations and use the Internet to establish a secure connection to their company's (or another organization's) private network.

VPNs generally address two types of communications security issues. The first is a mobile user that uses dial-up or other remote access methods from an Internet access point other than the host corporation's own dial connections. The second is to connect a remote office in a static location to the host corporation's LAN via an Internet connection.

In both cases, the company private data is encrypted and encapsulated, or wrapped, with a header that provides routing information in order to be sent across the public Internet; this is known as *tunneling*. Encryption and other security mechanisms allow the data to pass through the Internet (or any network) without being intercepted, since the tunneled data is indecipherable without the proper decryption keys. Thus a VPN connection logically behaves as a secure point-to-point connection to the private network, though it uses a public network to transport its data.

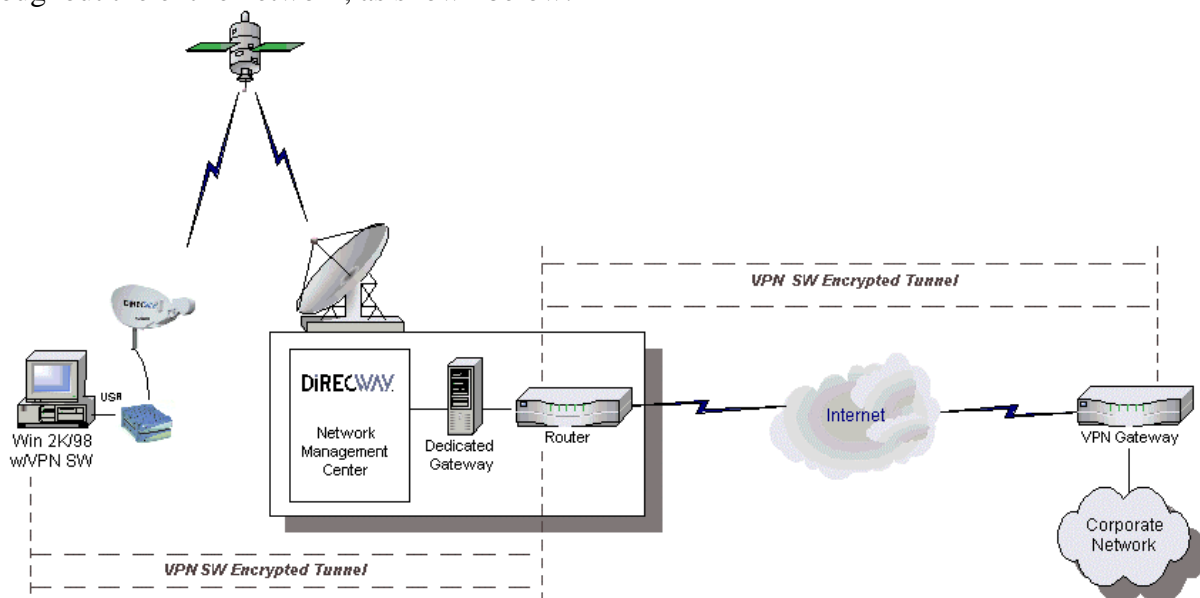
VPNs are used only as a secure transport mechanism for corporations. VPNs are not used as a primary user authentication tool, a user privilege tool, or a workstation level firewall. All of these applications can be bundled with a VPN application as the product manufacturer permits.

#### **4. Typical Client/Server Based VPN applications**

The most widely used VPN architecture over shared public networks is the client/server model. This, however, is **not** a Teleworker or Franchise network as described in Section 2 of this document. This solution is simply standard DIRECWAY Internet access via the DIRECWAY Business Edition, and where the user runs a client/server VPN application to secure the IP connectivity to the enterprise LAN.

This solution does not offer the enterprise a fully managed private network solution. Problems with this approach include licensing for the VPN applications, and remote support of the VPN application at the users sites. Another major disadvantage to this solution is that the VPN software will not allow the DIRECWAY network to accelerate the performance of TCP/IP over the satellite link. This translates to a significant performance difference while using a client/server base VPN application as compared to the normal performance of the DIRECWAY network.

