WAN Failover Scenarios

Using Digi Wireless WAN Routers

This document discusses several methods for using a Digi wireless WAN gateway to provide WAN failover for IP connections in conjunction with another router designated the primary route – for example connected to an MPLS network (see note 3 below). Other options are available, but the ones discussed here are the most common. In these examples the remote sites could be stores, restaurants, bank branches, substations, or any remote office or branch location.

There are two ways to connect the Digi gateway to the primary router:

- via a *WAN* Ethernet port (i.e., a port on a subnet separate from the LAN), or
- via a *LAN* Ethernet port

An Ethernet WAN port provides the simplest option since failover on the router is usually easier to configure. This mode also supports IP Pass-through where the mobile IP address is passed through to the router.

Failover via a LAN port is usually more difficult since a floating static route or similar must be configured with a higher metric to redirect traffic to the Digi's Ethernet address. VRRP however is not overly complex and is designed specifically for failover.

It is important to note, that in cases other than VRRP, the Digi device itself normally does not do anything to initiate or terminate the failover connection. It is up to the primary router to redirect traffic in the event of primary WAN failure.

Also note that Digi wireless WAN gateways are designed to maintain an always-on connection which helps facilitate quicker failover.

The configuration of the Digi gateway depends on the network design and the mode dictated by the network. There are five main modes of operation:

1. NAT mode (the default) without IPsec VPN: in this mode either security is not required, or the devices or workstations provide the security, or a private wireless plan is used.
2. NAT mode plus IPsec VPN and/or GRE: this is likely the required mode for retail stores, banks, etc. where end-to-end encryption and/or tunneling are required.
3. Pass-through mode is where the Digi gateway connects to a designated WAN Ethernet port on the router and some or all data is passed.
4. NAT Disabled: rarely used; static or dynamic routes are applied to the Digi gateway. This is usually only possible where the carrier provides a private plan – i.e., the traffic does not route via the Internet. IPsec VPN may be used if security requirements, such as PCI compliance, require it. The examples below show the more common VPN tunnel modes.
5. VRRP. Here the Digi device helps not only with "last-mile" failover, but can also backup the primary router itself.

Notes:

1: In most cases these same basic concepts can be applied when the Digi wireless WAN gateway is used as the primary *or* only *WAN connection.*

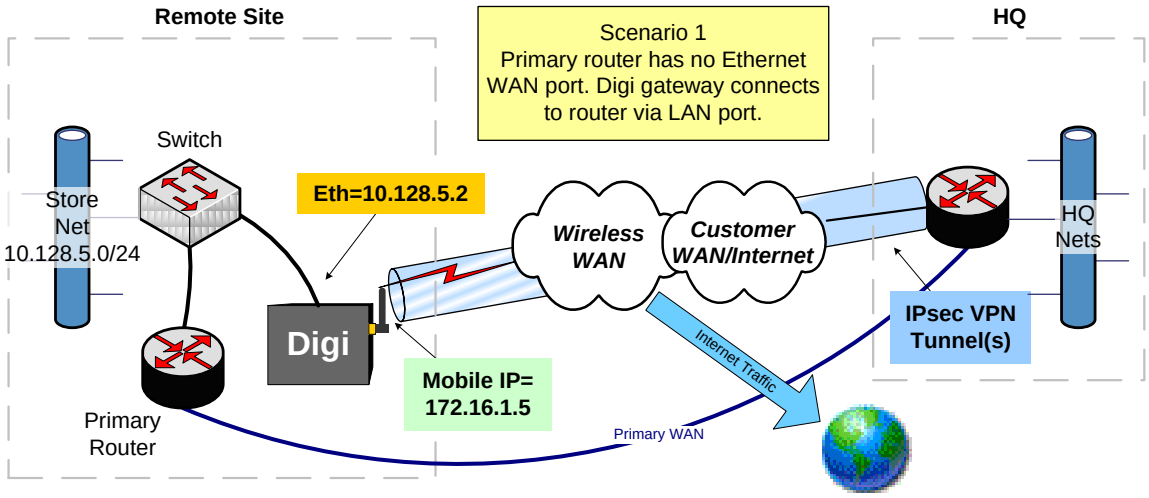
2: This document assumes the wireless carrier provides an Internet connected plan. Many carriers can provide private wireless plans where traffic does not touch the Internet, thus providing more security. Check with your carrier for details.

3: Digi TransPort routers with four Ethernet ports (including those with embedded ISDN or ADSL interfaces) can provide automatic failover *from a primary (e.g. DSL) to a secondary (e.g. cellular) without the need for an additional router. See the end of this document for more information.*

4: Remote out-of-band console management *is also available using the Digi gateway's serial port(s).*

NAT + IPsec VPN Split Tunneling

Here the Digi wireless WAN gateway itself builds VPN tunnels from the remote site to each subnet necessary at the home office. Each remote site must be on its own separate subnet, i.e., a different subnet from the home office and from other remote sites.



How it works: In most cases, the Primary Router will be configured with a floating static route using a higher metric, such as 256, pointing to the Digi gateway's Ethernet IP address (e.g., 10.128.5.2). In some cases, an intelligent layer 3 VLAN switch could handle the routing and failover (note the Digi gateway does not support VLAN itself).

In either case, the Digi gateway will likely need to protect and encapsulate the traffic with IPsec. VPN policies on the Digi device might look something like (assuming the remote site net is 10.128.5.0/24 and the Digi router supports 5+ tunnels):

Source	Destination	Dept
10.128.5.0/24	10.10.0.0/16	Payroll/Benefits
10.128.5.0/24	10.11.0.0/16	IT (Mail servers, Intranet, etc)
10.128.5.0/24	10.12.0.0/16	Inventory Control
10.128.5.0/24	10.13.0.0/16	Marketing
10.128.5.0/24	10.14.0.0/16	Credit
Split Tunnel = Yes		

Why use this scenario? There are two primary reasons:

(a) The primary router is connected to the Digi wireless WAN gateway via LAN port or an Ethernet switch. It is likely the router cannot initiate a VPN tunnel from a LAN port; nor does the switch support VPN. Therefore the Digi device must create the VPN connection as required by the company's security policies for example to comply with PCI (Payment Card Industry) regulations.

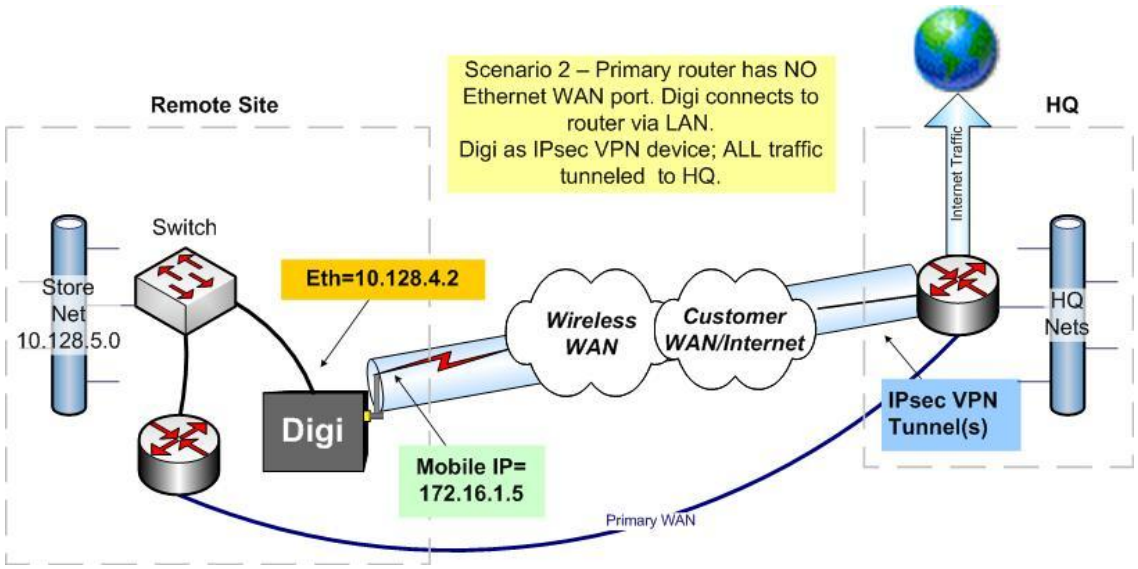
(b) Split tunneling where non-corporate Internet traffic flows outside the VPN tunnel(s) is acceptable (assuming the wireless plan allows Internet traffic).

The major drawbacks are (a) multiple policies must be defined for each remote subnet*, (b) there is less control of Internet traffic outside the realm of the VPN policies, and (c) IPsec VPNs can add significant overhead due to IPsec encapsulation.