However, the client/server VPN model can, and does work with DIRECWAY. In the client/server model, a software client is loaded on the remote computer that connects over the Internet to a VPN server or router located on the organization's private network. In the DIRECWAY network, the VPN client/server software encrypts and tunnels the data end to end throughout the entire network, as shown below:



As of 10/31/2001 the followin VPN clients that have been tested and certified for use with the Hughes Model DW4000 (DIRECWAY 2-way terminal):

- [Microsoft Windows VPN \(PPTP\)](#)
- [Cisco VPN CVPN-CLNT-30-K9](#)
- [Nortel Extranet Access Client.V02 62.33](#)
- [CheckPoint VPN-1 SecuRemote 4.1](#)
- **AT&T Netclient v5.03 (AT&T proprietary software)**

Other VPN clients continue to be evaluated, and this note will be updated periodically.

### Speed / Throughput Expectations Using Client/Server VPN Applications

A VPN client's performance on an FTP download will vary, but typical rates are approx. 1/3<sup>rd</sup> to 1/2 of the standard DIRECWAY speeds. Client/server VPN connections unfortunately cannot take advantage DIRECWAY performance-enhancing technologies because packets are tunneled by the VPN application from end to end. Typically, all applications that work without a VPN client will work with a VPN client, however often with some decrease in speed.

Following are some commonly asked questions regarding client/server VPN connections over DIRECWAY:

### 5. Frequently Asked Questions

Q: Are there any parameters that I can tune to speed up my client/server VPN service?

A: There is usually nothing that you can tune to speed up the service using a VPN client/server application. Some VPN client installations change the RWIN value of the Microsoft TCP/IP stack. DIRECWAY requires that the RWIN value remain at 200,000.

To check if your VPN client has changed this, go to the following registry entries:

- Win2000 HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters\GlobalMaxTcpWindowSize. This value should be 200000 and HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize. This value should be 200000
- Win98SE/ME HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP\DefaultRcvWindow. This value should be 200000

Q: I'm successfully connected and can ping sites within the corporate network, but HTTP does not work.

A: You must disable the HTTP proxy that is automatically set up by the DIRECWAY system. In your browser proxy setup, disable the proxy for the HTTP protocol. In Internet Explorer, click the tools menu, internet options menu, connection tab, lan settings button, in the Proxy Server section uncheck the box for use a proxy server. In Netscape, click the edit menu, preferences option, advanced option, proxies option, and make sure the button for direct connect to the internet is highlighted.

Q: Can I use a client/server VPN to access my network drives on my corporate network?

A: The inherent latency in satellite networks makes disk sharing difficult but not impossible. Each type of network would have to be evaluated and tuned by the enterprise user to work over the DIRECWAY network.

Q: Where can I purchase DIRECWAY Business Edition?

A: DIRECWAY Business Edition can be purchased via the network of Value Added Resellers. The Value Added Resellers provide local sales support, installation, and personalized attention to your DIRECWAY services.

Q: Can I use a client/server VPN to access my email on my corporate network?

A: Most enterprise email solutions such as Lotus Notes and Microsoft Exchange have several ways for remote users to access their email. The most popular are direct server/database access, Web based email, synchronized mail, and POP3/ SMTP mail. Synchronized mail, POP3 and Web based mail work reasonably well over a VPN connection. On the other hand, directly accessing the database or server with the email client either may not work at all or performance is severely limited.

Q: Can I share my DIRECWAY connection with other computers on a home LAN (e.g. with Microsoft Internet Connection Sharing) and have them connect to my corporate network through a VPN?

A: In most cases, the answer is yes. The VPN client should be installed on the computer that also has the DIRECWAY software. Once the VPN connection is established from the DIRECWAY computer, the computers on the LAN can then share the connection.

Q: My DIRECWAY system shows an error message that TCP/IP is not correctly bound to the Satellite Adapter every time I start the Navigator.

A: The DIRECWAY client performs essential startup diagnostics when Navigator starts. The installation of some VPN clients interferes with these diagnostic checks. These diagnostics include such things as: verifying the TCP/IP stack is installed, properly configured, only one adapter is installed, and the adapter is responding to simple commands, etc. An example of such a VPN client is the CheckPoint VPN -1 client, and requires a registry addition to the DIRECWAY client that disables this check.

The change is as follows:

Open registry editor (regedit.exe)

Create the following registry key if it does not already exist:

HKEY\_LOCAL\_MACHINE\Software\Hughes Network Systems\DirecPC\HealthReport

Under this key, create a DWORD value called ConfigTestEnable

To disable the startup diagnostics, set the ConfigTestEnable data value to 0

Close registry editor

The next time Navigator is started, the startup diagnostics will not be performed.