[* GRE is supported on some Digi routers such as the Digi TransPort. Routes can be injected into GRE interfaces, which can then be encapsulated into IPsec if encryption and authentication are needed. This would allow multiple subnets or IP address ranges be routed via one IPsec tunnel.]

NAT + IPsec VPN Tunnel All Mode

"Tunnel All" mode is similar to the above, except that ALL traffic from the remote site is tunneled back to the home office via IPsec – i.e., no split tunneling occurs. In the Digi device's VPN policy, the remote subnet is defined as 0.0.0.0/0.0.0.0. All routing and inspection is then done at HQ.



Here is a sample VPN Policy on the Digi gateway:

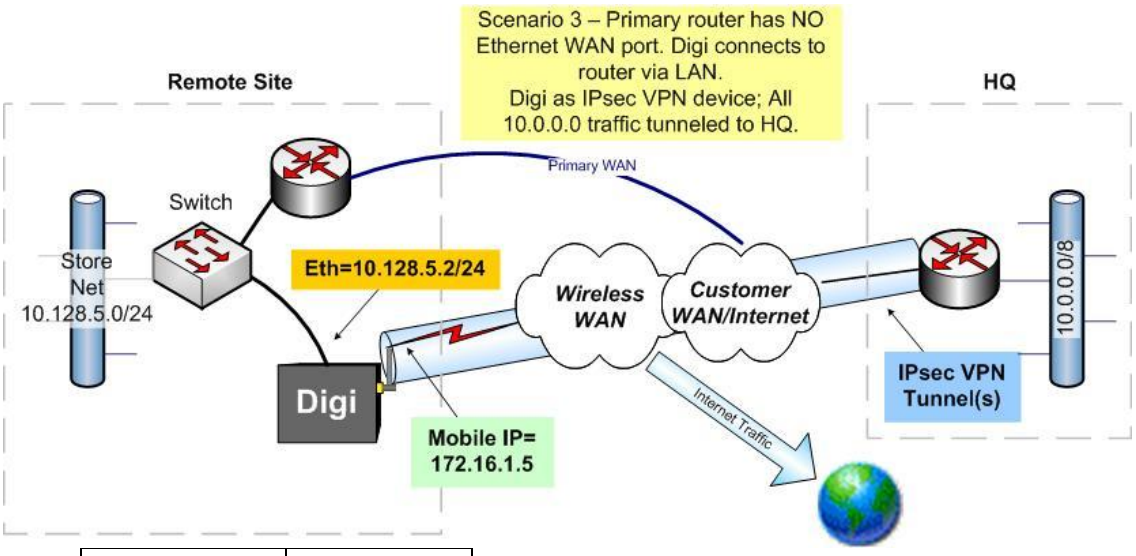
Source	Destination
10.128.4.0/24	0.0.0.0/0
Split Tunnel = No	

Pros: All traffic is routed to the host network providing total control of Internet traffic and enhancing security at HQ. Only one VPN policy is needed for the remote site.

Cons: All traffic is routed to the host network so more management and capacity is required for routing, filtering and controlling Internet traffic at HQ.

NAT + IPsec Tunnel All 10.0.0.0 (or similar)

Here the Digi gateway allows extending the 10.0.0.0 network to 10.x.y.z remote subnets (or similar network configuration). This would allow split tunneling of traffic outside the 10.0.0.0 network but with only one VPN policy similar to:

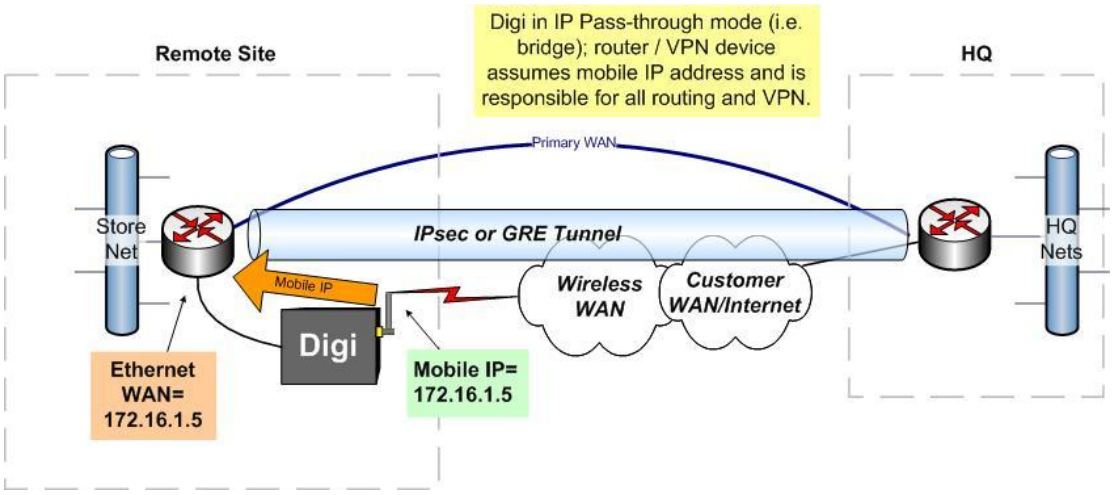


Source	Destination
10.128.5.0/24	10.0.0.0/8
Split Tunnel = Yes	

Why use this method? This is somewhat a comprise between the two approaches above. It still allows split tunneling but simplifies the VPN policy configuration and helps facilitate a "flat" network.

IP Pass-through Mode

In this mode the Digi gateway passes the mobile IP address through to a router or VPN device via Ethernet. The Digi gateway performs much like a bridge. An Ethernet port on the attached device is designated as a "public" WAN port and assumes the mobile IP address. This address can be assigned statically or via DHCP. In this case, the primary router would likely terminate a VPN or GRE tunnel.



Here the primary router/VPN device controls all traffic except for management traffic to the Digi device itself via management *pinholes*.

The primary router/VPN device must have an available port that can be designated as a *"WAN" port* in a subnet separate from the remote site LAN network and the primary WAN port(s). Low-end routers typically have no such option. This option is often used for primary connections in temporary or emergency situations.

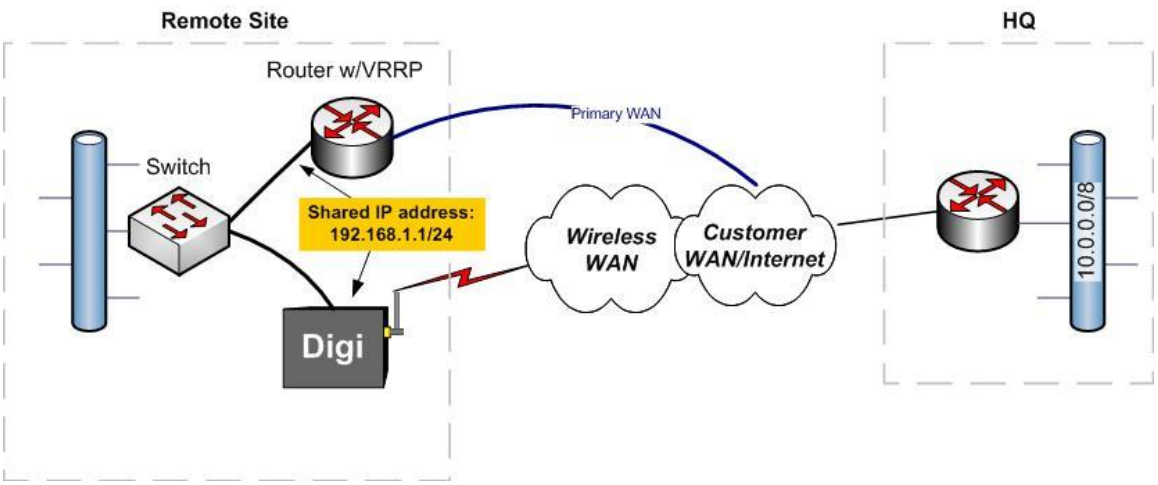
IP Pass-through mode provides management *pinholes* where the user can select protocols such as SSH, HTTPS and telnet that terminate on the Digi wireless WAN gateway itself to provide management functionality. iDigi remote management is also still available.

VRRP

VRRP, virtual router redundancy protocol, is an open standard used for router failover defined by RFC2338 (http://www.faqs.org/rfcs/rfc2338.html). Here the Digi gateway is typically in "stand-by" mode until needed. The Digi device and primary router share the same virtual IP and MAC addresses. This means the hosts on the LAN do not need to relearn new addresses in case of failover.

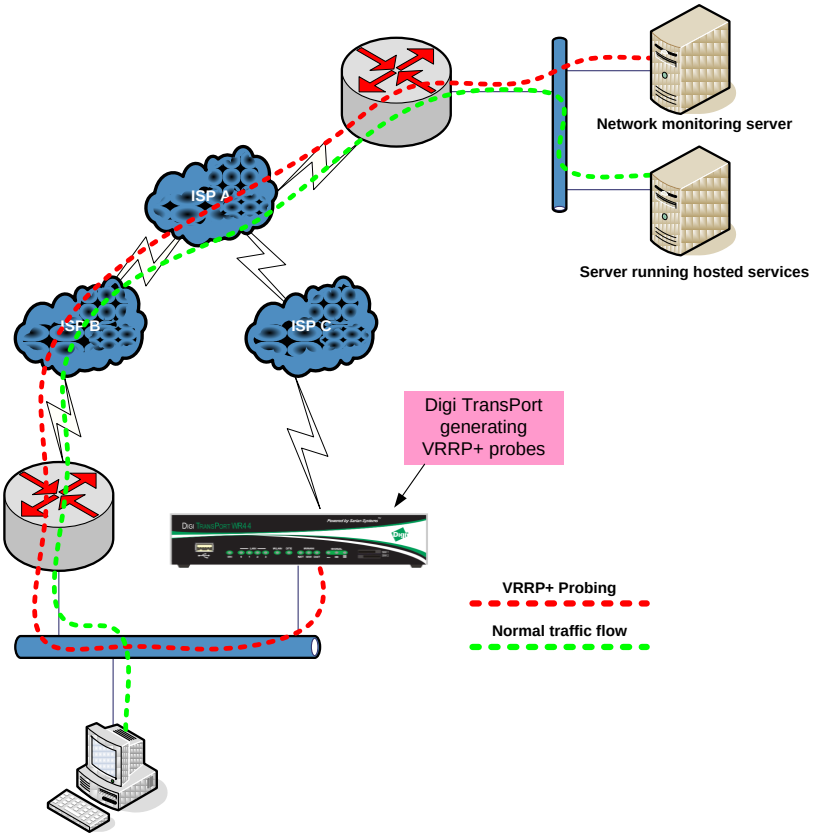
A priority is assigned to each router in the VRRP group, where the highest priority is assigned to the primary router. The backup (or standby) router sits idle until it senses the primary router is no longer available. It then assumes the role of primary and begins routing traffic.

With VRRP, the Digi gateway not only provides failover for the last mile, but the router itself. So, if the router dies, all routing goes through the Digi device.



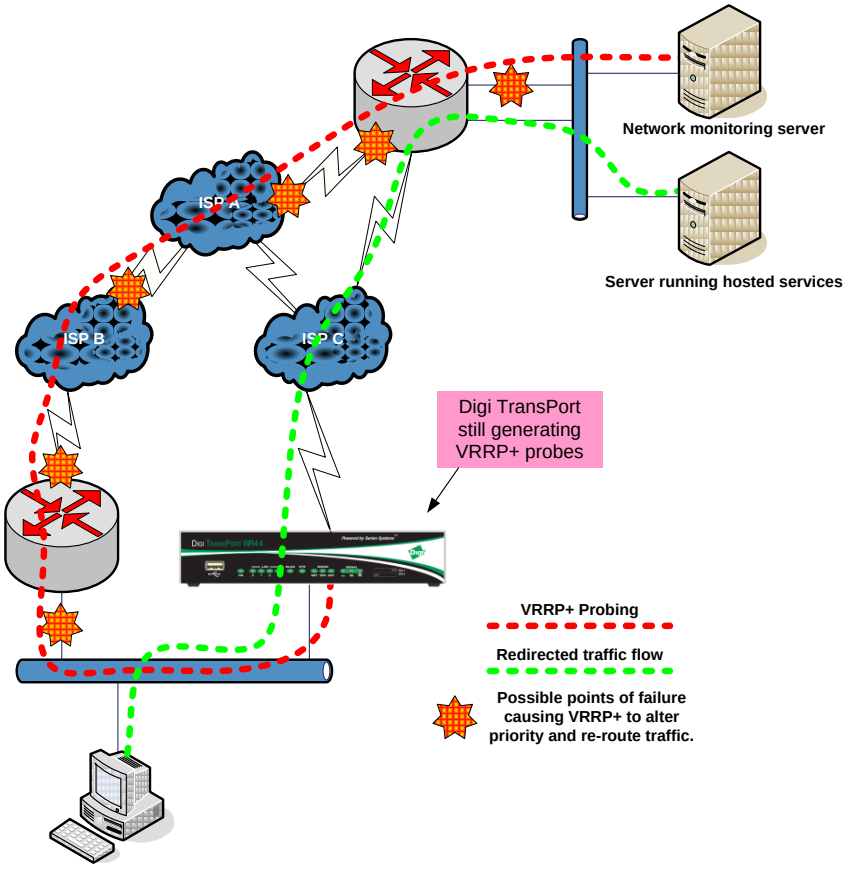
VRRP+

Digi TransPort series routers take VRRP a step further by sending a probe from the Digi TransPort router through the primary router to an IP address at a remote location. Digi's VRRP+ adds a level of robustness above normal VRRP by providing *logical* redundancy in addition to the *physical* redundancy of basic VRRP.



The diagram above shows the path of the VRRP+ probes sent from the Digi TransPort to a host on the remote network and the path of normal data traffic.

VRRP+ probes are sent *through the primary* router to (in this example) a network management server at HQ. If the probes fail to get a response after *n* number of attempts, the Digi TransPort raises its priority higher than the primary router and thus becomes the primary. The TransPort continues to send the probes while primary. The TransPort will lower its priority once the probe responses resume.



The above diagram shows the TransPort assuming the master router role while continuing to send probes.

Full details on VRRP+ are in the TransPort support doc "AN31 - Virtual router redundancy protocol (VRRP) and VRRP+" available at www.digi.com/support.

Other Options

There are other options where the Digi wireless WAN gateway remains in NAT mode and forwards IPsec ESP, GRE, or NAT-T traffic through to a router or VPN device. These methods may be chosen for any number of reasons such as security or specific functionality. These modes were supported before Digi implemented IP Pass-through but are still valid and used in some instances. One example is where the Digi gateway can create a DMZ where, for example, a web server is attached via Ethernet and is accessible from the outside, while a VPN firewall appliance is used to restrict LAN access to workstation. Here is a summary of these modes:

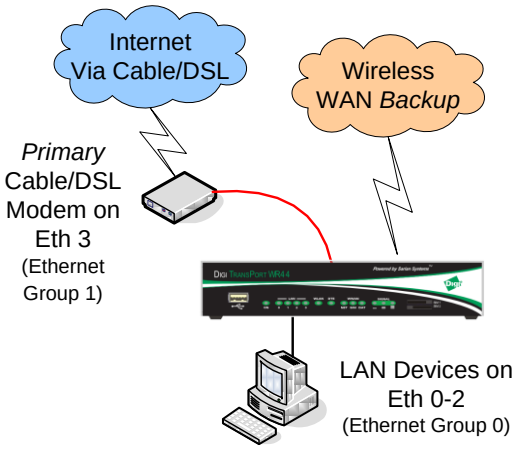
- GRE protocol is forwarded through NAT to a router on the remote site LAN. GRE tunnels can be initiated or terminated on Digi TransPort routers.
- IPsec ESP protocol is forwarded through NAT to a router or VPN device on the remote site LAN. UDP port 500 for IKE should also be forwarded.
- NAT-T: Here IPsec traffic is encapsulated typically in UDP (usually port 4500) in order to traverse NAT firewalls. This port and UDP port 500 for IKE are forwarded through to Ethernet.

Digi TransPort: Branch-in-a-Box with Automatic Failover

As stated in Note 3 above, a multi-Ethernet port Digi TransPort router can provide all-in-one primary and failover capabilities with one router. In most cases, which are covered below, the primary connection will be DSL or a cable modem and the backup connection cellular. But it could be the other way around, or the backup could be dial-up modem or ISDN. The TransPort can be configured in myriad ways.

Some Digi TransPort models have embedded ADSL modems in addition to a wireless WAN module. In this case, the ADSL interface would normally be the primary and the wireless WAN interface is the backup.

In the same way as shown here, one of the four Ethernet ports can be configured as a WAN port and be connected to an external DSL or cable modem or other network termination device that presents an Ethernet port. The TransPort can be configured to check the status of the primary connection and automatically re-route traffic to the backup connection. For GSM models, dual SIM and APN backup are supported.



Further information and assistance is available at www.digi.com or by calling Digi at 952-912-3444. Technical documents including manuals and application notes for specific VPN appliances, IP Pass-through, etc. can be found at www.digi.com/support.